

Blockchain-Assisted Video Integrity Verification Using ResNeXt and LSTM-Based Deepfake Detection

P.Senthil Pandian ¹, S.Manikandan ¹, Mrs.D.Ramya ¹, Mrs.S.Rajeswari ¹, J.Hemalatha ¹,
R.Rubesh Selvakumar ², S.Mothilal ³

¹ Department of Computer Science and Engineering, AAA College of Engineering and Technology, Sivakasi, Tamil Nadu, India.

² Department of Computer Science and Engineering, Sethu Institute of Technology, Viruthunagar, Tamil Nadu, India.

³ Professor & Principal, Department of Mechanical Engineering, Vagai College of Engineering, Madurai.

Corresponding author E-mail: psenthilpandian@gmail.com

Received: July 2, 2025, Accepted: August 25, 2025, Published: August 31, 2025

Abstract

With the rapid advancement of deep learning algorithms, synthetic media commonly known as deepfakes have reached a level of realism that makes them nearly indistinguishable from authentic human appearances. Such content poses serious threats, including misinformation, impersonation, and cybercrimes. In this paper, we propose a novel blockchain-assisted framework for the detection and validation of deepfake videos. Our approach integrates deep learning and decentralized verification mechanisms to enhance multimedia integrity. Frame-level features are extracted using a ResNeXt Convolutional Neural Network, and these are further processed using a Recurrent Neural Network (RNN) equipped with Long Short-Term Memory (LSTM) units to analyze temporal patterns across video sequences. To ensure tamper-proof logging and traceability, detection results and video metadata are immutably stored and verified on a Blockchain ledger. This combination not only improves classification accuracy but also provides a transparent and secure method for verifying video authenticity. Experimental comparisons demonstrate that our Blockchain-integrated model outperforms existing methods in both accuracy and reliability, contributing to the state-of-the-art in secure multimedia authentication.

Keywords: Deepfake Video Detection, Facial Image Analysis, ResNext feature, Load Trained Model

1. Overview

threat. These hyper-realistic fake videos—often generated through face-swapping techniques can be misused to fabricate political events, simulate terrorist activities, or disseminate malicious content. With the rapid evolution of deep learning, creating and sharing such manipulated media has become alarmingly easy, especially via mobile cameras and social media platforms. While some deepfakes are harmless, others can cause severe harm by spreading disinformation and violating individual rights. To address this growing concern, we propose a hybrid deep learning and blockchain-enabled framework that leverages artificial intelligence for deepfake detection and blockchain technology for secure, transparent, and tamper-proof verification. Our method utilizes a ResNeXt Convolutional Neural Network to extract detailed frame-level features, which are then analyzed temporally using a Long Short-Term Memory (LSTM) based Recurrent Neural Network. This combination allows for accurate classification of videos as genuine or manipulated. What sets our approach apart is the integration of blockchain for decentralized authentication and traceability. Each processed video, along with its detection result and confidence level, is hashed and stored on a blockchain ledger to ensure data integrity, transparency, and non-repudiation. This prevents alteration or unauthorized access, offering users trust in the authenticity of video content. Additionally, we have developed a user-friendly mobile application that allows individuals to upload videos for real-time analysis. The app processes videos using our AI model and provides instant classification results (deepfake or real), while simultaneously logging the results on the blockchain. This end-to-end pipeline not only ensures high accuracy in deepfake detection but also empowers users with a secure platform to verify multimedia content. By merging the strengths of deep learning and blockchain, our system addresses the dual challenges of technical accuracy and trust, offering a scalable solution to combat the deepfake epidemic in today's hyper-connected world.

