Progress In Deep Fake And Tampering : An In-Depth Analysis

Dr. Chethan L S[1], Aishwarya P[2], Chandana T S[2], Ganavi B R[2], Gowthami.D[2],

[1]*AssociateProfessor, Department of Computer Science and Engineering, PESITM, Shimoga*

[2]*UG Students, Department of Computer Science and Engineering, PESITM, Shimoga*

NH – 206, Sagar Road, Shimoga Dist., 577 204, Karnataka, India.

Email: chethan.ls@pestrust.edu.in, paishwarya623@gmail.com, tschandana03@gmail.com, ganavibrganu@gmail.com, gowthamid120846442@gmail.com

Abstract

The rise of deep fake technology has ignited widespread societal apprehensions about potential security risks and the dissemination of false information. Despite extensive research into deepfake detection, effectively discerning low-quality deepfakes and simultaneously identifying variations in their quality remains a significant and formidable challenge. This investigation explores the dynamic field of deep fake detection, focusing specifically on video analysis targeting facial manipulations. The study introduces Celeb-DF, a substantial dataset comprising high-quality deep fake videos of celebrities, challenging prevailing detection methods. Additionally, a revolutionary Quality-Agnostic Deep Fake Detection (QAD) framework addresses the intricate task of simultaneously recognizing diverse qualities of deep fakes, surpassing established benchmarks across multiple datasets. The paper highlights ongoing efforts to enhance deep fake detection strategies, incorporating advanced models such as Stable Diffusion, and employing interpretability-through-prototypesn by merging fine-tuned Vision Transformers with Support Vector Machines.

Keywords -- Deep fake technology, security risks, deep fake detection, Celeb-DF dataset, video analysis, Quality-Agnostic Deep Fake Detection (QAD), Stable Diffusion, Vision Transformers, Support Vector Machines.

I. INTRODUCTION

The widespread adoption of deepfake technology has raised serious concerns regarding the authenticity and reliability of digital media. This research tackles the pressing need for reliable deepfake detection as media manipulation becomes more accessible and pervasive. There have been numerous cases of false information being spread through synthetic content, showing its ability to mislead large audiences and undermine trust in social media platforms. Additionally, there has been an increase in deepfake-related theft and fraud, with the impact reaching into areas such as virtual reality and the creation of false memories.

To address these challenges, deep learning has proven to be an effective method for detecting and analyzing visual irregularities in media, offering a promising solution to combat the risks of deepfakes. This paper presents an approach using Vision Transformers to differentiate between deepfake images created by diffusion models and genuine ones. Custom datasets, incorporating various deepfake generation methods, were developed to train models, improving their ability to distinguish fake content from authentic media. The study also highlights the significance of model interpretability, utilizing Support Vector Machines (SVM) and eXplainable Deep Neural Networks (xDNN) classifiers to gain insights into the decision-making processes of deepfake detection systems.

Simultaneously, the rapid advancement of AI technologies, especially deep neural networks (DNNs), has enabled the production of highly convincing fake media, including images, videos, and synthetic voices. The rise of deepfake creation, driven by methods like Autoencoders, Variational Autoencoders, and Generative Adversarial Networks, has increased the risk of misinformation and raised significant ethical issues. A prominent example is the creation of deepfake videos featuring former U.S. Presidents, which has sparked conversations about the potential dangers posed by this technology.

The rapid advancement of AI technologies, especially deep neural networks (DNNs), has enabled the creation of highly convincing fake media, including images, videos, and synthetic voices. The increasing use of deepfake generation methods such as Autoencoders, Variational Autoencoders, and Generative Adversarial Networks has amplified the risks of misinformation and raised significant ethical concerns. Prominent cases, such as deepfake videos involving former U.S. Presidents, have sparked debates about the potential dangers of this technology.

Acknowledging the ethical, security, and privacy risks associated with deepfakes, there is a critical need for effective detection techniques. To develop these techniques, high-quality datasets are essential. This paper addresses the limitations of current deepfake datasets, particularly their lack of multimodal content, by introducing a new dataset: the Audio-Video Multimodal Deepfake Detection dataset, FakeAVCeleb. This dataset incorporates both video and audio deepfakes, offering a valuable resource for assessing and improving deepfake detection methods. The study also provides a detailed benchmark analysis, evaluating 11 different baseline methods on various popular deepfake datasets and demonstrating the significance of FakeAVCeleb.

