Volume: 14 Issue: III Month of publication: March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78370

Real-Time Detection of Fake AI-Generated Videos Using Deep Learning and Big Data Analytics: A Scalable Cyber Security Strategy

Rajendra Singh[1], Dr. Preeti Gupta[2]
[1]*Ph.D. Scholar, Department of Computer Science & Engineering, Mind Power University, Bhimtal, Nainital, Uttrakhand*
[2]*Assistant Professor, Department of Computer Science & Engineering, Mind Power University, Bhimtal, Nainital, Uttrakhand*

Abstract: The popular production of synthetic media that are of high quality and highly realistic, also referred to as deepfakes, is due to the rapid development of artificial intelligence (AI) and generative models. Although these technologies bring novel opportunities in the entertainment, education, and digital media production domain, they also present a big threat to cybersecurity, privacy, and social trust. The misinformation campaign, identity scams, political influence, and a fraud of money can be conducted with the help of the fake AI-generated videos. Therefore, timely deepfake video detection has emerged as a serious field of research in digital forensics and cybersecurity. The following review paper will present a plethora of current methods of identifying AI-produced fake videos with the help of deep learning and big data analysis. It investigates many types of deep learning frameworks like convolutional neural networks (CNNs), recurrent neural networks (RNNs), generative adversarial network (GAN) detection models, and transformer-based ones. The research also examines how the big data models like Hadoop, Spark and distributed cloud computing have facilitated scalability and real-time detection systems. Additionally, the paper examines benchmark data, measures of evaluation, detection issues, and future directions of research in deepfake detection. The article has identified the use of artificial intelligence coupled with big data infrastructure as essential in developing scalable cybersecurity measures that can process large quantities of multimedia data that are generated in the digital platform. The results propose that spatial, temporal, and behavioral hybrid models are more accurate in the detection. Also, the newly developed technologies explainable AI, federated learning, and blockchain are likely to make the deepfake detection systems even more reliable. The scope of this review will be summarized as offering researchers and cybersecurity practitioners a summarized view of the deepfake detectors and the advancement of real-time scalable security frameworks.

Keywords: Artificial Intelligence, Big Data Analytics, Cyber Security, Deep Learning, Deepfake Detection.

I. INTRODUCTION

In the recent years, technological advances in the field of artificial intelligence (AI) have transformed the digital media production. Deep learning-based generative models that include Generative Adversarial Networks (GANs) and autoencoders have made it possible to generate hyper-realistic synthetic images, audio, and videos. The creation of the so-called deepfake videos that are modified or completely produced videos created with the help of AI algorithms is one of the most alarming trends in this area. These videos are able to convincingly emulate real personalities, and it is not easy to detect between authentic and false material that is written by the human beings [1].

The spread of deepfake videos has created Great concern in the area of cybersecurity, journalism, politics, and verification of digital identity. Deepfake may be employed in malice and malicious intent in terms of misinformation campaigning, blackmail, and monetary fraud, and political propaganda. As an example, the manipulated videos of the prominent figures may affect the election, harm the image, or cause social conflicts. Availability of open-source deep fake tools and the enormous growth of social media networks have only added fuel to the proliferation of fake videos [2].

Conventional digital forensic methods were majorly created to identify solely complex picture manipulation or video editing artifacts. Nevertheless, the current AI-created videos involve using complex neural networks that allow producing highly realistic facial expressions, light effects, and motion patterns. Consequently, these sophisticated manipulations can no longer be discovered by using traditional detection approaches. This has prompted scientists to come up with deep learning-based detection algorithms that can analyze the slight abnormalities in video frames, movement of faces, as well as temporal variations [3].

Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are deep learning models that have shown encouraging performances in the process of detecting deepfake videos. The CNNs are also especially efficient in the spatial analysis of video frames, whereas RNNs are capable of learning the temporal correlation between video frames. Transformer-based models and attention mechanisms have also enhanced the accuracy of detection by detecting long-range relations in video sequences [4].

Besides more sophisticated data algorithm detection tools, the sheer volume of multimedia data being created within digital platforms necessitates a robust system of data processing. Hadoop, Apache Spark, and distributed cloud systems are also big data analytics frameworks that are important in processing and analysing large volumes of video data in real-time. Through the combination of deep learning models with big data architecture, scholars can create scalable cybersecurity frameworks that can identify deep fake videos on social media, streaming services and surveillance systems [5].