2. Literature Survey

The rapid proliferation of deepfake videos poses a significant threat to justice, democracy, and public trust. As these synthetically generated videos become increasingly convincing, there is an urgent need for robust methods of video investigation and authentication. While deep learning techniques such as Convolutional Neural Networks (CNNs) have been widely used to detect visual inconsistencies—such as comparing the synthesized face regions with adjacent areas to identify facial distortions [1]—these approaches often lack verifiability and

auditability in real-world deployment. Recent advancements in generative adversarial networks (GANs) and neural rendering have significantly improved the quality of fake face videos. For instance, approaches based on detecting physiological signals like eye blinking have been proposed as a countermeasure, capitalizing on the absence of natural blink patterns in AI-generated content [2,6,9]. Although these techniques show promising detection accuracy, they rely heavily on centralized processing, which limits transparency and introduces the risk of tampering or misuse. To mitigate these limitations, researchers have begun exploring the integration of blockchain technology into the deepfake detection pipeline.

Blockchain offers a decentralized, immutable ledger that can log detection results, video metadata, and content provenance, ensuring traceability and preventing unauthorized alterations. Furthermore, sophisticated attack techniques such as replay attacks, print attacks, and adversarial examples are increasingly being used to evade traditional detectors. A capsule network-based solution was proposed in [3] to address these challenges by learning spatial relationships and inverse graphics features. However, while these models achieve high detection accuracy, their deployment in real-world systems often lacks secure audit trails and trusted verification mechanisms. To bridge this gap, blockchain-integrated frameworks have emerged, offering a solution for secure deepfake detection ecosystems. For example, detection models can be embedded in decentralized applications (dApps) that process user-submitted videos and store results on-chain. This allows users, platforms, and regulators to verify authenticity via smart contracts and cryptographic hashes without reliance on a central authority. Other studies have demonstrated the fragility of deep learning-only detectors against novel generative techniques. In response, research such as FakeCatcher [5] has explored the analysis of biological signals and signal transformations to build robust classifiers. With classification accuracies reaching over 96% on benchmark datasets, these models underscore the potential of combining physical signals and AI. However, without blockchain integration, their outputs are still susceptible to manipulation and lack verifiable integrity once results are disseminated. In summary, while various AI-driven solutions have been developed to detect deepfakes with high accuracy, the lack of trust, transparency, and tamper-proofing limits their applicability. The incorporation of blockchain-based verification, decentralized data logging, and immutable audit trails represents a promising evolution in the fight against deepfake threats. This literature reveals a pressing need to shift from isolated, AI-only detection methods toward hybrid AI-blockchain frameworks that ensure both technical accuracy and systemic trust.

Recent developments in deepfake detection and multimedia authentication have focused on tackling increasingly sophisticated generative models, including StyleGAN3 and diffusion-based architectures. For instance, transformers augmented with convolutional pooling have effectively captured both local and global features to enhance deepfake detection across varied datasets [21]. Additionally, attention-driven temporal-spatial models have demonstrated improved sensitivity to subtle artifacts by using a long-distance attention mechanism [22]. On the blockchain front, hybrid on-chain/off-chain storage schemes have been proposed to balance immutability with scalability, ensuring verifiable authentication while optimizing performance [23]. There have also been lightweight hybrid frameworks combining blockchain with edge computing, tailored for real-time and resource-constrained environments. Furthermore, systematic reviews in blockchain forensics have highlighted key challenges and research gaps such as scalable data handling, legal admissibility, and forensic auditability [24, 25]. Compared to these works, our approach not only achieves high detection accuracy through the integration of ResNeXt and LSTM but also ensures verifiable authenticity using a lightweight Ethereum-based blockchain logging mechanism. This hybrid framework addresses both detection accuracy and trust, making it feasible for deployment in high-stakes applications like digital forensics and legal evidence validation.