II LITERATURE REVIEW

In this survey, we delve into the dynamic landscape of deep fake detection, focusing on cutting-edge methodologies and advancements in the field. Our exploration encompasses a curated selection of seminal papers obtained from reputable sources such as Google Scholar, IEEE Xplore, and Scopus. By meticulously examining these publications, we aim to distill key insights, innovations, and challenges in the realm of deep fake detection, contributing to a comprehensive understanding of this critical area in modern technology.

The research paper titled "Deepfake Video Detection Using Deep Learning" provides a thorough examination of deep fake video detection employing advanced deep learning techniques. The authors conducted comprehensive training and evaluation of eight deep fake video classification models, leveraging four distinct fake video generation methods and incorporating two state-of-the-art neural networks—Xception and MobileNet. The primary focus of the study was on the detection accuracy for both fake and real videos, particularly emphasizing the performance of models trained with NeuralTextures. Notably, the results revealed that the models exhibited satisfactory classification performance, achieving an overall fake detection accuracy exceeding 90%. Noteworthy distinctions were observed, with Xception models excelling in detecting real videos over fake ones, while the NeuralTextures model stood out with a 91% true positive rate and an 86% true negative rate. The MobileNets model also demonstrated strong performance, surpassing 90% detection accuracy for videos on specific platforms. The paper delved into the implementation of a voting mechanism, enabling the collaborative use of four models for the detection of diverse video types generated by different fake video methods. The authors underscored potential future exploration avenues, including investigating different loss functions and optimizers, along with comparing model performance between whole face and partial facial feature training. Emphasizing the importance of inter-frame pattern correlations in video-oriented detection techniques, the study concluded by suggesting the development of a user-friendly interface to enhance accessibility and interest, facilitating swift results from the model [1].

The research paper titled "Enhancing Deepfake Detection via Prototypical Interpretability in Diffusion Models" explores a novel approach to deepfake detection by leveraging fine- tuned Vision Transformers and Support Vector Machines. The core focus of the methodology is to enhance interpretability through the use of prototypes, leading to a more robust and accurate detection of deepfakes. Furthermore, the paper addresses a notable gap in the availability of open datasets for deepfake detection by curating custom datasets for thorough evaluation. The authors validate the efficacy of their proposed method across diverse datasets and offer insights into the decision-making process by incorporating explainability techniques. This paper contributes valuable perspectives to the advancement of deepfake detection methods, emphasizing the significance of interpretability and the creation of open datasets in this evolving field [2].

The paper titled "Quality-Agnostic Deepfake Detection with Intra-model Collaborative Learning" introduces an innovative approach to tackle the detection challenge posed by deepfakes of diverse qualities. Emphasizing the escalating threat of deepfakes and recognizing the limitations of current detection methods, particularly in identifying low-quality instances, the authors present a Quality-Agnostic Deepfake (QAD) detection framework. This framework employs intra- model collaborative learning, demonstrating superior performance compared to existing baselines across various quality levels. The paper underscores the importance of deepfake detection in addressing security, privacy, and societal concerns, highlighting the QAD framework as a promising solution. The potential real-world applications of the proposed method are emphasized, and the need for further research in this evolving domain is acknowledged. Overall, the QAD framework represents a substantial advancement in deepfake detection, providing an effective and scalable solution for the detection of deepfakes with varying qualities [3].

