International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Real-Time Deepfake Recognition

Thivya Sri.S
UG Scholar
Vels Institute of Science,
Technology And Advanced Studies (VISTAS),
Pallavaram, Chennai-600117,
Tamil Nadu, India.

Dr. Anbarasi .C
Associate Professor,
Vels Institute of Science,
Technology And Advanced Studies (VISTAS),
Pallavaram, Chennai-600117,
Tamil Nadu, India.

https://doi.org/10.55041/ijsmt.v2i5.055

Cite this Article: Sri.S, T. (2026). Real-Time Deepfake Recognition. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.055

Abstract: Deepfake technology has grown rapidly with the advancement of artificial intelligence and deep learning techniques, enabling the creation of highly realistic manipulated images and videos that are often difficult to distinguish from genuine content. While this technology has useful applications in media and entertainment, its misuse has raised serious concerns in areas such as identity verification, digital communication, and financial transactions. The increasing spread of fake videos across social media platforms has led to misinformation, identity fraud, and cyber security risks. Traditional verification methods are often slow and unreliable, especially when dealing with large volumes of digital content. Therefore, the development of an automated and efficient real-time detection system has become essential to ensure digital trust and security. This project presents a Real-Time Deepfake Recognition System designed to detect manipulated facial content using computer vision and deep learning techniques. The system captures screen content, detects human faces using OpenCV Haar Cascade classifiers, and classifies the detected faces using a Vision Transformer (ViT) model to determine whether the face is real or fake. To improve reliability, temporal smoothing techniques and a confidence threshold are applied to produce stable and accurate results. The final output is displayed visually with bounding boxes and labels indicating the classification result. By enabling fast and reliable detection of fake facial content, the proposed system enhances digital security and supports applications such as digital banking verification, online examinations, remote interviews, and identity authentication systems.

Keywords: Deepfake Detection, Real-Time Recognition, Computer Vision, OpenCV, Haar Cascade, Vision Transformer (ViT), Artificial Intelligence, Face Detection, Digital Security, Image Classification, Temporal Smoothing, Cyber Security

1.INTRODUCTION

Deepfake technology refers to the use of artificial intelligence and deep learning techniques to create highly realistic synthetic images and videos that appear authentic to human viewers. In recent years, the rapid growth of digital media and online communication platforms has significantly

increased the usage of visual content in daily life. While deepfake technology has beneficial applications in entertainment, education, and film production, it also presents serious risks when used for malicious purposes. Manipulated videos and images can be used to spread misinformation, damage reputations, and create security threats, making it increasingly difficult to trust digital content available on the internet.

With the growing dependency on digital platforms for communication, banking, education, and identity verification, ensuring the authenticity of visual content has become a major challenge. Traditional methods of detecting fake media often rely on manual inspection or basic image analysis, which may not be effective against advanced deepfake techniques. These methods are time-consuming and may fail to detect subtle differences between real and manipulated faces. As deepfake technology continues to evolve, there is an urgent need for intelligent and automated systems that can detect manipulated content quickly and accurately in real-time environments.

This project focuses on the development of a Real-Time Deepfake Recognition System that uses computer vision and deep learning techniques to identify manipulated facial content. The system continuously captures screen data, detects human faces, and analyzes them using advanced machine learning models to determine whether the detected face is real or fake. By providing instant and reliable results, the proposed system helps improve trust in digital platforms and supports secure verification processes. The implementation of this system contributes to strengthening cyber security and reducing the risks associated with the misuse of synthetic media in modern digital environments.

Types of Deepfake Content

The deepfake content can be categorized into different types based on how the facial data is manipulated. Understanding these types helps in developing effective detection systems.

- Face Swap Deepfakes

Face swap deepfakes replace one person's face with another person's face in images or videos. This type is commonly used to create misleading or fake visual content.

- Face Morphing Deepfakes

Face morphing combines facial features of two individuals to create a synthetic face. It is often used to bypass identity verification systems.

- Facial Expression Manipulation

This type modifies facial expressions or lip movements without changing identity. It is mainly used to create fake speeches or altered video content.

II. LITEATURE REVIEW

Recent studies show significant advancements in the field of deepfake detection to improve digital security and trust in online platforms. Rössler et al. (2019) introduced the FaceForensics++ dataset, which became one of the most widely used datasets for training deepfake detection models. This dataset provided a foundation for developing reliable machine learning techniques capable of identifying manipulated facial images and videos with improved accuracy.

Afchar et al. (2018) proposed the MesoNet model, a deep learning-based architecture designed to detect forged facial videos by identifying visual artifacts and inconsistencies. Similarly, Li et al. (2020) developed advanced detection techniques focusing on identifying hidden manipulation traces in synthetic images. These methods improved the accuracy of deepfake detection systems, especially for detecting low-quality manipulated content.