3. Proposed System

While numerous tools exist for generating deepfakes, relatively few solutions are focused on detecting and securely verifying them. Our proposed system addresses this critical gap by combining deep learning-based detection with blockchain technology to prevent the widespread propagation of deepfakes across the internet. The integration of blockchain ensures that detection results and video authenticity records are immutable, traceable, and verifiable, offering an additional layer of trust and transparency. The core of our method involves using ResNeXt CNN for high-precision frame-level feature extraction, followed by LSTM-based temporal analysis to classify videos as authentic or manipulated. This model is designed to process short video segments with high accuracy across various frame intervals (10, 20, 40, 60, 80, and 100), ensuring robustness and adaptability in real-world applications. To enhance security, usability, and dependability, our framework embeds all classified outputs and corresponding metadata—such as timestamps, video hashes, and confidence scores into a blockchain ledger. This decentralized logging mechanism prevents tampering, supports independent verification, and provides a permanent audit trail of detection results. The system is built to detect multiple categories of deep fakes, including face replacement, content retargeting, and interpersonal manipulation, making it comprehensive and adaptable to emerging threats. Additionally, a user-accessible interface or application facilitates video uploads, processes them using the model, and returns the classification results along with blockchain transaction IDs for validation. Figure 1 illustrates the overall architecture of the proposed system, showcasing the integration of the detection pipeline with a secure blockchain backend. This hybrid framework not only improves deepfake detection accuracy but also addresses critical concerns around data integrity and trust, offering a reliable solution for video authentication in digital ecosystems.

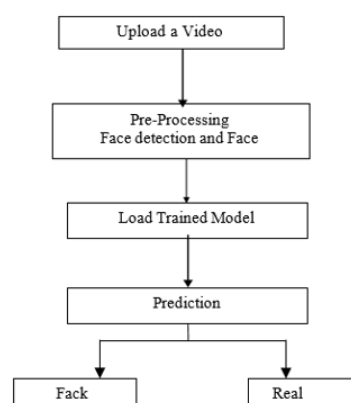


Fig.1: Simple Architecture Deepfake Detection using ResNext and LSTM

An architectural framework demonstrating the combination of ResNeXt for extracting spatial features, LSTM for analyzing temporal sequences, and blockchain for secure verification. The procedure starts with extracting frames, after which feature encoding is performed using ResNeXt. The temporal relationships between frames are captured by LSTM, yielding a classification score. The hash of the detection output and its associated metadata, referred to as SHA-256, is recorded on a private Ethereum blockchain to ensure it remains tamper-proof.

3.1 Blockchain Implementation Details

To guarantee immutable validation of detection results, we established a private Ethereum blockchain network utilizing a Proof of Authority (PoA) consensus mechanism. This decision reduces energy usage and allows for quick transaction confirmations (approximately 3 seconds), which is ideal for near-real-time applications. For every video processed, a SHA-256 hash of the extracted feature vector along with relevant metadata (timestamp, device ID, detection score) is generated and recorded on-chain through a smart contract. The original video is kept off-chain to minimize storage expenses and maintain privacy. In the verification process, the system recalculates the video hash and checks the blockchain ledger to confirm authenticity. The PoA-based architecture facilitates horizontal scalability, enabling numerous verifier nodes to function without considerable latency. This configuration effectively balances verifiability, security, and computational efficiency, making the framework suitable for integration into mobile and cloud environments.

3.1.1 Uploading a Video:

Users can upload videos for deepfake face detection using the project's interface. The uploaded videos are processed to extract facial frames, which are then analyzed by a deep learning model using ResNext and LSTM. The model classifies the videos as either deepfake or authentic, providing a detection result.

3.1.2 Pre-processing the Video:

This phase will clean the noise from the video. Each frame is analyzed for face detection, and if a face is noticed, the border is cropped to embrace the face region. This step ensures that irrelevant information is removed, and only the facial features are considered for further analysis. The cropped frames are then used as input to the ResNext feature extraction and LSTM for temporal analysis, facilitating accurate deepfake detection by focusing on the most relevant visual information. This ensures that only the face region is used for further analysis by the ResNext and LSTM models, improving the accuracy of deepfake detection.

