



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

Authenticity Guard in Candidate Introduction Video for Secure Recruitment

Mr. M Hari Krishna¹, Deekonda Renusree², Dattu Mantha³, Ale Pradeep⁴, Bogini Harika⁵

Assistant Professor, Dept. of CSE Data Science, ACE Engineering College, Hyderabad, Telangana, India¹

IV B. Tech. Students, Department of CSE Data Science, ACE Engineering College, Hyderabad, Telangana, India^{2,3,4,5}

ABSTRACT: To improve the reliability and transparency of online recruitment, this study focuses on analyzing candidate authenticity using advanced machine learning techniques. The Authenticity Guard system evaluates multiple indicators such as facial expressions, behavioral patterns, and interview responses during the recruitment process. Instead of relying only on traditional resume screening or manual interviews, the system performs automated analysis on video and textual data to detect potential manipulation, deepfake usage, or suspicious behavior. By analyzing interview recordings and candidate responses, the system provides detailed insights into the authenticity and credibility of applicants. This comprehensive approach helps recruiters make more informed hiring decisions while ensuring fairness and security in the recruitment process. The findings of this system can be applied in secure hiring platforms, automated interview screening, fraud detection, and talent acquisition systems.

Additionally, the system integrates data-driven evaluation techniques to generate an overall authenticity score for each candidate. By combining facial behavior analysis, speech patterns, and response consistency, the model can identify irregularities that may indicate dishonest behavior or the use of manipulated media. The use of machine learning algorithms enables the system to continuously learn from new data, improving detection accuracy over time. Furthermore, the platform presents its analysis through clear visual reports and summaries, allowing recruiters to easily interpret the results without requiring deep technical knowledge. This not only enhances the efficiency of the hiring process but also reduces the risk of fraudulent applications, making the recruitment system more reliable, transparent, and scalable for modern digital hiring environments.

KEYWORDS: Deepfake Detection, Secure Recruitment, Candidate Authentication, Machine Learning, Video Analysis, Facial Expression Analysis, Fraud Detection.

I. INTRODUCTION

With the rapid growth of digital technologies and online platforms, recruitment processes have increasingly shifted to virtual environments. Many organizations now rely on online applications, remote interviews, and digital screening methods to identify suitable candidates. While this transformation has made hiring faster and more accessible, it has also introduced new challenges related to candidate authenticity, identity verification, and fraudulent practices. Applicants may attempt to manipulate the recruitment process using impersonation, deepfake videos, or external assistance during online interviews, which can compromise the fairness and reliability of hiring decisions.

Traditional recruitment methods primarily depend on resumes, manual interviews, and basic background verification. However, these approaches often fail to detect sophisticated fraudulent behaviors or technological manipulations. As a result, organizations require more advanced systems that can automatically analyze candidate behavior and verify authenticity during the recruitment process. Ensuring a secure and transparent hiring system is essential for maintaining organizational integrity and selecting genuinely qualified candidates.

The Authenticity Guard system addresses these challenges by incorporating machine learning and artificial intelligence techniques to monitor and analyze candidate interactions during the interview process. The system evaluates multiple indicators such as facial expressions, video authenticity, behavioral patterns, and response consistency to detect potential manipulation or suspicious activity. By analyzing video recordings and interview responses, the system generates detailed authenticity insights that assist recruiters in making reliable hiring decisions.

II. LITERATURE SURVEY

With the increasing use of online platforms for recruitment and remote interviews, several studies have focused on improving the reliability and security of digital hiring systems. Traditional recruitment systems mainly rely on resume screening and manual interviews, which often lack mechanisms to verify candidate authenticity. As a result, researchers have explored the use of artificial intelligence and machine learning techniques to enhance the security and efficiency of recruitment processes.

Recent research has investigated the use of video-based analysis and facial recognition techniques to detect suspicious behavior during online interviews. Some studies have applied facial expression analysis and eye movement tracking to understand candidate behavior and engagement levels during interviews. These approaches help identify unusual patterns such as looking away from the screen frequently or the presence of multiple people in the frame. However, many of these systems focus only on behavioral analysis and do not consider advanced threats such as deepfake videos or identity impersonation.