The paper titled "Integrating EfficientNet and Vision Transformers for Face-based Deepfake Detection" introduces an innovative method for identifying deepfakes on facial images through the synergy of Vision Transformers and a convolutional EfficientNet B0. The research showcases the effectiveness of hybrid convolutional-transformer networks in deepfake detection, achieving top-tier results without relying on distillation techniques from convolutional or ensemble network-based models. The authors propose a novel architecture, termed Convolutional Cross ViT, which adeptly captures both local and global details, underscoring the significance of multi-scale analysis in discerning image manipulations. Additionally, a straightforward yet impactful voting scheme is introduced for managing multiple faces in videos during the inference phase, resulting in marginally superior and consistent outcomes compared to previous methodologies. In summary, this study contributes valuable insights into the potential of combining EfficientNet and Vision Transformers for video- based deepfake detection, presenting a promising strategy to address the complexities associated with detecting manipulated content [4]

The paper presents Celeb-DF, a large-scale challenging dataset for DeepFake forensics. The dataset contains high-quality DeepFake videos of celebrities, and it evaluates DeepFake detection methods and datasets to demonstrate the escalated level of challenges posed by Celeb-DF. The paper compares the performance of various DeepFake detection methods using the inference code and published pre-trained models. The results show that Celeb-DF is the most challenging dataset for DeepFake detection methods, and their overall performance on Celeb-DF is lowest across all datasets. The paper also discusses the refinements to the synthesis algorithm that improve the visual qualities of the DeepFake videos in the Celeb-DF dataset. The Mask-SSIM score is used as a referenced quantitative metric of visual quality of synthesized DeepFake video frames. The paper concludes by highlighting the implications of the emergence of AI-synthesized face-swapping videos, such as DeepFakes, on the trustworthiness of online information [5].

The paper presents a new audio-video multimodal deepfake dataset called FakeAVCeleb, which is designed to address the emerging threat of impersonation attacks using deepfake audios and videos. The dataset contains 1,000 deepfake videos and 1,000 corresponding real videos of 100 celebrities, with both audio and video modalities. The paper also evaluates the performance of several state-of-the-art deepfake detection methods on this dataset and compares it to existing deepfake datasets. The results show that the latest state-of-the-art detection models have achieved mediocre or low detection performance on FakeAVCeleb, in contrast to their high detection performance on existing deepfake datasets. The paper concludes by discussing the potential applications of deepfake detection technology and providing a dataset request form for researchers interested in using FakeAVCeleb [6].

This paper discusses the use of Shapley Additive Explanations (SHAP) to gain new insights into spoofing and deepfake detection. The authors demonstrate the efficiency and flexibility of the tool, making it applicable to a variety of architecture models and related applications. They also reveal unexpected classifier behavior and differences in the behavior of competing spoofing detection models. The paper highlights the need for explainable artificial intelligence in the field of spoofing and deepfake detection and advocates for the broader adoption of SHAP and similar tools. Overall, the paper provides valuable insights and information for researchers and practitioners working in the field of spoofing and deep fake detection [7].

The paper titled "Cross-Forgery Analysis of Vision Transformers and CNNs for Deepfake Image Detection" addresses the challenges of detecting manipulated images and videos, known as deepfakes, created using advanced Deep Learning techniques. Deepfakes, posing a threat to truth and credibility, require robust detection methods. The authors focus on employing Vision Transformers and Convolutional Neural Networks (CNNs) for deepfake detection, conducting experiments on the ForgeryNet dataset. Results reveal that Vision Transformers exhibit superior generalization and reduced bias towards specific anomalies introduced by diverse deepfake generation techniques. Conversely, CNNs, notably the EfficientNet model, demonstrate specialization in detecting deepfakes generated using known techniques. The paper emphasizes the importance of diverse approaches in deepfake detection and advocates for the evaluation of different solutions to build robust, enduring systems capable of detecting deepfakes generated through unpublished methods. Overall, the paper provides valuable insights into the challenges and potential solutions for deepfake detection using deep learning architectures [8].

The paper titled "Undercover Deepfakes: Detecting Fake Segments in Videos" delves into the realm of deepfake detection, particularly focusing on the identification of fake segments within videos. The search results reveal that the paper explores the use of neural textures for image synthesis and deferred neural rendering, emphasizing the generation of realistic textures in real-time. Additionally, it references studies on face capture and reenactment of RGB videos, involving the real-time manipulation of facial expressions. The search results also highlight the mention of GAN-based facial editing for forgery detection and segmentation. Various deepfake detection models and techniques, such as artifact detection and collaborative feature learning, are discussed, indicating a comprehensive exploration of the field. Attention mechanisms and transformers for image recognition at scale are also referenced. The search results contribute to an understanding of the challenges and techniques in media forensics, with specific papers addressing pairwise interaction learning, exposing deepfakes using inconsistent head poses, and multi-attentional deepfake detection. Furthermore, an ablation study on varying window sizes for temporal segmentation suggests optimal results with a window size of 5 and an overlap of 4. Collectively, these findings provide valuable insights into the ongoing efforts in deepfake detection and related methodologies within the realm of computer vision and pattern recognition [9].