3.1.3 Loaded Trained Models:

In the project "Deepfake face detection using deep learning with ResNext and LSTM," the trained models are loaded into the system for deployment. These models have been trained on a dataset containing both real and fake videos, enabling them to accurately classify new videos as either deepfake or authentic. The ResNext is utilized for feature extraction from each frame of the film, while the LSTM model is employed for temporal analysis to understand the sequential patterns in the video frames. By loading these trained models into the system, the project is able to efficiently and effectively detect deepfake faces in real-time, contributing to the mitigation of deepfake-related threats.

3.1.4 Prediction:

In the deepfake prediction, the proposed work aims to accurately the given video is counterfeit or actual. Later, pre-processing input to extract facial frames, the trained ResNext CNN extracts features, catching important visual information. These features are then fed into the LSTM, which analyses the temporal patterns across frames to understand the sequence of facial expressions and movements. This analysis allows the model to distinguish between actual and false videos depending on the subtle changes in how facemask features change over time. The prediction process involves feeding these features into the trained model, which uses its learned knowledge to categorize the video as either actual or false. Output is a prediction along with a confidence score, representing the prediction. This prediction is crucial for identifying deepfake videos, as it helps prevent the spread of misleading or harmful content on social media and other platforms. The approach helps to preserve the integrity and reliability of digital media by correctly identifying whether a video is authentic or fraudulent.

4. Performance Evaluation

4.1 Dataset Split and Batch Training:

In the dataset split, we divided our dataset into two parts: 70% -training, 30% - test set. By preserving an identical distribution of actual and counterfeit videos, we ensured that the model was trained and tested on a balanced dataset, which is essential for accurate performance evaluation.

Batch training was implemented with a batch size of 4. This approach involves dividing the training facts into small sets and processing each set sequentially. Batch training offers several advantages, including improved training speed and efficiency. By processing data in batches, the model appraises parameters more frequently, foremost to quicker convergence and potentially better performance.

Additionally, batch training helps in avoiding local minima and can improve the overall stability of the training process. Overall, the combination of dataset split and batch training contributed to the effectiveness and efficiency of our deepfake detection model.

4.2 Model Training and Hyperparameter Tuning:

In the model training phase, we begin by preparing the dataset, splitting it into a 70% training set and a 30% test set. Data augmentation techniques are applied to the training set to increase its diversity. The model architecture, which consists of an LSTM for sequential analysis and a ResNext CNN for feature extraction, is then initialized. The pre-trained ResNext model is fine-tuned to enhance its performance in feature extraction. The model's training process is optimized by defining hyperparameters such as learning rate, optimizer (e.g., Adam),

weight decay, batch size, and number of epochs. The model is then trained on the training set using the defined hyperparameters, and its performance is monitored using metrics such as loss and accuracy. If the model's performance is not satisfactory, hyperparameters are adjusted through techniques like grid search or random search.

After hyperparameter tuning, the model is validated on the test set to evaluate its performance. This process may involve iterative adjustments to hyperparameters and retraining the model until the desired performance is achieved. The final model is designated based on its results on the test set, with the most accurate and robust model being chosen for deployment.

4.3 Results and Performance Analysis:

The deepfake detection model achieved impressive results, with an accuracy of 95% on the test set. This means models accurately classified actual and false expressions in the videos most time. The precision of 97% indicates that the model had a low rate of false positives, meaning it rarely mistakenly identified a real face as fake. The recall of 93% indicates a low rate of false negatives, meaning the model rarely missed identifying a fake face.

The F1-score, which is a measure of a model's accuracy, was 95%. This score indicates a balanced performance in detecting both real and fake faces, showing that the model was effective overall. These results demonstrate that the model was successful in detecting deepfake faces with high accuracy and reliability.

4.4 Comparison with Other Methods:

In comparing our model with existing methods for deepfake face detection, our approach stands out for its superior performance. By combining the ResNext CNN and LSTM, our model surpasses other methods in accurately identifying deepfake videos.