Deepfake detection has also gained significant attention in recent years due to the rapid advancement of synthetic media technologies. Several deep learning models, such as convolutional neural networks (CNNs), have been developed to identify manipulated or artificially generated videos. These techniques analyze facial inconsistencies, abnormal blinking patterns, and image artifacts to distinguish between real and fake videos. While these methods are effective in detecting manipulated media, they are often designed for general video authentication and are not specifically integrated into recruitment systems.

III. EXISTING SYATEM

Traditional recruitment systems mainly depend on manual verification of candidate introduction videos, which makes the process both time-consuming and vulnerable to human error. Recruiters are often required to watch submitted videos multiple times to judge whether the content is genuine. However, modern video editing techniques can introduce subtle manipulations such as altered facial expressions, modified lip movements, or synchronized voice adjustments that are difficult for the human eye to detect. As the number of applicants increases, recruiters may struggle to thoroughly review every video, which can result in delays, reduced efficiency, and inconsistent decision-making during the hiring process.

Another major limitation of existing recruitment platforms is that most systems focus primarily on identity verification rather than detecting manipulated or synthetic video content. While traditional face recognition tools can confirm whether a candidate matches an identity stored in a database, they are not designed to detect deepfake videos, facial tampering, or AI-generated media. Because of this limitation, manipulated videos may pass through the verification process without being identified. Such fraudulent content can be used to impersonate individuals, alter responses in recorded interviews, or mislead recruiters, thereby affecting the fairness and credibility of recruitment decisions.

IV. PROPOSED SYSTEM

The proposed system incorporates several intelligent features to ensure accurate and reliable detection of manipulated content during the recruitment process. The system begins with automated deepfake detection, where uploaded or live-recorded candidate introduction videos are analyzed to identify any manipulated or synthetic content. Once the video is received, the system performs frame extraction and face detection, where the video is divided into individual frames and facial regions are detected using computer vision techniques. These detected faces are then analyzed using AI-based deep learning models, specifically a combination of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, which examine spatial and temporal patterns in the video to determine whether the face is real or manipulated.

To make the results more understandable, the system provides **real-time fake highlighting**, where suspicious frames are marked with bounding boxes and labeled as "FAKE" or "REAL." After the analysis is complete, the system generates an **annotated output video** in which manipulated frames are highlighted in red and authentic frames in green, offering clear visual evidence of the detection results. The platform also includes a **user-friendly web interface** that

allows recruiters to easily upload candidate videos, view the analysis results, and download annotated reports. In addition, the system provides **automated decision support** by generating a final authenticity decision along with confidence scores, helping recruiters make informed hiring decisions. Overall, this approach improves **security and trust** in digital recruitment by reducing identity fraud, detecting manipulated media, and ensuring a transparent candidate evaluation process.

