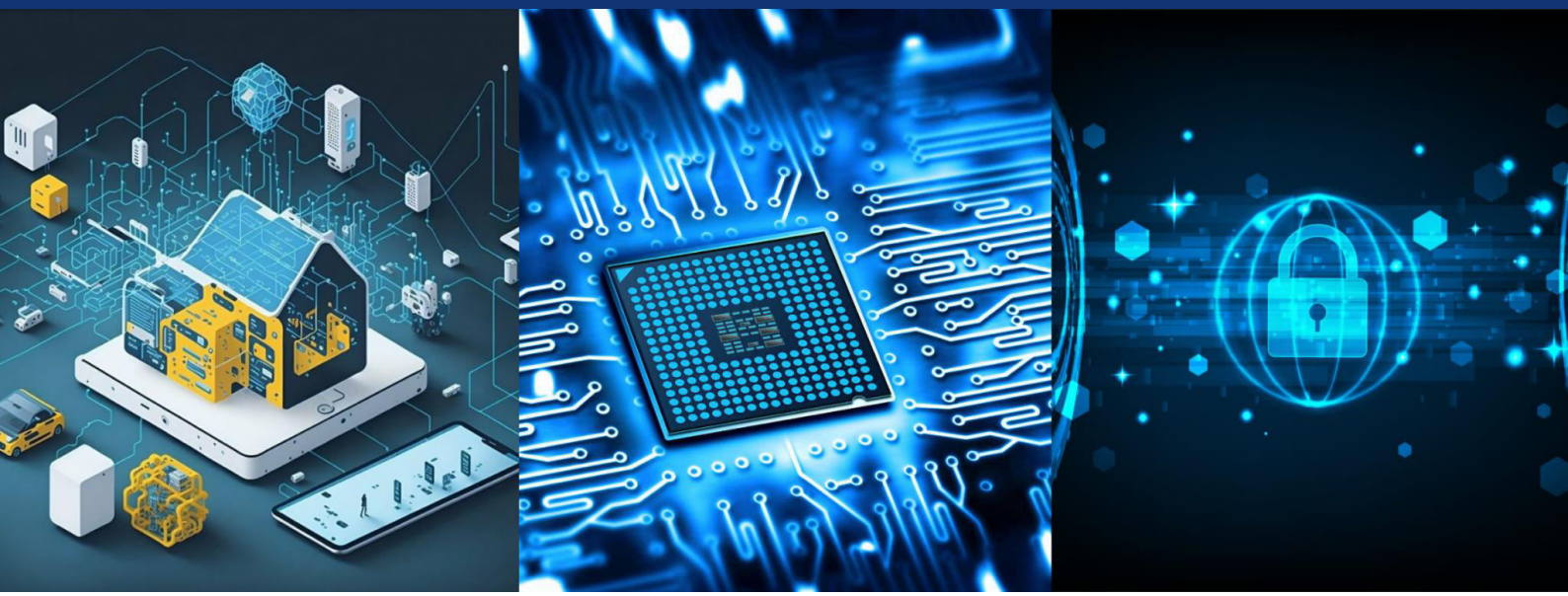
IJIRCCE

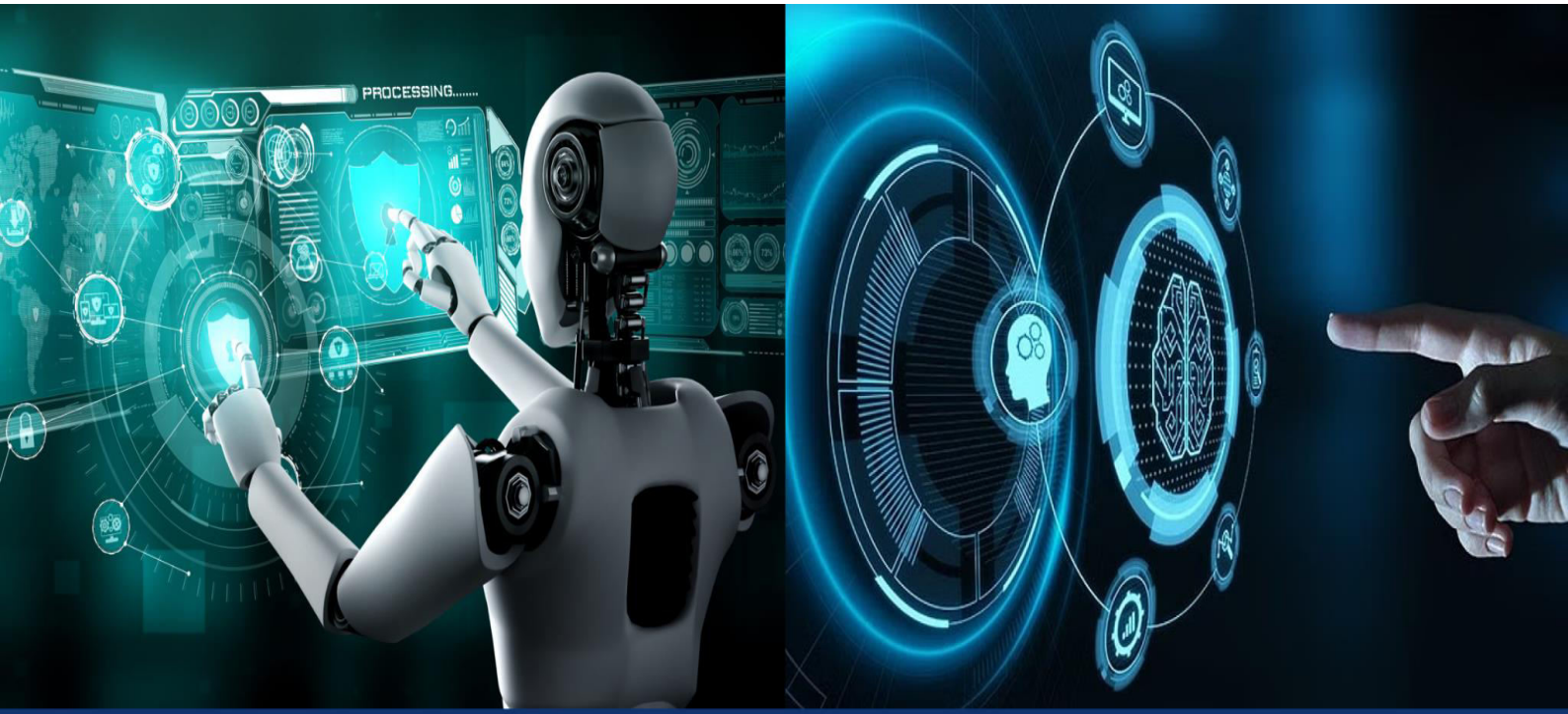
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304282

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Dual Attention Network Approaches Face Forgery and Video Detection

Bhuvaneswari.S

Assistant Professor, PG & Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences Women(Autonomous), Tiruchengode, Tamil Nadu, India

Nishanthini.S

II-MCA**,** PG & Research Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Tamil Nadu, India

ABSTRACT:
The rapid advancement and widespread adoption of digital technologies have significantly contributed to the proliferation of forged photographs and videos on the Internet. This escalation poses serious concerns regarding the rise of fraudulent identities, thereby impacting societal security. Traditional forgery detection methods, commonly referred to as classical approaches, exhibit limitations in accurately identifying such fraudulent activities. These constraints primarily stem from their reliance on publicly available centralized datasets, which do not adequately address privacy and security concerns. Consequently, their effectiveness in detecting counterfeit content is compromised.To address these challenges, this study introduces an advanced deep learning methodology based on federated learning, designed to enhance forgery detection.The model was trained using three widely recognized forensic datasets: FaceForensics++, Deepforensic-1.0, and WildDeepfake. Canonical Correlation Analysis was employed to construct a comprehensive feature vector, which was subsequently utilized to train Convolutional Neural Networks (CNNs) for detecting manipulated visual content. The model's performance was systematically evaluated against existing deep learning techniques within federated learning environments. The experimental results demonstrate that the proposed approach outperforms conventional models, exhibiting superior accuracy in identifying forgeries while ensuring data privacy and security. Our proposed approach demonstrated exceptional performance, achieving an accuracy rate of 98.99% when evaluated on the merged dataset.

KEYWORDS: Advanced technologies, forged photographs, fraudulent identities, federated learning, deep learning, Convolutional Neural Networks, FaceForensics++, Deepforensic-1.0, WildDeepfake.