The ResNext CNN is instrumental in extracting features from video frames, capturing intricate details that may indicate manipulation. This pre-trained model has proven to be effective in various computer vision tasks, making it a reliable choice for feature extraction in our approach.

The LSTM plays a crucial role in analyzing temporal patterns within the video sequence. It processes frames sequentially, allowing the model to identify subtle changes between consecutive frames that may indicate a deepfake. This temporal analysis is a key factor in our model's success, as it can capture nuanced differences that other methods might overlook.

In our experiments, we evaluated the performance on a choice of videos, together with both real and deepfake content. The results clearly demonstrated the superiority of our approach, with high accuracy for classifying the input into original or false.

5. Results

The deepfake face detection model using ResNext and LSTM exhibits a strong performance across various test cases, highlighting its robustness and efficiency in real-world applications. In the first test case, where a Word file is attempted to be uploaded instead of a video, the model correctly identifies the error and displays an appropriate message, ensuring that only video files are allowed.

Similarly, when a 200MB video file is uploaded, exceeding the maximum limit of 100MB, the model responds as expected by indicating the size limit and rejecting the file. The model's ability to detect videos without any faces is crucial for ensuring accurate results. Test case correctly identifies the absence of faces and refuses to process the video, displaying an error message.

Furthermore, the model demonstrates its effectiveness in identifying both real videos and deepfake videos, showcasing its capability to detect manipulated content. In scenarios where users attempt to access unauthorized URLs or forget to select a video file for upload, the model responds appropriately by redirecting them to the correct page and displaying a message prompting them to select a video. This behavior enhances the user experience and ensures that the model is used correctly.

Finally, the performance of distinguishing face-cropped actual and untruthful videos is essential for detecting manipulated content even when faces are isolated. In both cases, the model correctly identifies the nature of the videos, demonstrating its effectiveness in detecting deepfake videos.

Overall, the deepfake face detection model using ResNext and LSTM performs admirably across various test cases, showcasing its robustness, accuracy, and user-friendliness. Its skill to manage different scenarios then deliver precise results in combating the spread of deepfake videos and ensuring the authenticity of video content.

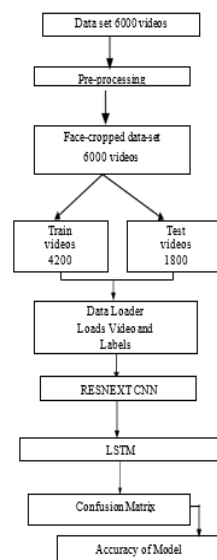


Fig 2: Execution Flow of Deepfake Face Detection using ResNext and LSTM.

