International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

AI-Based Interview Fraud Detection Platform

Divya C. B.[1]
divyacb7990@gmail.com
Assistant Professor
Department of Artificial Intelligence and Machine Learning
Kalpataru Institute of Technology, Tiptur, Karnataka, India

Deekshitha N. M.[2]
deekshagowda602@gmail.com
USN: 1KI23AI013
Department of Artificial Intelligence and Machine Learning
Kalpataru Institute of Technology, Tiptur, Karnataka, India

Ganavi V. C.[3]
ganavivc2@gmail.com
USN: 1KI23AI015
Department of Artificial Intelligence and Machine Learning
Kalpataru Institute of Technology, Tiptur, Karnataka, India

Jeevan K. J.[4]
jeevankj926@gmail.com
USN: 1KI23AI027
Department of Artificial Intelligence and Machine Learning
Kalpataru Institute of Technology, Tiptur, Karnataka, India

M. Shreyas[5]
mshreyas94198@gmail.com
USN: 1KI23AI033
Department of Artificial Intelligence and Machine Learning
Kalpataru Institute of Technology, Tiptur, Karnataka, India

Visvesvaraya Technological University, Karnataka, India

Abstract

The increasing adoption of online interviews has created new challenges in maintaining the authenticity and fairness of recruitment processes. Candidates may use manipulated identities, deepfake videos, prerecorded responses, synthetic voices, or unauthorized external assistance during virtual interviews. Traditional interview methods often lack automated mechanisms to identify such suspicious activities. This paper proposes an Artificial Intelligence (AI)-Based Interview Fraud Detection Platform designed to improve the reliability of online recruitment. The proposed platform integrates facial verification, liveness detection, deepfake analysis, voice authenticity checking, and suspicious activity monitoring. Machine learning and computer vision techniques are used to analyze visual and audio information and generate a fraud risk assessment for review by authorized recruiters. The system aims to provide real-time monitoring, automated alerts, and structured reports while maintaining candidate privacy and human oversight. The proposed approach can support organizations in identifying potential interview irregularities and improving trust in digital recruitment.

Key Words: Artificial Intelligence, Interview Fraud Detection, Deepfake Detection, Face Verification, Voice Analysis, Machine Learning.

1. INTRODUCTION

Online interviews have become an important part of modern recruitment because they allow organizations to interview candidates remotely. They reduce travel requirements, save time, and make recruitment more accessible. However, the use of online interview platforms also introduces several security challenges.

Some candidates may attempt to gain an unfair advantage through identity substitution, prerecorded video responses, deepfake technology, synthetic voice generation, or unauthorized assistance from external sources.

These activities make it difficult for recruiters to verify

whether the person participating in an interview is genuine and whether the responses are provided independently.

Artificial Intelligence (AI) provides useful techniques for analyzing facial information, voice characteristics, video frames, and interview-related activities. Computer vision and machine learning can help identify unusual patterns that may indicate possible manipulation.

This research proposes an AI-Based Interview Fraud Detection Platform that combines multiple verification techniques into a unified system. The platform analyzes interview-related information and generates alerts when suspicious patterns are detected.

The final decision is intended to remain with the recruiter rather than relying entirely on automated predictions.

2. PROBLEM STATEMENT

The major problem in online recruitment is the difficulty of identifying fraudulent activities during virtual interviews. Existing interview platforms generally provide communication facilities but may not offer an integrated mechanism to verify candidate identity, detect manipulated media, and monitor suspicious activities.

Therefore, an intelligent platform is required to analyze multiple interview signals and assist recruiters in identifying possible fraud.

3. OBJECTIVES

The main objectives of the proposed platform are:

- To verify the identity of candidates using facial recognition techniques.
- To detect possible deepfake or manipulated video content.
- To analyze voice signals for possible synthetic or prerecorded audio.
- To monitor unusual activities during online interviews.
- To generate alerts when suspicious patterns are identified.
- To provide a fraud risk report for recruiters.
- To improve the transparency and reliability of online interviews.

4. LITERATURE SURVEY

Artificial Intelligence and machine learning have been widely studied for detecting manipulated digital media and identifying suspicious patterns.

Ro¨ssler et al. introduced FaceForensics++, a dataset and benchmark for facial manipulation detection. Their work demonstrates the importance of analyzing facial information to identify manipulated videos [1].