This review paper analyses the present situation in the study of deepfake detection with special attention to deep learning framework and big data analytics approaches to allow real-time detection. Such topics as benchmark datasets, evaluation methods, system architectures, and new technologies that may strengthen deepfake detection abilities are discussed in the paper, too. Lastly, the paper outlines the major challenges and research areas moving forward to develop a strong cybersecurity measures against AI-enabled fake videos.

II. BACKGROUND OF DEEPFAKE TECHNOLOGY

Deepfake technology was created as a result of the progress in the field of deep learning and generative models. Deepfake is a portmanteau of deep learning and fake, which means that the process of deep learning is used to produce AI-based media and use it to manipulate visual or audio data to resemble a real person but is fabricated [6].

Majority of deepfake videos are produced with the help of machine learning models that include Generative Adversarial networks (GANs), Variational autoencoders (VAEs) and face-swapping algorithms. GANs are two neural networks; the generator and the discriminator which compete. Synthetic content is generated by the generator and the discriminator tries to recognize real and generated samples. During training, the generator is trained to give more and more realistic outputs [7].

The techniques of first-generation deepface were mainly based on face-swapping algorithms, in which the face shapes of a person are transferred to a different face in a video. Modern deepfake systems are capable, however, of producing fully synthetic faces, voice clones and realistic facial expressions. Such developments have made it much harder to find manipulated data [8].

The accessibility of deepfake generators like DeepFaceLab, FaceSwap and StyleGAN has allowed untrained people to produce realistic fake videos with only basic knowledge of how to do so. Consequently, the use of deepfakes has become more prevalent in the social media and online communities.

III. DEEP LEARNING METHODS OF DEEPFAKE DETECTION

The power of deep learning has made it the most useful tool in the detection of AI-generated fake videos because it can automatically extract complex patterns and features with large volumes of data [9].

A. *Convolutional Neural Networks (CNNs)*

CNN-based models examine spatial features of video frames to identify inconsistencies due to manipulations done by AI. Such networks are able to detect irregular patterns of textures, unnatural patterns of lighting, and irregular shapes of the face that can hardly be identified by the human eye [10].

The most popular CNN architectures that are applicable in detecting deepfakes are ResNet, VGGNet, and EfficientNet. These models are trained on a large set of real and fake videos to be taught about discriminative features.

B. *Recurrent Neural Networks (RNNs)*

RNNs are known to analyze sequential data, thus they can be applied to video analysis. RNNs preserve the temporal relationships of frames unlike CNNs, which only analyze each frame. Facial movement, blinking patterns and lip synchronization analysis between video sequences are typically analyzed using Long Short-Term Memory (LSTM) networks [11].

C. *Transformer-Based Models*

The application of transformers in deepfake detection has recently become popular because of its capability to capture long-range dependencies in the video sequences. Spatial and temporal features Vision Transformers (ViTs) and attention-based networks have the capability to analyze complex features simultaneously [12].

D. Detection of Motion vectors Artifact in Compressed Videotapes

A majority of current methods of deepfake detection are based on the analysis of fully decoded video frames by computationally expensive deep learning models. These methods are very accurate but they consume a lot of computational power and are not suitable in real-time detection of large scale multimedia data. Recent studies have overcome this shortcoming by attempting to use low-computational detection methods that use compressed video formats like H.264.

Video compression rules such as the H.264 rely on motion estimation to decrease the redundancy among successive images. In this procedure, motion vectors are computed in order to show the movement of macroblocks among the frames. These motion vectors represent valuable temporal data concerning the movement of objects in the scene and the dynamic nature of the scene. Motion vectors of genuine videos are usually in a smooth and uniform motion pattern. Nevertheless, deep fake video may create anomalies in motion vectors fields as they do not align with generated frames and original motion vectors.

These abnormal patterns are detected by motion vector artifact-based detection systems that do not completely decode the video frames. This greatly decreases the complexity of the computations since the algorithm is run using features in the compressed-domain instead of pixel-level data. Various works have shown that the analysis of the difference in motion vectors and prediction residuals, macroblock inconsistencies can be a strong method of separating real and AI-created videos.