The paper "LipForensics: In the Wild" proposes a novel approach for detecting forged face videos, called LipForensics. This method leverages rich representations learned via lipreading to target inconsistencies in semantically high-level mouth movements. The key contributions of LipForensics include achieving state-of-the-art generalization to unseen forgery types and demonstrating significant robustness to various common corruptions. The authors emphasize the importance of meeting both of these objectives for face forgery detection in real-life scenarios. The paper also acknowledges the financial support received and the institution where the studies were conducted. The paper "LipForensics: In the Wild" compares its approach to existing systems for detecting forged face videos. The authors note that current deep learning-based methods often rely on low-level artifacts that are specific to the forgery method used, making them vulnerable to common post-processing operations. Additionally, these methods often struggle to generalize to unseen forgery types and exhibit poor robustness to common corruptions. The paper cites several existing systems, including DeepFakes, which is a popular face- swapping tool that has been used to create many forged videos. Other existing systems include MesoNet, which uses a deep convolutional neural network to detect manipulated images and videos, and XceptionNet, which uses a deep neural network to detect face tampering [10].

The paper "Implicit Identity Driven Deepfake Face Swapping Detection" introduces a novel approach for detecting face swapping in deepfake images. The proposed method leverages both explicit and implicit identities to effectively distinguish between real and fake faces. The explicit identity contrast loss and implicit identity exploration loss are key components of the framework, enabling the embedding of face images into the implicit identity space. Through extensive experiments and evaluations, the proposed method demonstrates superior performance compared to state-of-the-art approaches, particularly in cross-dataset and cross-manipulation evaluations. The framework's ability to generalize and differentiate between real and fake samples is highlighted, showcasing its potential for practical applications in detecting manipulated images [11].

III. PROPOSEDFRAMEWORKSAND METHODOLOGIES

This paper introduces the Quality-Agnostic Deepfake Detection (QAD) framework to tackle the complex challenge of detecting deepfakes of varying qualities. Utilizing intra-model collaborative learning, QAD achieves outstanding performance by identifying both high- and low-quality deepfakes within a single model. The paper emphasizes the framework's advantage over existing models, showcasing its ability to handle different quality levels effectively. With its scalable and efficient approach, QAD makes a significant contribution to the evolving field of deepfake detection, providing a strong solution to combat the growing threat of deepfake content.

This paper presents the Quality-Agnostic Deepfake Detection (QAD) framework to address the complex challenge of detecting deepfakes with varying levels of quality. By utilizing intra-model collaborative learning, QAD achieves outstanding performance in detecting both high and low-quality deepfakes within a single model. The framework’s superiority over existing benchmarks is highlighted, demonstrating its effectiveness in handling a range of quality variations. Offering a scalable and efficient solution, QAD significantly advances the field of deepfake detection, providing a strong defense against the increasing spread of deepfake content. Additionally, the paper introduces the Critical Forgery Mining (CFM) framework, which focuses on improving the generalization and robustness of face forgery detection. By incorporating fine-grained triplet learning and relation learning prototypes, CFM boosts detection accuracy. Addressing the limitations of existing methods, CFM demonstrates cutting-edge forgery detection capabilities. The paper underscores the significance of detailed analysis and prototype-based learning, offering valuable contributions to the advancement of face forgery detection technologies

This paper presents Celeb-DF, a detailed dataset created to assess and enhance deepfake detection techniques. The dataset includes high-quality deepfake videos of celebrities, establishing a challenging benchmark for testing detection algorithms. By comparing different methods on Celeb-DF, the paper highlights the increased difficulty in identifying deepfakes within this dataset. Additionally, the paper addresses improvements in the synthesis algorithm, emphasizing the ongoing progression of deepfake technology and the continuous need for reliable detection methods.