Li et al. introduced the Celeb-DF dataset to study deepfake video detection. The research highlights the challenges involved in detecting realistic manipulated facial videos [2].

Tolosana et al. presented a survey of facial manipulation and deepfake detection methods. Their study discusses different approaches for identifying manipulated facial content using computer vision techniques [3].

The ASVspoof research initiative investigates spoofed and synthetic speech detection. It provides useful research directions for analyzing audio authenticity and detecting manipulated speech [4].

These studies provide a research foundation for developing an integrated interview fraud detection platform that combines video, audio, and identity verification.

5. EXISTING SYSTEM

Traditional online interview systems mainly provide video conferencing, audio communication, and candidate interaction facilities.

However, several limitations exist:

- Manual identity verification may not identify sophisticated identity manipulation.
- Conventional platforms may not detect deepfake video content.
- Synthetic and prerecorded voice may be difficult to identify manually.
- Suspicious interview activities may go unnoticed.
- Recruiters may need to depend entirely on manual observation.
- Separate verification tools may increase complexity.

Thus, an integrated AI-based monitoring approach can assist in addressing these limitations.

6. PROPOSED SYSTEM

The proposed AI-Based Interview Fraud Detection Platform combines different AI techniques to analyze candidate authenticity during online interviews.

The system consists of the following major modules:

1. **Candidate Registration:** Candidates register and provide the required identity information.

2. **Face Verification:** The system compares the candidate's live facial information with the registered reference image.
3. **Liveness Detection:** The system checks whether the facial input appears to come from a live person rather than a static image or replay.
4. **Deepfake Detection:** AI models analyze video frames to identify possible facial manipulation.
5. **Voice Analysis:** Audio signals are examined for possible synthetic speech or prerecorded responses.
6. **Activity Monitoring:** The system identifies predefined suspicious events during the interview.
7. **Fraud Risk Assessment:** Evidence from the different modules is combined to generate a risk indicator.
8. **Recruiter Dashboard:** Recruiters can review alerts, verification information, and interview reports.

The proposed system is designed to assist human decision-making and should not automatically reject candidates based only on AI-generated alerts.

The proposed system is designed to assist human decision-making and should not automatically reject candidates based only on AI-generated alerts.

7. SYSTEM ARCHITECTURE

The proposed platform follows a modular architecture in which different AI-based components work together to analyze interview activities.

The architecture consists of four major layers:

1. **Input Layer:** Collects live video, audio, and candidate registration information.
2. **Processing Layer:** Processes facial images, video frames, and audio signals.
3. **AI Detection Layer:** Performs face verification, liveness detection, deepfake analysis, and voice authenticity checking.
4. **Output Layer:** Generates fraud alerts, risk indicators, and interview reports for recruiters.

The modular architecture allows individual detection components to operate independently while contributing information to the final fraud risk assessment.

8. METHODOLOGY

The proposed platform uses a combination of computer vision, machine learning, and audio processing techniques.

8.1 Face Verification

Face verification is performed by extracting facial features from the candidate's live video and comparing them with the registered reference image. Facial embedding techniques can be used to calculate similarity between the two representations.

8.2 Liveness Detection

Liveness detection identifies whether the candidate's facial input represents a live person. Facial movements, eye blinking, and other temporal characteristics can be analyzed to distinguish genuine participation from static images or replay attempts.

8.3 Deepfake Detection

The deepfake detection module analyzes video frames to identify possible facial manipulation. Machine learning and deep learning models can examine facial inconsistencies, visual artifacts, and frame-level features.

8.4 Voice Authenticity Analysis

The audio processing module analyzes speech characteristics to identify possible synthetic or prerecorded audio. Features such as Mel-Frequency Cepstral Coefficients (MFCC), spectral characteristics, and temporal patterns can support audio classification.

8.5 Suspicious Activity Monitoring

The platform monitors predefined activities during the interview, including repeated absence from the camera frame, multiple-face appearances, and unusual visual or audio patterns. Detected events are recorded for recruiter review.

8.6 Fraud Risk Assessment

The outputs from the individual detection modules are combined to generate an overall risk indicator.