Compressed-domain features are also useful in the creation of scalable features that can be used to detect large video streams in real time. These methods are especially useful in the case of social media, surveillance, and video streaming services where millions of videos are uploaded every day. With the combination of motion vector analysis and lightweight machine learning or deep learning models, researchers may develop effective cybersecurity systems to detect deepfake videos with a minimal computational cost.

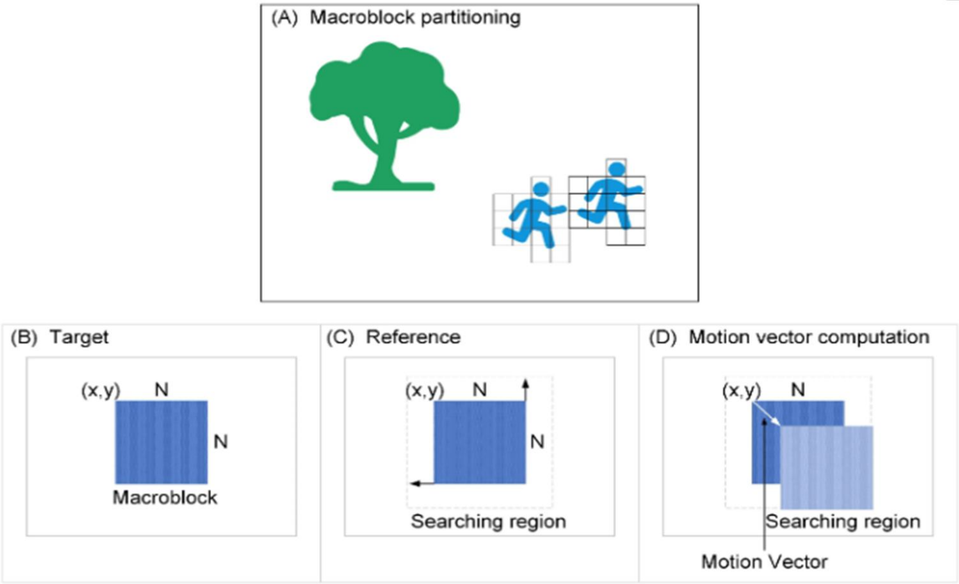

Figure 1: Block-based motion estimation method. (A) The image is divided into macroblocks. (B) A macroblock in the target frame. (C) Reference frame, where the macroblock searched for similar blocks. (D) The macroblocks in the target frame are found to be the most similar blocks within the specified search range by using a block matching algorithm in the reference frame [13]

This figure 1 indicates that motion vectors are created in the H.264 video compression to indicate the change in the positions of macro blocks between two frames. In natural videos, motion vectors tend to take smooth patterns. Nevertheless, deepfake videos generated by AI are usually associated with irregular distributions of motion vectors, which can be identified to identify manipulation with high efficiency.

IV. BIG DATA ANALYTICS AS PART OF REAL-TIME DETECTION

The high amount of video information produced on social media networks necessitates scalable systems to process and analyze.
Distributed computing services like Hadoop and Apache Spark have been used as the big data analytics platforms to enable the deep learning models to work on the large size of video data simultaneously.

Cloud computing systems also contribute to scalability by allowing on-demand computing infrastructure on training and deploying deepfake detection models [14].

Table 1: Comparison of Deep Learning Techniques for Deepfake Detection

Method	Strength	Limitation	Accuracy Range
CNN	Strong spatial feature extraction	Limited temporal analysis	85–95%
RNN	Captures temporal patterns	High computational cost	80–92%
CNN + LSTM	Combines spatial and temporal features	Complex training	90–97%
Transformers	Long-range dependency analysis	Large dataset required	92–98%

This table 1 is a comparison of popular deep learning systems in deepfake detection. CNN models are suitable in extracting spatial features, whereas RNN models are used in extracting temporal features. The Hybrid CNN-LSTM represents a better version of the CNN and LSTM models as it has elevated the accuracy of detection. Models involving transformers offer better performance, but are expensive to train on limited datasets and cannot use limited computing resources.

V. DEEPFAKE DETECTION DATASET

Several publicly available datasets are used to train and evaluate deepfake detection system.