I. INTRODUCTION

The forgery of images has evolved from a labor-intensive process to a rapid and accessible one due to advancements in Generative Adversarial Networks (GANs), enabling anyone with basic resources to create face-swapping deepfake videos. While deepfake technology has legitimate uses in media, its malicious application causes social harm, especially with forged videos targeting public figures. Detecting such forgeries is challenging due to their realistic appearance, making it difficult for the public to identify manipulated content.Video Media Forensics (VMF) has become increasingly important, especially with the rise of social media and digital information reliance. Convolutional Neural Networks (CNNs) are widely used for detecting deepfake videos, but deep generative models like GANs have evolved to evade detection. Traditional methods focus on detecting visual artifacts or inconsistencies in facial features, but they struggle to generalize across datasets due to variations in image sources, compression methods, and devices.This study introduces a 3D Morphable Model (3DMM) to decompose facial images into five components: 3D geometry, common texture, identity texture, ambient light, and direct light. Among these, identity texture and direct light are key to detecting forgery, as they are harder to simulate and show noticeable high-frequency artifacts. We propose a two-stream network, **FD2Net**, that combines clues from the original image and facial details, with a supervised attention mechanism to highlight distinguishing features for forgery detection.Furthermore, we address privacy concerns and dataset limitations with a novel Federated Learning approach, **FedForgery**, for training face forgery detection models.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304282

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

FIGURE 1. SAMPLE IMAGES FROM FF++ AND DFDC DATASETS

II.LITERATURE SURVEY

Video forgery and deepfake detection have become critical areas of research due to the increasing accessibility and misuse of synthetic video generation technologies. Various researchers have proposed methods and datasets to identify, analyze, and counter these manipulations effectively.

[1] S. K. N. and H. R. Chennamma Provided a comprehensive survey of video forgery detection techniques, categorizing methods into spatial, temporal, and spatio-temporal approaches. Their work lays a strong foundation by summarizing the evolution and challenges in detecting video manipulations.
[2] Vaccari and Chadwick Explored the sociopolitical impact of deepfakes, particularly how synthetic political videos affect public perception, trust, and the spread of misinformation. Their findings highlight the real-world implications of deepfake technology beyond the technical realm**.**
[3] Bonettini et al. Developed a deep learning-based approach using an ensemble of Convolutional Neural Networks (CNNs) to detect facial manipulations in videos.
[4] Afchar et al. Introduced **MesoNet**, a compact and efficient neural network specifically tailored for facial forgery detection in videos. It focuses on mesoscopic features, balancing performance and computational efficiency, making it suitable for real-time applications.
[5] Li and Lyu Proposed a method to detect face warping artifacts, a common issue in synthesized faces, providing a practical way to expose deepfakes with minimal computational resources. Additionally, their work on eye blinking detection [10] and head pose inconsistencies [8] introduced unique physiological cues for forgery detection.
[6] Karras et al. Significantly advanced generative models with their StyleGAN architecture, indirectly contributing to forgery detection research by setting the benchmark for high-quality synthetic face generation.
[7] Yang et al. Proposed methods to detect GAN-generated faces through inconsistencies in facial landmarks and unnatural head poses. These studies provided crucial insights into geometric and physical inconsistencies of deepfakes.
[8] Matern et al. Focused on visual artifacts introduced during face manipulation processes, offering methods to exploit these artifacts for deepfake detection. Their work served as an early recognition of artifact-level detection strategies.
[9] Rossler et al. Contributed the **FaceForensics++** dataset, a large-scale benchmark for evaluating face manipulation detection models. This dataset has become a standard in training and evaluating deepfake detection algorithms.
[10] Dolhansky et al. Released the **DeepFake Detection Challenge (DFDC)** dataset, further enabling the development and benchmarking of detection models on a diverse and extensive video dataset.
[11] Tan and Le Introduced **EfficientNet**, an architecture that balances model performance and computational load. EfficientNet has been widely adopted in deepfake detection due to its scalability and accuracy.
[12] Woo et al. Presented the **Convolutional Block Attention Module (CBAM)**, an attention mechanism that enhances feature learning in CNNs. CBAM has been incorporated into many detection models to improve performance on subtle manipulations.
[13] Zhao et al. Designed a multi-attentional framework that leverages spatial and temporal features, showing significant improvements in detecting complex video manipulations.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304282

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

[14] Guo et al. Proposed an adaptive network for extracting manipulation traces, focusing on residual features that remain consistent across different forgery methods.

[15] Saikia et al Introduced a hybrid CNN-LSTM model utilizing optical flow features to capture both satial and motion-based inconsistencies in deepfake videos.

III. METHODOLOGY

The initial step involves examining the image metadata. While metadata can be easily altered using simple programs, most images we encounter will have unmodified metadata, which helps in detecting alterations. The image is then converted into an error level analysis (ELA) format and resized to 100x100 pixels—one for a fake image and another for a real one. A fine-grained classification method is used for deepfake detection, incorporating a novel multi-attentional deepfake detection network. Additionally, DenseNet is utilized for pre-processing to enhance traces left by forgeries, improving detection accuracy. By integrating DenseNet with CNN, a deep forgery detector called DenseNet is developed.