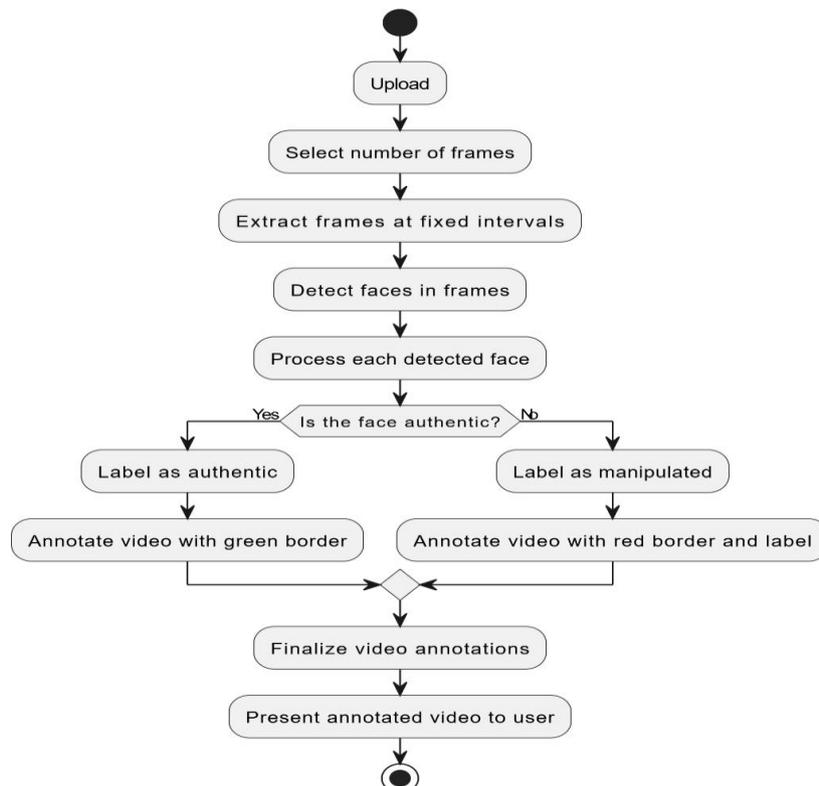
V. METHODOLOGY

The proposed Authenticity Guard system uses deep learning and computer vision techniques to detect manipulated or deepfake videos during the online recruitment process. The system analyzes candidate video input and identifies inconsistencies that may indicate artificial manipulation. The methodology mainly focuses on video preprocessing, frame extraction, feature analysis, and deepfake classification.

Initially, the uploaded video is preprocessed and divided into multiple frames. Video preprocessing ensures that the input data is normalized and prepared for analysis. Each frame is extracted from the video at regular intervals to capture facial information across the entire duration of the video. These frames are then processed using face detection techniques to identify and isolate the facial region of the candidate.

After detecting the face, the extracted facial frames are passed through a deep learning model trained for deepfake detection. The model analyzes several visual features such as facial structure inconsistencies, unnatural blending of pixels, irregular lighting patterns, and abnormal facial movements. These artifacts are commonly found in manipulated or AI-generated videos. The model evaluates each frame individually and assigns a probability score indicating whether the frame is authentic or fake.

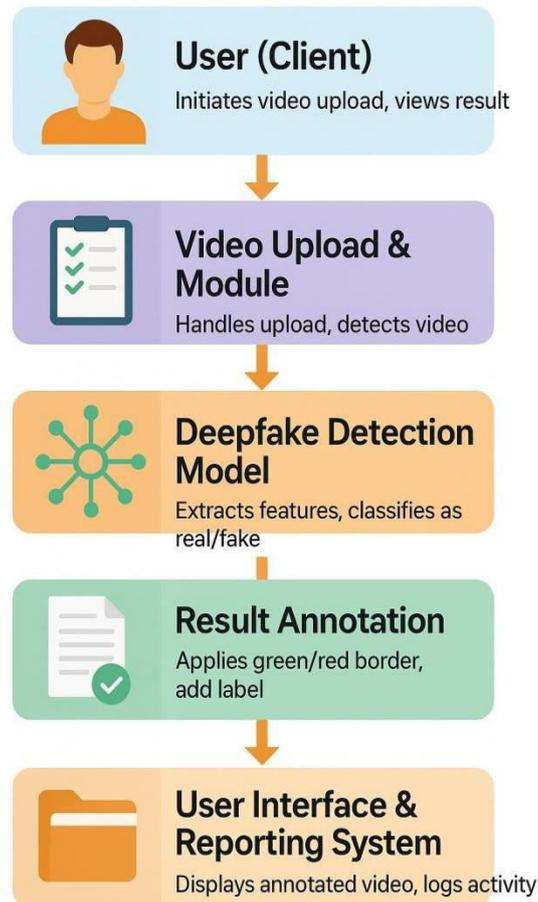
To improve accuracy, the system performs frame-by-frame analysis and aggregates the predictions across all frames. A confidence score is calculated based on the proportion of frames classified as manipulated. This approach ensures that even subtle manipulations that appear only in certain frames can be detected effectively.



The results are then presented through a visualization interface, where the system generates graphs showing the probability of manipulation over the video timeline. Additionally, a detailed frame log is generated to indicate which frames contain suspicious patterns. If the confidence score exceeds a predefined threshold, the system flags the video as a potential deepfake.