Table 2: Deepfake Detection Dataset [15]

Dataset	Description	Size
FaceForensics++	Contains manipulated videos generated using various techniques	1,000+ videos
DeepFake Detection Challenge (DFDC)	Large-scale dataset released by Facebook	100,000+ videos
Celeb-DF	High-quality deepfake videos of celebrities	5,000+ videos
DeeperForensics	Dataset designed for real-world detection scenarios	60,000+ videos

The table 2 above gives widespread benchmark datasets in deepfake detection studies. FaceForensics++ and Celeb-DF deal with datasets of face manipulations, and DFDC is a large-scale dataset that can be used to train deep learning models. DeeperForensics presents both realistic distortions and environmental changes to test detection systems in practice.

VI. DEEPFAKE DETECTION ON REAL TIME SYSTEMS [16]

An effective deepfake detector system is usually scalable and has several components:

1) Data collection layer
2) Miniprocessing and feature integration.
3) Deep learning detection frameworks.
4) Big data analytics architecture.
5) Real-time alert system

Table 3: Architecture Components of a Real Time Detection System

Component	Function
Data Acquisition	Collects videos from online platforms
Preprocessing	Extracts frames and facial features
Detection Model	Applies deep learning algorithms
Big Data Engine	Handles large-scale data processing
Decision Module	Generates alerts or flags content

This table identifies the major parts of a scalable deep fake detector architecture. Multimedia data on the internet is collected through data acquisition and preprocessing transforms video frames into a format that can undergo analysis. Deep learning models are used to accomplish detection work, and big data engines are used for scalable processing. The decision module sends alerts in case suspicious videos are found.

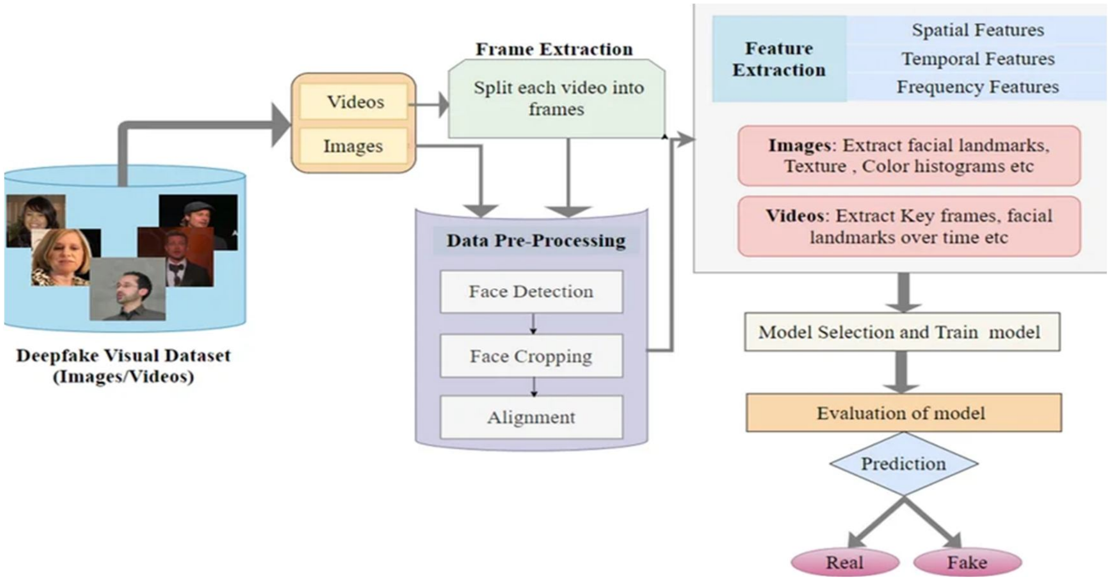
Frame Extraction
Split each video into frames
Videos
Images
Feature Extraction
Spatial Features
Temporal Features
Frequency Features
Images: Extract facial landmarks, Texture , Color histograms etc
Videos: Extract Key frames, facial landmarks over time etc
Data Pre-Processing
Face Detection
Face Cropping
Alignment
Deepfake Visual Dataset (Images/Videos)
Model Selection and Train model
Evaluation of model
Prediction
Real
Fake

Figure 2: Flow chart of visual deepfake detection [17]

Figure 2 represents the design of a real-time deepfake detector. The entire process starts by acquiring the videos online, then preprocessing is done and then the frame is extracted. Deep learning models consider both the spatial and temporal characteristics to determine manipulations. Big data designs permit scalability of processing, and the decision unit identifies suspicious videos to verify it further.