The paper introduces the FakeAVCeleb dataset, which tackles the growing issue of deepfake audio and video in impersonation attacks. This innovative dataset includes both video and audio formats, offering a valuable resource for testing multimodal deepfake detection approaches. When evaluating leading models on FakeAVCeleb, the study reveals challenges and reduced detection accuracy compared to other datasets. The research highlights the importance of diverse datasets to improve the reliability and efficiency of deepfake detection across multiple modalities, contributing to the broader conversation on deepfake security risks.

This paper introduces a spatio-temporal fusion feature-based authentication approach to enhance the accuracy of deepfake face video detection. By tackling the complexities of detecting manipulated facial features in deepfake videos, the study improves detection methods. The spatio-temporal fusion technique offers a valuable solution to reduce the risks associated with the widespread use of deepfake face videos, advancing efforts to strengthen deepfake detection mechanisms.

This paper presents a novel method for detecting face swapping in deepfake images by leveraging both explicit and implicit identities. The proposed framework uses explicit identity contrast loss and implicit identity exploration loss, achieving outstanding performance in differentiating between real and fake faces. The study highlights the importance of embedding face images into an implicit identity space, enhancing the development of robust techniques for detecting deepfake face swapping. The focus on identity-driven detection offers a significant contribution to the growing field of deepfake detection research.

IV. KEY FINDINGS AND COMPARISONS

papers presented together provide a thorough summary of progress in deepfake detection and tampering identification techniques. Key insights from each paper include:

The QAD framework demonstrates exceptional capability in detecting deepfakes across varying qualities, offering improved performance over current benchmarks. This highlights the necessity for quality-agnostic methods to keep pace with the rapidly advancing deepfake technology.

CFM sets a new standard in forgery detection by utilizing fine-grained triplet learning and relation learning prototypes. The paper highlights the significance of in-depth analysis and prototype-based learning in enhancing face forgery detection techniques.

Celeb-DF presents a major challenge for deepfake detection, emphasizing the ongoing advancement of deepfake technology. This dataset acts as an important reference for assessing the effectiveness of detection algorithms.

The FakeAVCeleb dataset tackles the growing concern of deepfake audio and video content, offering a multimodal resource to assess detection techniques. The reduced detection accuracy on this dataset highlights the importance of diverse datasets in improving the reliability of detection methods.

The spatio-temporal method improves the effectiveness of detecting deepfake face videos. This approach plays a key role in advancing detection techniques to tackle the challenges presented by altered facial features in videos.

One approach utilizes a Transformer Block, combining multi-head attention and a feed-forward block to generate frame-level predictions for input videos. To reduce noise, a smoothing method using majority voting within a sliding window is applied. Another technique involves the Vision Transformer (ViT), which processes data by sequentially accumulating feature vectors for temporal segmentation. Performance is assessed using metrics such as Intersection over Union (IoU) and Area Under the ROC Curve (AUC) across various datasets. Additionally, a method applying a Multi-Layer Perceptron (MLP) head to ViT for frame classification proves effective for both temporal segmentation and video-level detection. The Vision Transformer Encoder, with its multi-head attention and feed-forward block, plays a crucial role in frame-level predictions. Together, these methods and frameworks contribute to the advancement of deepfake detection, highlighting innovations in attention mechanisms, temporal segmentation, and classification, and offering valuable insights into enhancing the field's accuracy and robustness.

The suggested method for detecting deepfake face swapping based on implicit identity demonstrates exceptional performance, highlighting the significance of embedding facial images into an implicit identity space [11].

V. TAMPER DETECTION

As security technologies continue to evolve, innovative methods for improving tamper detection have become a key area of research. Leveraging deep learning models, anomaly detection techniques, and sensor fusion approaches, these efforts tackle significant challenges in identifying various types of tampering, enhancing environmental resilience, and ensuring system dependability. By exploring a wide range of datasets, applying cutting-edge computer vision techniques, and integrating data from multiple sensors, ongoing research is contributing to the development of a robust framework that pushes the boundaries of current tamper detection methods. These advancements play a crucial role in reinforcing security across diverse and complex situations, demonstrating the transformative potential of these technologies within the broader field of security research.