With the advancement of artificial intelligence, transformer-based models have gained popularity in recent years. Dosovitskiy et al. (2021) introduced Vision Transformer (ViT) architecture, which demonstrated high performance in image classification tasks. Researchers have also explored combining

spatial and temporal analysis methods to improve detection performance in real-time environments.

Despite these advancements, challenges still exist in detecting highly realistic deepfakes efficiently in real-time systems. Many detection methods require large computational resources and may not perform well under real-time conditions. Therefore, the current project focuses on developing an optimized real-time deepfake recognition system that balances accuracy and performance using computer vision and transformer-based techniques.

III. PROBLEM DEFINITION

Deepfake technology presents several major challenges in modern digital environments. One of the primary concerns is the misuse of manipulated videos and images to spread misinformation and fake news across social media platforms. Such content can mislead the public, damage reputations, and create confusion in sensitive situations. The rapid sharing of deepfake content increases the difficulty of identifying genuine information from manipulated media.

Another significant issue is identity fraud and digital impersonation. Deepfake technology allows attackers to create fake identities by modifying facial images or videos, which can be used to bypass verification systems in banking, online examinations, and remote interviews. This creates security risks and financial losses for individuals and organizations.

Additionally, traditional verification methods are often time-consuming and ineffective when dealing with large volumes of digital data. Manual inspection of videos is not practical in real-time scenarios, especially when deepfake technology becomes more advanced and realistic. The lack of reliable automated detection systems increases the risk of cyber threats and reduces trust in digital communication platforms.

Therefore, the problem addressed in this project is the need to develop an automated real-time deepfake recognition system capable of accurately identifying manipulated facial content. The system aims to enhance digital security, reduce identity misuse, and improve the reliability of online authentication systems.

IV. PROPOSED SYSTEM

The proposed system of this project is a Real-Time Deepfake Recognition System designed to detect manipulated facial content using computer vision and deep learning techniques. The system operates as a continuous pipeline that captures screen data, processes facial features, and classifies images into real or fake categories. The system consists of several major steps as described below.

1. Screen Capture**:** The system captures a selected region of the desktop screen continuously using the mss library. This allows real-time monitoring of video content such as video calls, verification screens, and online interactions.
2. Face Detection: The captured frames are processed using OpenCV Haar Cascade classifiers to detect human faces. Only the detected face regions are selected for further analysis, reducing unnecessary computations.
3. Face Pre-processing**:** The detected facial region is cropped and converted into RGB format. The image is resized according to the input requirements of the deep learning model to ensure consistent processing.
4. Deep Learning Classification**:** The processed facial images are passed into a Vision Transformer (ViT) model, which analyses facial features and generates probability scores indicating whether the face is real or fake.
5. Decision and Output Display: To improve accuracy, temporal smoothing techniques are applied by averaging recent predictions. A predefined confidence threshold is used to determine the final classification. The output is displayed in real time using bounding boxes labelled REAL or FAKE.

The proposed system improves detection efficiency, reduces manual verification efforts, and ensures reliable identification of manipulated content in real-time environments.

Screen Capture using MSS Library:

The screen capture module is responsible for continuously capturing a selected region of the desktop screen in real time. The system uses the mss library, which allows fast and efficient screen capturing with minimal delay. Each captured frame is processed instantly, enabling the system to monitor live video content such as video calls, online examinations, and verification screens. This real-time capturing process ensures continuous monitoring of facial data for deepfake detection.

OpenCV Haar Cascade for Face Detection:

The OpenCV Haar Cascade classifier is used to detect human faces from the captured screen frames. This method identifies facial regions by analyzing patterns of light and dark areas in an image. Once a face is detected, the system draws a bounding box around the facial region and extracts it for further processing. Haar Cascade detection is fast and reliable, making it suitable for real-time applications where quick identification of facial features is required.

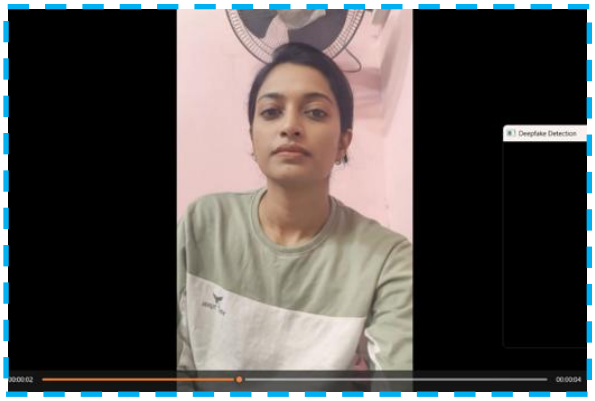
Vision Transformer (ViT) for Deepfake Classification:

The Vision Transformer (ViT) is a deep learning model used to classify facial images as real or fake. It processes the input face image by dividing it into smaller patches and analyzing relationships between these patches using attention mechanisms. The model generates probability scores indicating whether the detected face is genuine or manipulated. Vision Transformer models are highly effective for image classification tasks and provide improved accuracy in identifying deepfake content.