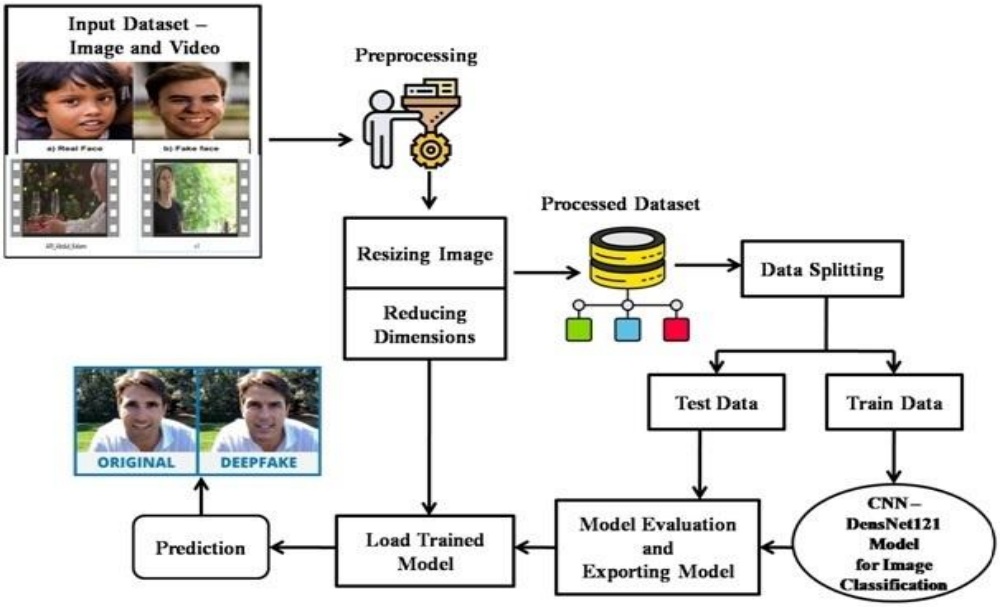


FIGURE 2: FLOW DIAGRAM OF FACE FORGERY DETECTION

The image illustrates a deepfake detection pipeline using Convolutional Neural Networks (CNN), specifically DenseNet121. The process begins with an input dataset comprising real and fake images and videos. Preprocessing steps include resizing and dimensionality reduction. The data is then split into training and testing sets. The DenseNet121 model is trained on the processed data for classification. The trained model is evaluated, exported, and used for prediction on new inputs, distinguishing between original and deepfake content.

IV. PROPOSED SYSTEM

In proposed first checks the image metadata. Image metadata is not that much reliable since it can be altered using simple programs. But most of the images we come across will have non-altered metadata which helps to identify the alterations. The image is converted into error level analyzed format and will be resized to 100px x 100px image. One for fake image and one for real image. A fine-grained classification method for deepfake detection and proposed a new multi-attentional deepfake detection network to implement it. Then proposed an DenseNet for pre-processing to enhance the traces that are generated by a forgery to improve detection. They integrated DenseNet with CNN to construct a deep forgery detector called DenseNet.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI:10.15680/IJIRCCE.2025.1304282

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

V.OUTPUT

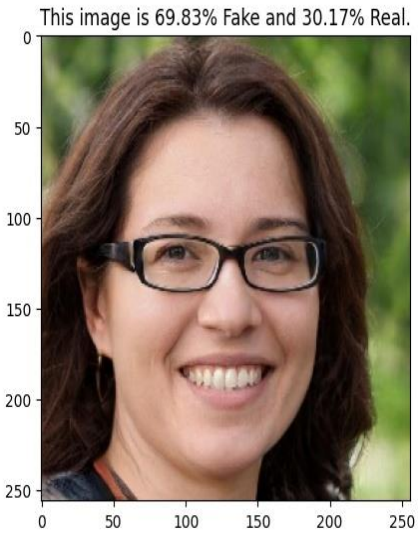


FIGURE 3: RESULT AND ANALYSIS

Figure displays an example of a detected synthetic image with a **69.83% probability of being fake and 30.17% probability of being real**. The model has effectively assigned a higher probability to the image being fake, indicating its capability to distinguish AI-generated images from real ones. This classification is achieved by leveraging the hierarchical feature representations learned by DenseNet. The model examines intricate details such as **facial symmetry, texture inconsistencies, and unnatural lighting artifacts** commonly found in deepfake images.