A weighted risk score can be represented as:

$$R = W_f F + W_l L + W_d D + W_v V + W_A \quad (1)$$

Where:

- R = Overall fraud risk score.
- F = Face verification risk.
- L = Liveness detection risk.
- D = Deepfake detection risk.
- V = Voice authenticity risk.

- A = Suspicious activity risk.
- W_f, W_l, W_d, W_v, W_a = Assigned weights.

The weights are determined during system development and validation. The resulting score is intended as an indicator for human review rather than proof of fraudulent behavior.

9. TECHNOLOGIES USED

The proposed platform can be developed using the following technologies:

Table 1: Technologies Used in the Proposed Platform

Component	Technology
Programming	Python
Frontend	HTML, CSS, JavaScript
Backend	Flask / FastAPI
Database	MongoDB
Computer Vision	OpenCV, MediaPipe
Machine Learning	Scikit-learn
Deep Learning	TensorFlow / PyTorch
Audio Processing	Librosa
Visualization	Dashboard and Reports

10. IMPLEMENTATION

The implementation of the proposed platform involves developing individual modules and integrating them into a unified web application.

Initially, candidates register and provide the required information. During the interview, the system captures video and audio inputs through the authorized device.

The captured information is processed by the respective AI modules. Face verification checks candidate identity, liveness detection examines live facial activity, and deepfake detection analyzes possible video manipulation.

Similarly, the voice analysis module examines audio characteristics, while activity monitoring records predefined suspicious events.

The results are transmitted to the backend, stored in the database, and displayed on the recruiter dashboard. Recruiters can review the detected events and generated risk indicators before making a final decision.

11. EXPECTED RESULTS

The proposed platform is expected to provide an integrated mechanism for identifying potential irregularities during online interviews.

The expected outcomes include:

- Improved candidate identity verification.
- Identification of possible manipulated video content.
- Detection of suspicious synthetic or prerecorded audio.
- Monitoring of predefined unusual interview activities.
- Generation of automated alerts.
- Centralized interview monitoring reports.
- Better support for recruiters during candidate evaluation.

Actual performance must be evaluated using representative datasets and appropriate experimental metrics.

12. ADVANTAGES

The proposed system offers several advantages:

- Combines multiple verification techniques in one platform.
- Reduces dependence on manual monitoring alone.
- Supports real-time suspicious activity alerts.
- Provides structured reports for recruiters.
- Uses modular AI components for future improvements.
- Supports more transparent online recruitment.

13. LIMITATIONS

Although the proposed platform provides multiple verification mechanisms, certain limitations must be considered.

Detection accuracy may depend on video quality, lighting conditions, microphone quality, network connectivity, and dataset diversity.

AI models may produce false positives or false negatives. Facial movements and gaze direction should not be treated as reliable evidence of dishonesty or fraud.

The system also requires appropriate consent, secure data storage, access control, and privacy protection when processing candidate information.

14. CONCLUSION

This paper presents an AI-Based Interview Fraud Detection Platform designed to improve the reliability and transparency of online recruitment. The proposed approach integrates facial verification, liveness detection, deepfake analysis, voice authenticity checking, and suspicious activity monitoring into a unified platform.

By combining these techniques, the system aims to identify potential interview irregularities and provide useful information to recruiters through automated alerts and structured reports.

The platform is intended to support human decision-making rather than replace recruiter judgment. Future development will focus on improving detection accuracy, integrating advanced deepfake detection models, expanding training datasets, and evaluating the platform using real-world interview scenarios.

15. FUTURE ENHANCEMENTS

Future improvements to the platform may include:

- Advanced deepfake detection using transformer-based architectures.
- Improved real-time audio and video analysis.
- Enhanced detection of multiple-person appearances.
- Integration with additional recruitment platforms.
- Large-scale dataset development and model evaluation.
- Improved privacy-preserving processing techniques.

References

[1] A. Ro¨ssler et al., "FaceForensics++: Learning to Detect Manipulated Facial Images," in Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 2019.

[2] Y. Li et al., "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020.

[3] R. Tolosana et al., "DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection," Information Fusion, vol. 64, pp. 131–148, 2020.

[4] X. Wang et al., "ASVspoof 2019: A Large-Scale Public Database of Synthesized, Converted and Replayed Speech," Computer Speech & Language, 2020.