VII. DIFFICULTIES OF REAL-TIME DEEPFAKE DETECTION

Even with all these developments, there are still a number of issues regarding the identification of AI-generated fake videos [18].

To begin with, the deepfake generation technologies are advancing at a fast rate such that detection systems are hard to keep up. New generative models are able to generate more realistic videos with few artifacts [19].

Second, deep learning detection models need large labeled datasets to be trained. But the acquisition of good-quality annotated datasets is difficult because of the privacy issues and constraints of data collection [20].

Third, real time detection consumes a lot of computational resources. The detection systems are limited in the complexity of the deep learning models that may introduce latency when processing high-resolution videos [21].

Fourth, detection systems can be bypassed with the help of adversarial attacks. The attackers can purposefully alter deepfakes videos to circumvent the detection algorithms [22].

VIII. THE NEW TECHNOLOGIES TO DETECT DEEPFAKES

Some emerging technologies promise to enhance the process of deepfake detection.

Explainable AI methods are used to gain a better understanding of deep learning models and to give transparency in detection decisions.

Federated learning facilitates the joint training of models in more than two organisations without exchanging sensitive information.

The blockchain technology can be used to offer a safe digital signature to verify the validity of multimedia content [23], [24], [25].

IX. FUTURE RESEARCH DIRECTIONS

Further studies are necessary to create the multimodal detection systems to examine video, audio, and contextual metadata all at the same time. More effective detection can be achieved by hybrid designs based on deep learning with conventional forensic tools.

Also, big data infrastructures will be combined with artificial intelligence to accommodate the sheer volume of multimedia data created over the internet.

X. CONCLUSION

The Deepfake technology is one of the most relevant cybersecurity threats in the digital age. Artificial intelligence generated videos are becoming real, and this has become dangerous to political stability, financial security, and trust among the population. These videos are hard to detect with a single model of deep learning unless those models are scaled using large infrastructures of big data.

The current review paper has analyzed the different deep learning methods that are applied to deepfake detection and these methods are CNNs, RNNs, and transformer-based models. The use of big data analytics to facilitate scalable detection systems had also been talked about. The paper has also reviewed benchmark datasets, detection architectures and some upcoming technologies that may be employed to improve cybersecurity strategies.

The results indicate that hybrid detection models involving spatial and temporal analysis are more accurate as compared to single models. In addition, the detection systems can be more reliable and transparent by incorporating explainable AI, federated learning, and blockchain technologies.

Since the impact of deepfake technology is still evolving, researchers and cybersecurity experts should devise scalable and responsive solutions in countering the use of AI-generated fake news. The future ways of detecting should be centered on real-time processing, multimodal analysis, and collaborative security frameworks to adequately deal with the increasing threat of fake AI-generated videos.

REFERENCES

[1] F. Abbas and A. Taeihagh, “Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence,” 2024. doi: 10.1016/j.eswa.2024.124260.

[2] M. Alrashoud, “Deepfake video detection methods, approaches, and challenges,” 2025. doi: 10.1016/j.aej.2025.04.007.

[3] L. Stroebel, M. Llewellyn, T. Hartley, T. S. Ip, and M. Ahmed, “A systematic literature review on the effectiveness of deepfake detection techniques,” 2023. doi: 10.1080/23742917.2023.2192888.

[4] G. Petmezas, V. Vanian, K. Konstantoudakis, E. E. I. Almaloglou, and D. Zarpalas, “Video deepfake detection using a hybrid CNN-LSTM-Transformer model for identity verification,” Multimed. Tools Appl., 2025, doi: 10.1007/s11042-024-20548-6.

[5] N. K. Sagar and S. Arukonda, “A Novel CNN-LSTM Approach for Robust Deepfake Detection,” in Procedia Computer Science, 2025. doi: 10.1016/j.procs.2025.04.436.

[6] A. H. Soudy et al., “Deepfake detection using convolutional vision transformers and convolutional neural networks,” Neural Comput. Appl., 2024, doi: 10.1007/s00521-024-10181-7.

[7] S. Yadav and S. S. Mangalampalli, “Deepfake defense: Combining spatial and temporal cues with CNN–BiLSTM–transformer architecture,” PLoS One, 2025, doi: 10.1371/journal.pone.0334980.