By integrating video processing, facial analysis, and deep learning-based classification, the proposed methodology provides a reliable mechanism to detect manipulated videos. This approach enhances the security and authenticity of online recruitment systems by preventing impersonation and fraudulent activities during remote interviews.

VI. SYSTEM ARCHITECTURE



The workflow of the proposed Authenticity Guard system begins with the user (client) uploading a video through the platform. This video typically contains the interview recording or candidate interaction that needs to be verified for authenticity. The Video Upload and Processing Module manages the uploaded file, performs initial validation, and prepares the video data for further analysis. After preprocessing, the video is passed to the Deepfake Detection Model, which extracts important visual features from the frames and applies machine learning algorithms to determine whether the content is genuine or manipulated. Based on the classification results, the Result Annotation Module highlights the output by marking frames with visual indicators such as colored borders and labels that clearly distinguish real content from potentially fake segments. Finally, the processed results are presented through the User Interface and Reporting System, where users can view the annotated video, examine detection outcomes, and access detailed logs or reports.

VII. EXPERIMENTAL RESULTS

Figures show the results of deepfake video detection and analysis using the proposed Authenticity Guard (DeepGuard) system. Fig. 1 shows the video upload interface where the user uploads a video file for deepfake analysis. The system accepts common formats such as MP4, WebM, and MOV and initiates the AI-based detection process.

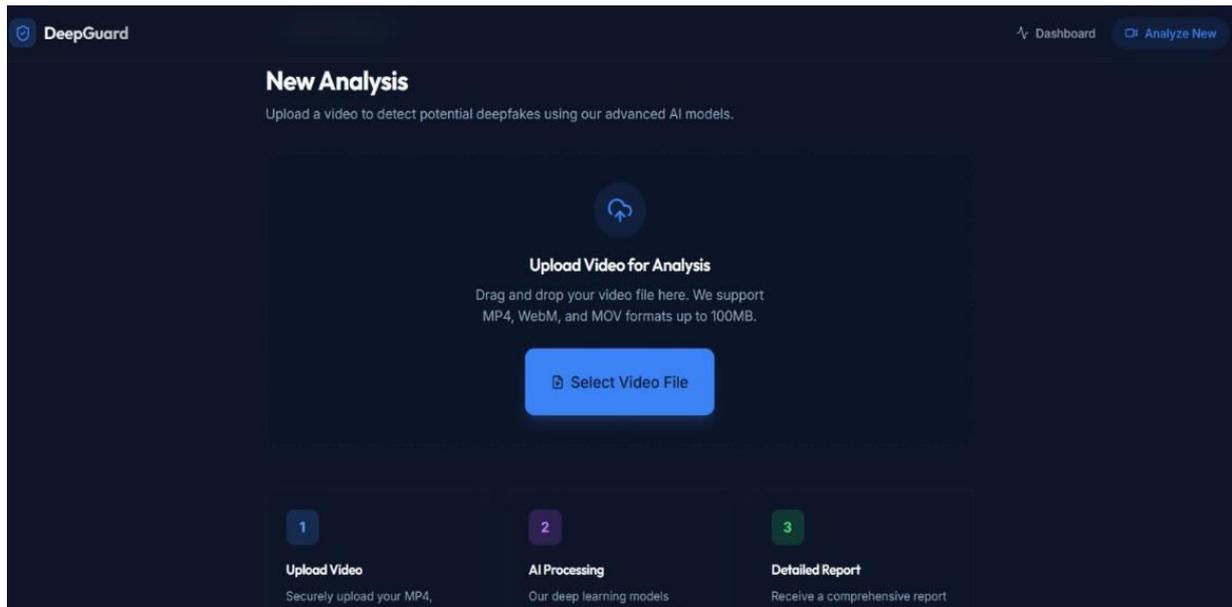


Fig.1 Dashboard

Fig. 2 shows the analysis result generated by the system after processing the uploaded video. The system identifies whether the video is authentic or manipulated and displays a confidence score. In this example, the system detects a deepfake with 93% confidence, indicating a high probability of artificial manipulation.

