Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
International Conference on Emerging Trends in Design and Arts
May 2024 5(ICETDA24), 312–315

DEEPFAKE DILEMMA: A REVIEW STUDY ON VIDEO SYNTHESIS TECHNOLOGY

Akshat Kedawat[1], Dr. Aloke Das[2]

[1]Student, Animation and VFX Department, Poornima University, Jaipur, Rajasthan
[2]Associate Professor, Animation and VFX Department, Poornima University, Jaipur, Rajasthan

ABSTRACT

This review paper provides information of deepfake video technology, a rapidly evolving dimension of artificial intelligence with profound implication for media, privacy & Society.

Exploring the fundamental methods used to create deepfakes, this paper explores the advancements in machine leaning, particularly focusing on Generative Adversarial Networks (GAN)s & Neural Architecture Network responsible for hyper-realistic synthesis of facial expression, gestures and voices.

An important part of the investigation is devoted to ethical questions, asking whether deepfake technology might be used as a weapon to spread misinformation, steal identities, or invade privacy.

The impact on Society as a whole is highlighted in the report, along with the necessity for preventative actions to lessons the negative consequences of malicious deepfake distribution & the decline in public confidence in digital media

The review addresses the persistent challenges of detecting deepfake content, closely examine methodologies from traditional forensics to innovate machine leaning based approaches

Highlighting the Cat & mouse game between creators & Detectors, the paper discusses the limitations of existing detection methods & the urgent requirements for more advanced & expandable solution

Keywords: Deepfake, Face swapping, Video Synthesis, Detection, Ethics, Artificial Intelligence, Misinformation

Corresponding Author

Akshat Kedawat
Akshat.Kedawat@gmail.com

DOI
10.29121/shodhkosh.v5.iICETDA24.2024.2033

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The advent of deepfake technology has brought in a new paradigm that is both promising and dangerous in an era marked by rapid technical breakthroughs and the pervasiveness of digital media. The manipulation of audiovisual content has been revolutionized by deepfakes, which are powerful synthetic media made with artificial intelligence algorithms that allow for the seamless modification of faces, voices, and gestures in videos. Deepfakes present new prospects for narrative, entertainment, and the creation of digital material, but they also represent serious threats to privacy, security, and public confidence.

As a result of the widespread use of deepfake films, a complicated network of ethical, sociological, and technological issues known as the "deepfake dilemma" has emerged, supporting the conversation around this new technology. Deepfake technology, while pushing the limits of what is feasible in terms of digital content generation and manipulation, is on the one hand an incredible achievement of ingenuity. However, it also brings up serious issues about how it might be abused, manipulated, and how people's confidence in digital media could be damaged.

The goal of this review paper is to present a thorough analysis of the deepfake problem by concentrating on three main areas: video synthesis methods, detection difficulties, and ethical considerations. This paper aims to deepen our understanding of the complex interplay between technology and society in the digital age by examining the underlying methodologies driving deepfake synthesis, critically analysing the ethical considerations surrounding deepfake technology, and scrutinizing the ongoing difficulties in detecting synthetic content.

This review paper aims to clarify the complex nature of the deepfake dilemma by synthesizing recent research, critical analysis, and real-world examples. It also provides insights into the societal implications, ethical conundrums, and technological nuances that influence the conversation around deepfake technology. In the end, it is critical to approach the deepfake problem with caution, forethought, and a dedication to supporting ethical innovation in the digital sphere.

2. DEEPFAKE VIDEO GENERATION

Following the initial release of deepfake films, additional modification algorithms—the majority of which are based on generative networks—are frequently developed. Deepfake algorithms can be employed in these techniques to produce fake content that violates people's privacy and has a gravely negative impact on society. After reviewing the history of deepfake algorithm development, this part will discuss two different varieties of deepfake algorithms.

2.1 DEVELOPMENT OF DEEPFAKE TECHNOLOGIES

Face manipulation is not a freshly developed technology. The famous image of US President Abraham Lincoln from 1865 contains the first instance of facsimile in literature. The advancement of computer graphics technology has made it simple to manipulate digital images [12–14]. Advances in deep learning have led to a fundamental advancement in the field of face manipulation technologies. As stated by The two types of face modification algorithms that are now in use—facial swapping and face reenactment—can be attributed to their distinct objectives.