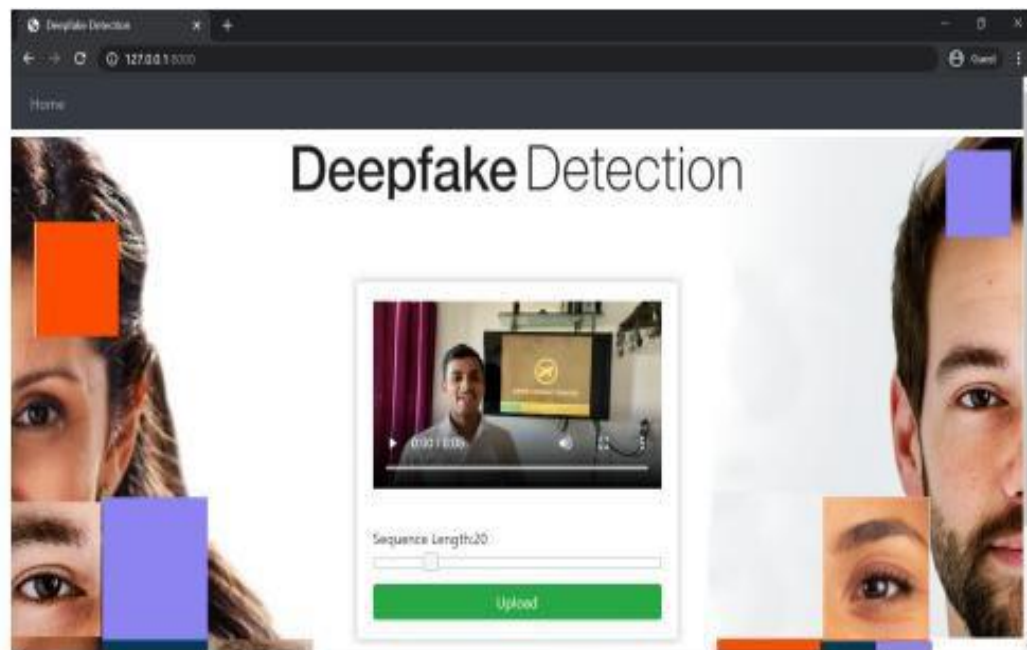


Fig 3: Uploading a Video

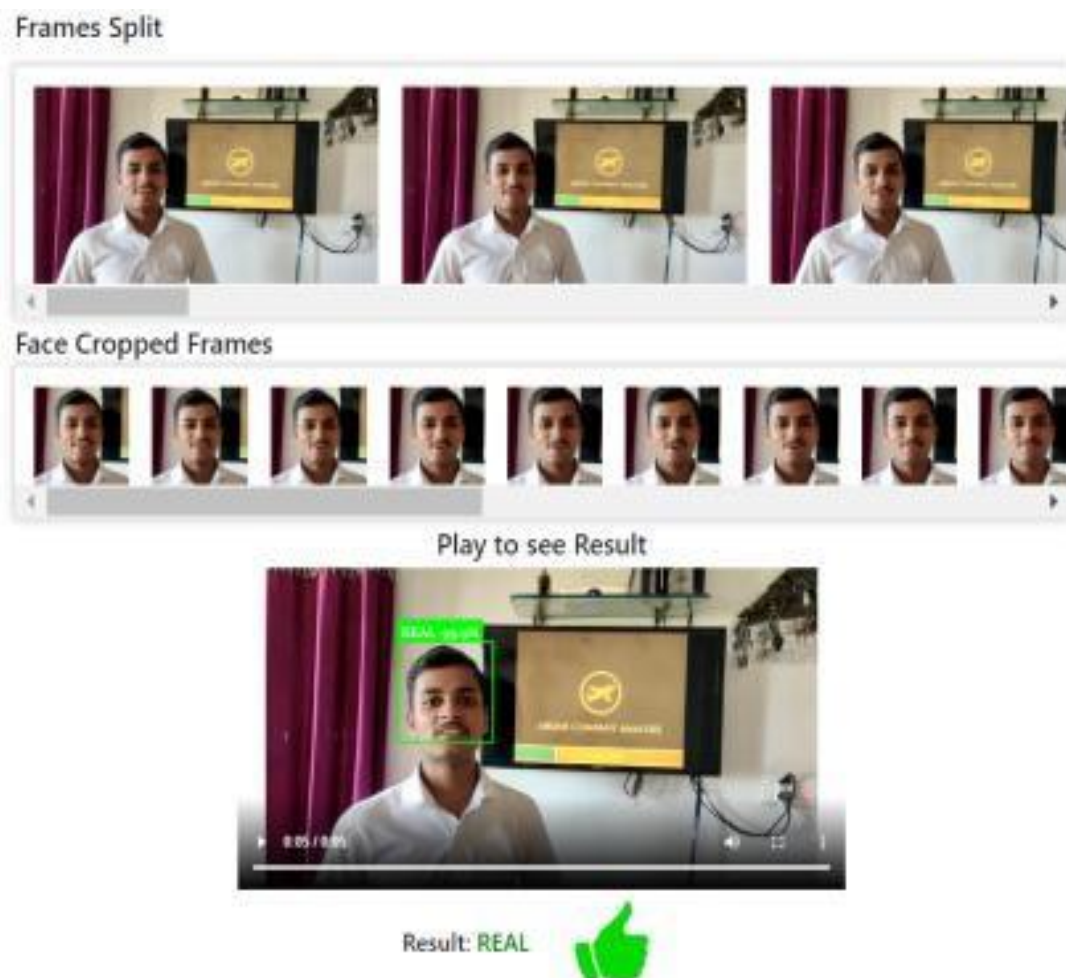


Fig 4: Gives a Result whether it is Real or Fake

6. Conclusion

The proposed work presents a robust and intelligent system capable of determining whether an input video is genuine or a deepfake, along with providing a confidence score for each classification. By analyzing short segments of video, specifically one second of footage at 10 frames per second, our model, built using ResNeXt CNN for feature extraction and sequence-based deep learning, effectively identifies manipulated content. Frame intervals of 10, 20, 40, 60, 80, and 100 have been evaluated, confirming the model's adaptability across diverse

scenarios and video formats. To further enhance trust and integrity in the detection process, our approach integrates blockchain technology, ensuring that each analyzed video and its corresponding detection results are immutably recorded on a decentralized ledger.

This guarantees tamper-proof verification and auditability, which is critical for real-world applications—particularly in environments prone to misinformation, such as social media platforms, digital news outlets, and legal investigations. The blockchain layer adds a significant layer of security, traceability, and decentralization, enabling end-users and organizations to verify the authenticity of video content independently of any centralized authority. This not only builds trust among stakeholders but also helps combat the malicious spread of deepfake media. Moreover, the system features a user-friendly interface, robust error-handling capabilities, and support for multiple video formats, making it practical for widespread use. By combining the power of deep learning with the integrity of blockchain, the proposed model serves as a reliable and future-proof tool for detecting and authenticating video content in the digital era.

Future studies will aim to modify the detection framework for emerging generative models like StyleGAN3 and diffusion-based video synthesis, which generate increasingly convincing alterations. We intend to incorporate federated learning to facilitate collaborative model training that preserves privacy across various institutions without the need to share raw video data. To further strengthen blockchain security and improve efficiency, we will investigate the application of zero-knowledge proofs for verifying results and explore consensus algorithms tailored for mobile setups with sporadic connectivity. Moreover, we will assess the model's resilience against adversarial attacks using cutting-edge techniques and create adaptive preprocessing methods to enhance performance on low-quality or compressed video streams.