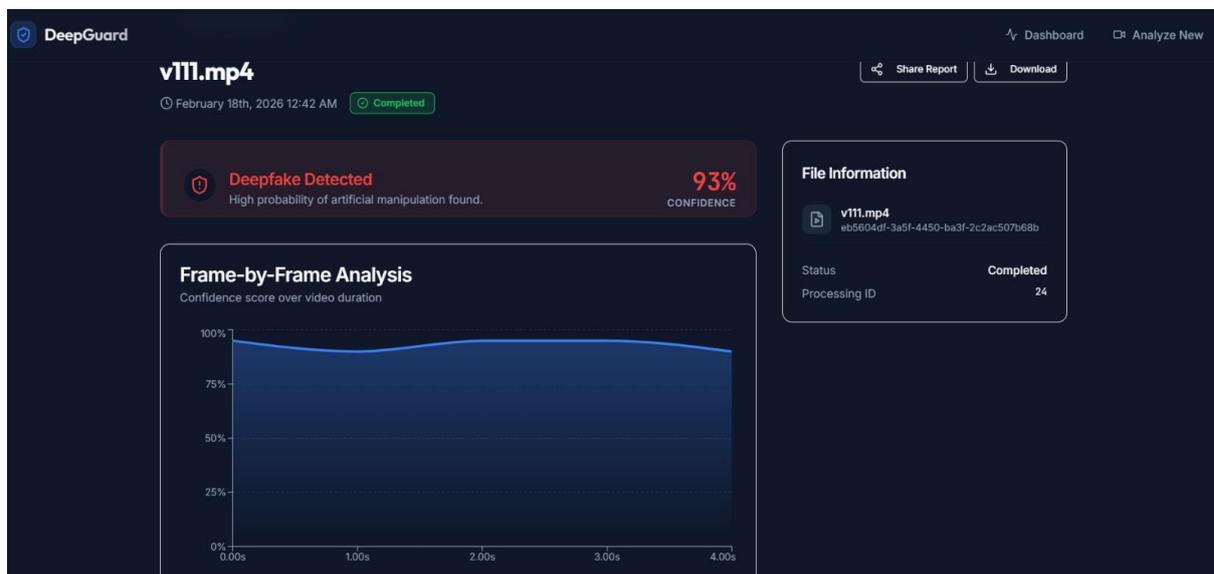


Fig.2 Analysis

Fig. 3 presents the frame-by-frame analysis graph, where the confidence scores of individual frames are plotted across the video duration. This visualization helps identify segments of the video where manipulation artifacts are more prominent.