Temporal Smoothing and Threshold-Based Decision:

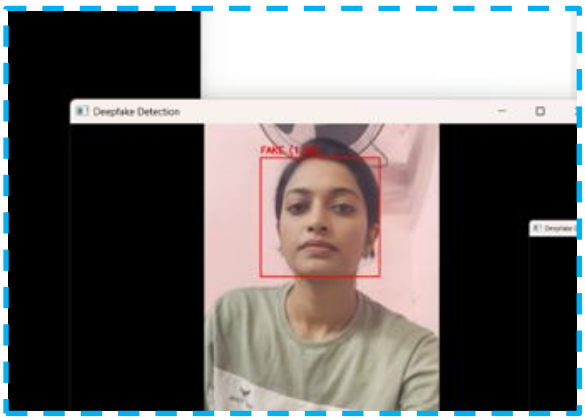
Temporal smoothing is applied to improve the stability of detection results. The system stores recent prediction values and calculates their average to reduce sudden changes in classification output. A predefined confidence threshold is then used to determine whether the detected face is real or fake. This process helps produce consistent and reliable results during real-time operation and reduces false predictions.

Fig 1 Real-Time Deepfake Detection Interface



This figure shows the real-time working interface of the proposed system. The screen region is captured continuously, and detected faces are highlighted using bounding boxes. The system classifies each detected face as REAL or FAKE based on the trained Vision Transformer model.

Fig 2 Face Detection and Prediction Output



This figure illustrates the detection of human faces using the Haar Cascade classifier. After detecting the face region, the cropped image is

passed to the classification model. The prediction result is displayed with color-coded labels for easy interpretation.

Fig 3 Final Prediction Result

This figure represents the final output generated by the system after analyzing the input frame. The classification result indicates whether the detected face is real or manipulated. The probability score improves reliability and helps in decision-making.

V. CONCLUSION

In conclusion, the development of the Real-Time Deepfake Recognition System represents a significant advancement in improving digital security and trust in modern communication systems. The proposed system effectively integrates computer vision and deep learning techniques to detect manipulated facial content in real time. By using OpenCV Haar Cascade for face detection and Vision Transformer models for classification, the system demonstrates reliable performance in identifying real and fake facial data.

The implementation of temporal smoothing and threshold-based decision-making enhances the stability and accuracy of predictions. The real-time visual output allows users to quickly identify manipulated content, reducing the chances of identity misuse and misinformation. The system also supports multiple applications, including online verification processes, remote interviews, and digital banking authentication.

Overall, the proposed project provides an efficient and scalable solution to address the growing challenges associated with deepfake technology. By improving detection accuracy and reducing reliance on manual verification, the system contributes to building secure digital environments and strengthening trust in online communication platforms. With further improvements and real-world implementation, this system has the potential to play an important role in future cybersecurity and digital authentication systems.

REFERENCES

1. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 1-11.

2. Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., & Canton Ferrer, C. (2020). The DeepFake Detection Challenge Dataset. arXiv:2006.07397.

3. Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I. (2018). MesoNet: A compact facial video forgery detection network. IEEE International Workshop on Information Forensics and Security (WIFS), 1-7.

4. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Uszkoreit, J., & Houlsby, N. (2021). An image is worth 16x16 words: Transformers for image recognition at scale. International Conference on Learning Representations.

5. Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 1251-1258.

6. Li, L., Bao, J., Yang, H., Chen, D., & Wen, F. (2020). Face X-ray for more general face forgery detection. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 5001-5010.

7. Zhang, X., Karaman, S., & Chang, S. F. (2019). Detecting and simulating artifacts in GAN fake images. IEEE International Workshop on Information Forensics and Security.

8. Korshunov, P., & Marcel, S. (2018). Deepfakes: A new threat to face recognition? Assessment and detection. arXiv:1812.08685.

9. Nguyen, H. H., Yamagishi, J., & Echizen, I. (2019). Capsule-forensics: Using capsule networks to detect forged images and videos. IEEE International Conference on Acoustics, Speech and Signal Processing.

10. Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.