[8] Vishal Manishbhai Patel and Dr. Sheshang Degadwala, “Deepfake Detection Using Convolutional Neural Networks and LSTM Modelling,” Int. J. Sci. Res. Sci. Technol., 2025, doi: 10.32628/ijsrst2512361.

[9] A. G. Singh and P. Sharma, “A Hybrid Deep Learning Framework for Robust Deepfake Detection Using CNN, LSTM, and Vision Transformers,” 2024.

[10] W. H. Abir et al., “Detecting Deepfake Images Using Deep Learning Techniques and Explainable AI Methods,” Intell. Autom. Soft Comput., 2023, doi: 10.32604/iasc.2023.029653.

[11] Y. Zhang, Q. Li, Z. Yu, and L. Shen, “Distilled transformers with locally enhanced global representations for face forgery detection,” Pattern Recognit., 2025, doi: 10.1016/j.patcog.2024.111253.

[12] E. M. Sathwik Reddy, A. Pavan Kumar, and P. Swetha, “Deepfake video detection using CNN and RNN with OPTICAL FLOW features,” in 2024 IEEE International Students’ Conference on Electrical, Electronics and Computer Science, SCEECS 2024, 2024. doi: 10.1109/SCEECS61402.2024.10482344.

[13] D. Shao, N. Wang, P. Chen, Y. Liu, and L. Lin, “A Novel Video Compression Approach Based on Two-Stage Learning,” Entropy, 2024, doi: 10.3390/e26121110.

[14] D. A. Coccomini, R. Caldelli, F. Falchi, and C. Gennaro, “On the Generalization of Deep Learning Models in Video Deepfake Detection,” J. Imaging, 2023, doi: 10.3390/jimaging9050089.

[15] A. Naitali, M. Ridouani, F. Salahdine, and N. Kaabouch, “Deepfake Attacks: Generation, Detection, Datasets, Challenges, and Research Directions,” 2023. doi: 10.3390/computers12100216.

[16] E. Temir, “Deepfake: New Era in The Age of Disinformation &amp; End of Reliable Journalism TT - Deepfake: Dezenformasyon Çağında Yeni Dönem ve Güvenilir Haberciliğin Sonu,” Selçuk İletişim, 2020.

[17] N. Sandotra and B. Arora, “A comprehensive evaluation of feature-based AI techniques for deepfake detection,” 2024. doi: 10.1007/s00521-023-09288-0.

[18] F. Ding, R. Kuang, Y. Zhou, L. Sun, X. Zhu, and G. Zhu, “A survey of Deepfake and related digital forensics,” J. Image Graph., 2024, doi: 10.11834/jig.230088.

[19] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Niessner, “FaceForensics++: Learning to detect manipulated facial images,” in Proceedings of the IEEE International Conference on Computer Vision, 2019. doi: 10.1109/ICCV.2019.00009.

[20] Y. Li, M. C. Chang, and S. Lyu, “In Ictu Oculi: Exposing AI created fake videos by detecting eye blinking,” in 10th IEEE International Workshop on Information Forensics and Security, WIFS 2018, 2018. doi: 10.1109/WIFS.2018.8630787.

[21] H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, “Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos,” in 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems, BTAS 2019, 2019. doi: 10.1109/BTAS46853.2019.9185974.

[22] B. Batagelj, A. Kronovšek, V. Štruc, and P. Peer, “Robust cross-dataset deepfake detection with multitask self-supervised learning,” ICT Express, 2025, doi: 10.1016/j.icte.2025.02.011.

[23] L. Guarnera, O. Giudice, and S. Battiato, “DeepFake detection by analyzing convolutional traces,” in IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2020. doi: 10.1109/CVPRW50498.2020.00341.

[24] D. S. AC, M. K. KM, P. M, P. Chincholi, P. H B, and R. a, “Experimental Detection of Deep Fake Images Using Face Swap Algorithm.,” SSRN Electron. J., 2025, doi: 10.2139/ssrn.5253609.

[25] J. Hu, X. Liao, W. Wang, and Z. Qin, “Detecting Compressed Deepfake Videos in Social Networks Using Frame-Temporality Two-Stream Convolutional Network,” IEEE Trans. Circuits Syst. Video Technol., 2022, doi: 10.1109/TCSVT.2021.3074259.