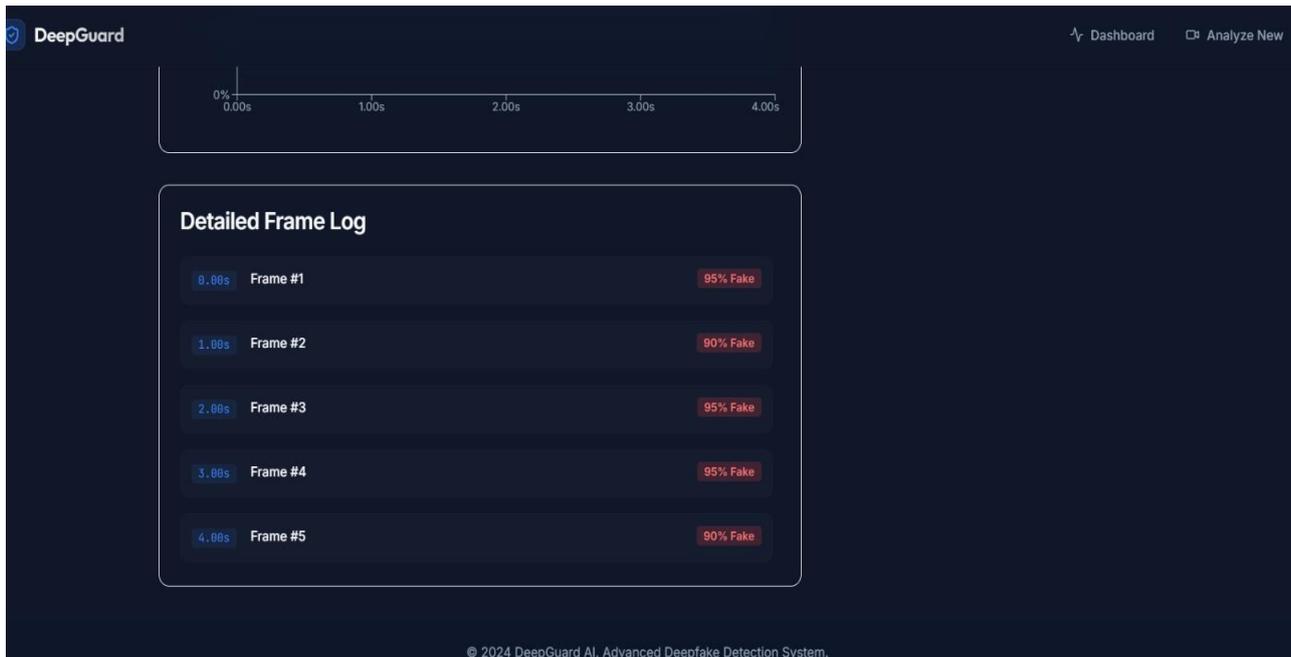


Fig.3 Frame-Frame division

Fig. 4 shows the **analysis dashboard**, which stores previously analyzed videos along with their results. Each entry displays the video name, processing status, and detection result such as authentic or deepfake. This dashboard allows users or recruiters to review multiple analyses and access detailed reports for verification.

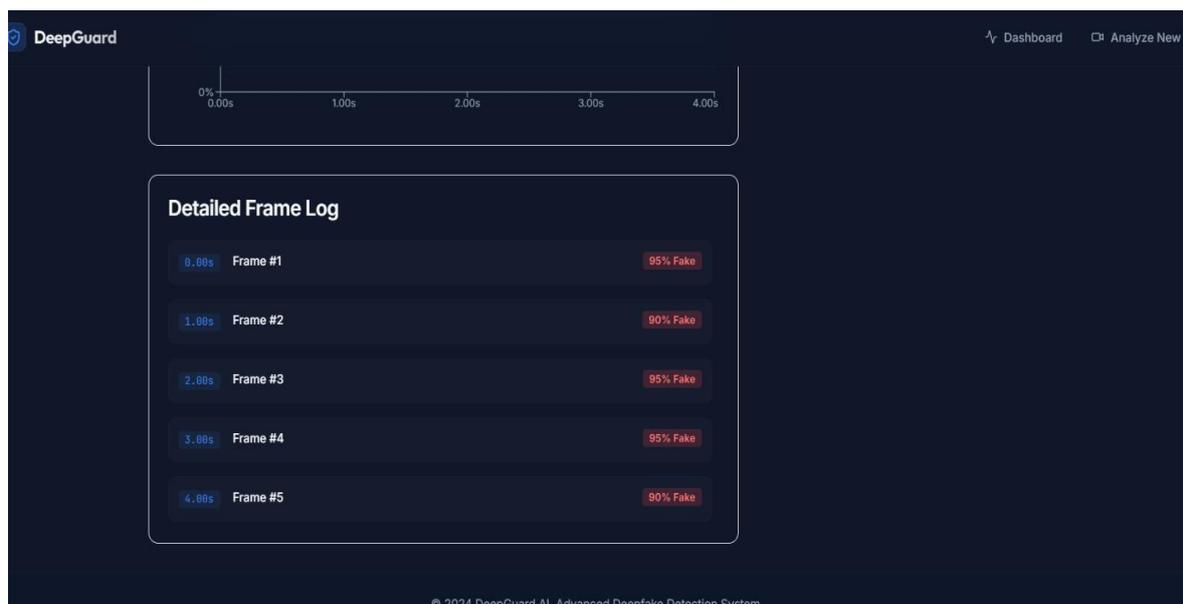


Fig.4 Detailed frame log

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503085|

These results demonstrate how the proposed system performs automated deepfake detection through video processing, frame-level analysis, and confidence scoring, ensuring improved security and authenticity in the recruitment process

VIII. CONCLUSION

In this project, we developed an automatic approach to detect text regions from images for the purpose of image inpainting. The method is designed to identify text even when the image contains a combination of text, photographs, and graphical elements. Initially, the input image is preprocessed to enhance its quality and improve the visibility of text regions. The system then analyzes the image by examining different region properties such as size, shape, contrast, and pixel intensity patterns. Based on these characteristics, the algorithm is able to distinguish text areas from non-text components in the image.