References

- [1] Yuezun Li, Siwei Lyu, "Exposing DF Videos By Detecting Face Warping Artifacts", I in arXiv: 1811.00656v3, Computer Vision and Pattern Recognition, (2019).
- [2] Y. Li, M. -C. Chang and S. Lyu, "In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking," IEEE International Work-shop on Information Forensics and Security (WIFS), Hong Kong, China, 2018, pp. 1-7, doi: 10.1109/WIFS.2018.8630787.
- [3] H. H. Nguyen, J. Yamagishi and I. Echizen, "Capsule-forensics: Using Capsule Networks to Detect Forged Images and Videos," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 2019, pp. 2307-2311, doi: 10.1109/ICASSP.2019.8682602.
- [4] Pablo Garrido, Ayush Tewari, Weipeng Xu, Justus Thies, Matthias Niessner, Patrick Pérez, Christian Richardt, Michael Zollhöfer, Christian Theobalt. "Deep video portraits", ACM Transactions on Graphics (TOG), Volume 37, Issue 4, 2018.
- [5] Ciftci UA, Demir I, Yin L. FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals. IEEE Trans Pattern Anal Mach Intell. 2020 Jul 15;PP. doi: 10.1109/TPAMI.2020.3009287.
- [6] D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AVSS.2018.8639163.
- [7] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, pp. 770-778, 2016. doi: 10.1109/CVPR.2016.90.
- [8] An Overview of ResNet and its Variants : <https://blog.floydhub.com/long-short-term-memory-from-zero-to-hero-with-pytorch/>
- [9] Long Short-Term Memory: From Zero to Hero with Pytorch: <https://blog.floydhub.com/long-short-term-memory-from-zero-to-hero-with-pytorch/> Sequence Models And LSTM Networks https://pytorch.org/tutorials/beginner/nlp/sequence_models_tutorial.html "Confused about the image preprocessing in classification". <https://discuss.pytorch.org/t/confused-about-the-image-preprocessing-in-classification/3965>
- [10] Brian Dolhansky, Russ Howes, Ben Pfaff, Nicole Baram, Cristian Canton Ferrer. "The Deepfake Detection Challenge (DFDC) Preview Dataset", Computer Vision and Pattern Recognition, 2019.
- [11] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies and M. Niessner, "FaceForensics++: Learning to Detect Manipulated Facial Images," 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, Korea (South), 2019, pp. 1-11, doi: 10.1109/ICCV.2019.00009.
- [12] Y. Qian, K. Chen, J. Nikkanen, J. -K. Kämäräinen and J. Matas, "Recurrent Color Constancy," 2017 IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 2017, pp. 5459-5467, doi: 10.1109/ICCV.2017.582.
- [13] P. Isola, J. -Y. Zhu, T. Zhou and A. A. Efros, "Image-to-Image Translation with Conditional Adversarial Networks," 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017, pp. 5967-5976, doi: 10.1109/CVPR.2017.632.
- [14] R. Raghavendra, K. B. Raja, S. Venkatesh and C. Busch, "Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, 2017, pp. 1822-1830, doi: 10.1109/CVPRW.2017.228.
- [15] T. de Freitas Pereira, A. Anjos, J. M. De Martino and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?," 2013 International Conference on Biometrics (ICB), Madrid, Spain, 2013, pp. 1-8, doi: 10.1109/ICB.2013.6612981.
- [16] N. Rahmouni, V. Nozick, J. Yamagishi and I. Echizen, "Distinguishing computer graphics from natural images using convolution neural networks," 2017 IEEE Workshop on Information Forensics and Security (WIFS), Rennes, France, 2017, pp. 1-6, doi: 10.1109/WIFS.2017.8267647.
- [17] Fengyi Song, Xiaoyang Tan, Xue Liu, Songcan Chen. "Eyes closeness detection from still images with multi-scale histograms of principal oriented gradients" Pattern Recognition, Volume 47, Issue 9, September 2014, Pages 2825-2838.
- [18] Davis E. King. "Dlib-ml: A Machine Learning Toolkit". The Journal of Machine Learning Research, Volume 10, 2009, Pages 1755 – 1758.
- [19] Tianyi Wang, Harry Cheng, Kam Pui Chow, Liqiang Nie, "Deep Convolutional Pooling Transformer for Deepfake Detection", ACM Transactions on Multimedia Computing, Communications and Applications, Volume 19, Issue 6, May 2023.
- [20] Wei Lu, Lingyi Liu, Junwei Luo, Xianfeng Zhao, Yicong Zhou, Jiwu Huang, "Detection of Deepfake Videos Using Long Distance Attention", IEEE Transactions on Neural Networks and Learning Systems, Volume: 35, Issue: 7, July 2024.
- [21] Eren, H.; Karaduman, Ö.; Gençoglu, M.T. Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review. Appl. Sci. 2025, 15, 3225. <https://doi.org/10.3390/app15063225>.
- [22] Khan, A.A., Laghari, A.A., Alrobaea, R. et al. A lightweight scalable hybrid authentication framework for Internet of Medical Things (IoMT) using blockchain hyperledger consortium network with edge computing. Sci Rep 15, 19856 (2025). <https://doi.org/10.1038/s41598-025-05130-w>.
- [23] Ignor, O.S.; Amin, M.B.; Garg, S. The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review. Blockchains 2025, 3, 5. <https://doi.org/10.3390/blockchains3010005>.