The paper "Detection of Tamper Forgery Image in Security Digital Image" explores the growing challenges of maintaining image security in various industries, given the increasing ease of digital image manipulation. It highlights the urgent need for new techniques to detect image forgery in response to advancements in tampering methods. The importance of image security is stressed in fields like forensics and public safety, where the widespread use of digital imaging raises concerns about the authenticity of images. The paper discusses several methods for detecting tampered images, including both active techniques, which rely on pre-embedded data such as watermarks, and passive techniques like copy-move forgery detection and splicing. A comprehensive review of existing detection algorithms, such as logistic regression, interquartile range, and discrete Fourier transform, is provided, with an evaluation of their strengths and weaknesses. The paper also highlights common tampering techniques, such as copy-move and splicing, and stresses the need for more innovative detection solutions. It offers valuable insights into the challenges of image security and calls for the development of new detection methodologies to address evolving image manipulation practices [13].

The paper "Digital Image Tamper Detection Techniques - A Comprehensive Study" by Minati Mishra and Flt. Lt. Dr. M. C. Adhikary offers an in-depth examination of methods for detecting tampered digital images, focusing on the challenges posed by the ease with which digital images can be manipulated and the need for reliable detection techniques. The authors categorize these techniques into two main types: active detection methods and passive (blind) methods. They highlight the similarities between traditional photo manipulations and digital image tampering, stressing that digital images are much easier to alter. The paper also details common image manipulation techniques such as retouching, splicing, copy-pasting, cropping, cloning, and the use of steganography for covert data transmission.

The authors highlight the crucial role of photographs as reliable and influential forms of communication, stressing the importance of developing effective tamper detection methods to safeguard their authenticity. The paper explores the technical aspects of digital image tamper detection, offering a deeper understanding of the complexities involved in verifying the legitimacy of digital images. It also references the work of Siwei Lyu and Hany Farid, particularly their study "How Realistic is Photorealistic?", which contributes to the broader understanding of digital image manipulation. Overall, this paper serves as an essential resource for researchers, professionals, and anyone interested in the field of digital image tamper detection. It emphasizes the growing challenge of image manipulation and the need for robust detection methods to uphold the trustworthiness and authenticity of digital image [14].

The paper titled "Tamper Detection and Localization in Forensic Images" examines the essential area of forensic image analysis, with a particular focus on identifying and locating tampering. The authors explore various challenges related to maintaining the integrity of forensic images, addressing issues such as authenticity, manipulation, and the dependability of forensic evidence. The paper emphasizes the importance of strong tamper detection and localization methods to uphold the credibility of forensic images in legal and investigative contexts. It reviews current systems and methodologies, stressing the need for advanced technologies to improve tamper detection and localization capabilities. The authors highlight the rapidly evolving field of forensic image analysis and call for continued advancements and research to combat image tampering effectively and ensure the integrity of forensic investigations. Overall, the paper offers valuable perspectives on the complexities of tamper detection and localization in forensic images, contributing to the broader field of forensic science and its practical applications[15].

In the development of advanced security systems, key considerations include the choice between ResNet and SSD architectures for object detection, with an emphasis on utilizing diverse datasets and data augmentation to improve model training and enhance recognition of various tampering scenarios. Anomaly detection algorithms are integral, focusing on feature extraction for normal behavior, setting deviation thresholds, and adapting to new scenarios through dynamic learning. Sensor fusion plays a vital role, integrating data from multiple sensors, applying fusion algorithms for consensus, and minimizing false positives to ensure system reliability. To address current limitations, the proposed solution integrates a varied dataset that is resilient to tampering scenarios and strengthens environmental robustness through advanced computer vision techniques and data augmentation. By incorporating sensor fusion, the solution overcomes the limitations of single-source sensor systems, ensuring precise detection even in difficult situations. A real-time monitoring and alert system continually analyzes sensor data, enabling quick detection of tampered signs and eliminating response delays seen in some existing systems, leading to a more proactive and effective security framework. Overall, these combined strategies offer a comprehensive and reliable approach to enhancing security systems through deep learning, anomaly detection, and sensor fusion.