The detection performance is evaluated using standard metrics such as **accuracy, precision, recall, and F1-score**. The DenseNet-based model demonstrates superior performance in deepfake detection compared to traditional CNN architectures due to its efficient feature propagation and ability to capture complex patterns across multiple layers.

VI. CONCLUSION

This study introduces three significant contributions to addressing the deepfake detection challenge. First, the SRAB attention mechanism, FFAM, enhances the model's ability to identify warping traces. Second, DenseNet is employed as the backbone network to develop a novel architecture, DAFDN, specifically designed for detecting manipulated images. Third, the detection results of DAFDN are visually interpreted using heatmaps. The proposed method was evaluated on two publicly available datasets, demonstrating superior performance compared to DenseNet and other traditional deepfake detection approaches. These findings confirm the effectiveness of the two attention mechanisms incorporated in DAFDN for deepfake image detection

REFERENCES

[1] S. K. N. and H. R. Chennamma, "A survey on video forgery detection," Mar. 2021, arXiv:1503.00843.
[2] C. Vaccari and A. Chadwick, "Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news," Social Media Soc., vol. 6, no. 1, pp. 1–13, Feb. 2020.
[3] N. Bonettini, E. D. Cannas, S. Mandelli, L. Bondi, P. Bestagini, and S. Tubaro, "Video face manipulation detection through ensemble of CNNs," in Proc. 25th Int. Conf. Pattern Recognit. (ICPR), Jan. 2021, pp. 5012–5019.
[4] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "MesoNet: A compact facial video forgery detection network," in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2022, pp. 1–7.
[5] Y. Li and S. Lyu, "Exposing DeepFake videos by detecting face warping artifacts," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, Dec. 2019, pp. 46–52.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

[6] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2019, pp. 4401–4410.
[7] X. Yang, Y. Li, H. Qi, and S. Lyu, "Exposing GAN-synthesized faces using landmark locations," in Proc. ACM Workshop Inf. Hiding Multimedia Secur., Jul. 2019, pp. 113–118.
[8] X. Yang, Y. Li, and S. Lyu, "Exposing deep fakes using inconsistent head poses," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), May 2019, pp. 8261–8265.
[9] F. Matern, C. Riess, and M. Stamminger, "Exploiting visual artifacts to expose DeepFakes and face manipulations," in Proc. IEEE Winter Appl. Comput. Vis. Workshops (WACVW), Jan. 2019, pp. 83–92.
[10] Y. Li, M.-C. Chang, and S. Lyu, "In ictu oculi: Exposing AI created fake videos by detecting eye blinking," in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2018, pp. 1–7.
[11] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to detect manipulated facial images," in Proc. IEEE/CVF Int. Conf. Comput. Vis., Oct. 2019, pp. 1–11.
[12] B. Dolhansky, J. Bitton, B. Pflaum, J. Lu, R. Howes, M. Wang, and C. C. Ferrer, "The DeepFake detection challenge (DFDC) dataset," 2020, arXiv:2006.07397.
[13] M. Tan and V. Quoc Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," in Proc. 36th Int. Conf. Mach. Learn., vol. 97, 2019, pp. 6105–6114.
[14] S. Woo, J. Park, J. Y. Lee, and I. S. Kweon, "CBAM: Convolutional block attention module," in Proc. Eur. Conf. Comput. Vis., 2018, pp. 3–19.
[15] H. Zhao, T. Wei, W. Zhou, W. Zhang, D. Chen, and N. Yu, "Multiattentional deepfake detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2021, pp. 2185–2194.
[16] N. Bonettini, E. D. Cannas, S. Mandelli, L. Bondi, P. Bestagini, and S. Tubaro, "Video face manipulation detection through ensemble of CNNs," in Proc. 25th Int. Conf. Pattern Recognit. (ICPR), Jan. 2021, pp. 5012–5019.
[17] Z. Guo, G. Yang, J. Chen, and X. Sun, "Fake face detection via adaptive manipulation traces extraction network," Comput. Vis. Image Understand., vol. 204, Mar. 2021, Art. no. 103170.
[18] P. Saikia, D. Dholaria, P. Yadav, V. Patel, and M. Roy, "A hybrid CNNLSTM model for video deepfake detection by leveraging optical flow features," 2022, arXiv:2208.00788.
[19] D. Zhang, F. Lin, Y. Hua, P. Wang, D. Zeng, and S. Ge, "Deepfake video detection with spatiotemporal dropout transformer," 2022, arXiv:2207.06612.
[20] K. Shiohara and T. Yamasaki, "Detecting deepfakes with self-blended images," 2022, arXiv:2204.08376.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details