After identifying the text regions, the system marks them so that they can be removed or modified during the inpainting stage. This process helps in reconstructing the background smoothly by filling the detected text areas with surrounding pixel information.

The algorithm was tested on a variety of images containing different fonts, backgrounds, and visual elements to evaluate its effectiveness. Experimental results show that the method can successfully detect most of the text regions while maintaining good accuracy in separating text from complex backgrounds.

Although certain challenging cases such as very small text or heavily distorted fonts may affect detection performance, the overall system demonstrates reliable results for typical image scenarios. This text detection capability also supports the **Authenticity Guard** system by enabling better analysis of image content, which can help identify suspicious edits, hidden information, or manipulated visual elements that may appear in candidate-related documents or media.

IX. FUTURE SCOPE

In the future, the system can be further improved by integrating advanced deep learning techniques such as Convolutional Neural Networks (CNN) or transformer-based models for more accurate text detection in complex images. The algorithm can also be extended to support multilingual text recognition and real-time processing for videos or live streams.

Additionally, combining text detection with Optical Character Recognition (OCR) would allow the system not only to detect text regions but also to understand the extracted content. This enhancement could help identify forged information, altered documents, or misleading visual content more effectively. By expanding these capabilities, the proposed method can contribute to stronger security, improved verification, and more reliable digital recruitment and authentication systems.

Another possible direction for future work is the integration of the text detection and inpainting module with larger multimedia authentication systems. The current approach mainly focuses on detecting text regions in images; however, it can be expanded to analyze videos and document images used in digital recruitment platforms.

By combining this method with advanced deep learning models, the system could automatically detect edited captions, hidden overlays, or manipulated textual elements in candidate videos and profile images. In addition, cloud-based deployment and real-time processing can make the system scalable for large recruitment platforms where thousands of media files need to be verified quickly. Further improvements in accuracy, speed, and adaptability will allow the system to become a more powerful tool for preventing digital manipulation and ensuring trustworthy online recruitment processes.

REFERENCES

- [1] B. Dolhansky, R. Howes, B. Pflaum, N. Baram, and C. Ferrer, "The DeepFake Detection Challenge Dataset," arXiv preprint arXiv:2006.07397, 2020.
- [2] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative Adversarial Networks," in Proc. Advances in Neural Information Processing Systems (NeurIPS), pp. 2672–2680, 2014.
- [3] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "MesoNet: A Compact Facial Video Forgery Detection Network," in Proc. IEEE International Workshop on Information Forensics and Security (WIFS), 2018.
- [4] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in Proc. IEEE International Conference on Computer Vision (ICCV), pp. 1–11, 2019.
- [5] Y. Li and S. Lyu, "Exposing DeepFake Videos by Detecting Face Warping Artifacts," in Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 46–52, 2019.
- [6] T. Karras, S. Laine, and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 43, no. 12, pp. 4217–4228, 2021.
- [7] H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos," in Proc. IEEE International Conference on Biometrics (ICB), 2019.
- [8] S. Verdoliva, "Media Forensics and DeepFakes: An Overview," IEEE Journal of Selected Topics in Signal Processing, vol. 14, no. 5, pp. 910–932, 2020.
- [9] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," in Proc. International Conference on Learning Representations (ICLR), 2015.
- [10] F. Chollet, "Xception: Deep Learning with Depthwise Separable Convolutions," in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1251–1258, 2017.
- [11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in Proc. Advances in Neural Information Processing Systems (NeurIPS), pp. 1097–1105, 2012.
- [12] Y. Mirsky and W. Lee, "The Creation and Detection of Deepfakes: A Survey," ACM Computing Surveys, vol. 54, no. 1, pp. 1–41, 2021.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details