VI. CONCLUSION

The survey offers an in-depth review of recent developments in deepfake and tamper detection techniques. The studies discussed introduce innovative frameworks, datasets, and perspectives to tackle the rapidly changing landscape of deepfake technology. Key insights highlight the significance of quality-agnostic methods, prototype-driven learning, multimodal datasets, and spatio-temporal fusion in improving detection accuracy and effectiveness.

REFERENCES

[1]. D. Pan, L. Sun, R. Wang, X. Zhang and R. O. Sinnott, "Deepfake Detection through Deep Learning," 2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), Leicester, UK, 2020, pp. 134-143, doi: 10.1109/BDCAT50828.2020.00001.

[2]. A. Aghasanli, D. Kangin and P. Angelov, "Interpretable-through-prototypes deep fake detection for diffusion models," in 2023 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), Paris, France, 2023 pp. 467-474.
doi: 10.1109/ICCVW60793.2023.00053

[3]. Binh M. Le, Simon S. Woo "Quality-Agnostic Deepfake Detection with Intra-model Collaborative Learning" arXiv:2309.05911

[4]. Davide Coccomini, Nicola Messina, Claudio Gennaro, and Fabrizio Falchi," Combining EfficientNet and Vision Transformers for Video Deep fakeDetection" 2022

[5]. Y. Li, X. Yang, P. Sun, H. Qi and S. Lyu, "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 2020, pp. 3204-3213, doi: 10.1109/CVPR42600.2020.00327.

[6]. Khalid, Hasam, Shahroz Tariq and Simon S. Woo. "FakeAVCeleb: A Novel Audio-Video Multimodal Deepfake Dataset." ArXiv abs/2108.05080 (2021): n. pag.

[7]. W. Ge, J. Patino, M. Todisco and N. Evans, "Explaining Deep Learning Models for Spoofing and Deepfake Detection with Shapley Additive Explanations," ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, Singapore, 2022, pp. 6387-6391, doi: 10.1109/ICASSP43922.2022.9747476.

[8]. Coccomini, Davide & Caldelli, Roberto & Falchi, Fabrizio & Gennaro, Claudio & Amato, Giuseppe. (2022). Cross-Forgery Analysis of Vision Transformers and CNNs for Deepfake Image Detection. 52-58. 10.1145/3512732.3533582.

[9]. S. Saha, et al., "Undercover Deepfakes: Detecting Fake Segments in Videos," in 2023 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), Paris, France, 2023 pp. 415-425.
doi: 10.1109/ICCVW60793.2023.00048

[10]. A. Haliassos, K. Vougioukas, S. Petridis and M. Pantic, "Lips Don't Lie: A Generalisable and Robust Approach to Face Forgery Detection," in 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 2021pp.5037-5047.
doi: 10.1109/CVPR46437.2021.00500

[11]. B. Huang, et al., "Implicit Identity Driven Deep fake Face Swapping Detection," in 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Vancouver, B C, Canada,2023pp.4490-4499.
doi: 10.1109/CVPR52729.2023.00436

[12]. Juan Hu, Xin Liao, Difei Gao, Satoshi Tsutsui,Qian Wang, Zheng Qin, Mike Zheng Shou "Mover: Mask and

Recovery based Facial Part Consistency Aware Method for Deepfake Video Detection" arXiv:2303.01740

[13]. Mohammed Fakhrulddin Abdulqader, Adnan Yousif Dawod, Ann Zeki Ablahd,
Detection of tamper forgery image in security digitalmage, 2023, 100746, ISSN 2665-9174

[14]. Mishra, Minati & Adhikary, Munesh. (2013). Digital Image Tamper Detection Techniques - A Comprehensive Study.

[15]. Chroni, Maria & Katsi, Athanasia & Nikolopoulos, Stavros & Polenakis, Iosif & Vouronikos, Vasileios. (2023). Tamper Detection and Localization in Forensic Images. 117-122.
10.1145/3606305.3606317.