2.2 FACE SWAPPING

Videos that switch a person's identity between two videos, or face swapping, have gained popularity recently. Since 2017, related studies have been established. Convolutional neural networks (CNNs) were trained to detect the appearance of target identity from an unstructured photo collection in the study by Korshunova et al. [15]. This allowed the creation of high-quality face-swapping images. But since time continuity is ignored, this method cannot be used for the creation of high-quality videos. Olszewski et al. [16] presented an innovative method to create films using a source video sequence and a single RGB image in the same year. Using source textures and a single target texture, a deep generative network was trained to infer per frame texture deformations of the target identity. Using the schema of [17], the freshly produced face might be composited into the source footage based on this technique, replacing the original face.

In December 2017, a Reddit user shared the first face-swapping movie created using the deepfake technique, shocking people all over the world. Deepfake algorithms are widely believed to have been inspired by [15], where face-swapping images were created using CNNs.

3. METHODOLOGY

LITERATURESEARCHSTRATEGY

Use pertinent terms like "deepfake," "video synthesis," "deep learning," "detection," "ethics," and "societal implications" to conduct methodical searches throughout academic resources including PubMed, IEEE Xplore, ACM Digital Library, Google Scholar, and Scopus. Utilize Boolean operators to enhance search terms and guarantee that pertinent literature is included. To stay up to date on the most recent developments and insights in deepfake technology, retrieve peer-reviewed journal articles, conference papers, books, and authoritative reports that have been published within the last ten years.

INCLUSION AND EXCLUSION CRITERIA

Add research on video synthesis methods, difficulties with detection, and the moral implications of deepfake technology. Studies that don't clearly address the review paper's main themes or that lack scholarly rigor and empirical support should be disregarded.

DATA EXTRACTION AND SYNTHESIS

Systematically gather pertinent information, such as methodology, theoretical underpinnings empirical support, and important conclusions, from a chosen number of studies. Sort the retrieved data into themes that relate to the three main topics of the review paper: ethical considerations, detection difficulties, and video synthesis methods. Integrate research

results to detect recurring themes, contradictions, and gaps in the body of knowledge. Utilize narrative synthesis strategies to combine many points of view and produce logical narratives that offer thorough insights into the deepfake conundrum.

CRITICAL ANALYSIS AND INTERPRETATION

Analyse the synthesized literature critically in order to assess the advantages and disadvantages of various approaches to video synthesis, detection strategies, and ethical frameworks. Determine which parts of the literature are in agreement and disagreement, emphasizing the areas that need for more investigation. Analyze results in light of wider societal ramifications, moral issues, and policy and practice ramifications. Provide complex analyses and theoretical ideas that advance our knowledge of the deepfake conundrum and its ramifications for society, technology, and ethics.

ETHICAL CONSIDERATIONS

Respect intellectual property rights and perform literature evaluations in accordance with ethical standards that guarantee openness, honesty, and integrity. Recognize that the chosen literature may contain biases, and make an effort to provide a fair and impartial assessment of the deepfake conundrum. Take into account the moral ramifications of sharing knowledge regarding deepfake technology, making sure to interact and communicate with stakeholders in an ethical manner.

4. CONCLUSION

Deepfake technologies—which rely on deep learning—have been evolving at a never-before-seen rate in recent years. Because the Internet is so widely used, malicious face-manipulated films produced by deepfake algorithms have the potential to spread quickly and jeopardize both individual privacy and social stability. In order to lessen the detrimental effects that deepfake films have on individuals, business enterprises and research organizations around the world are carrying out pertinent studies. In this In this post, we first describe the deepfake video generating technology, then we analyse the current detection technology, and last, we talk about the direction that future research should go. This study places special emphasis on promising research and the issues that exist with current detection techniques. This review places special emphasis on robustness and generalization. We hope that academics working on deepfake detection will find this paper beneficial.

In this paper, we provide a novel deep learning approach that can reliably differentiate artificial intelligence (AI)-generated false videos (Deepfake Videos) from authentic videos. Our approach is Based on the findings that the Deepfake algorithm as it exists now can only produce images with a certain resolution; these images must then undergo additional processing in order to match the faces that need to be substituted in the original movie. These transformations leave behind some unique artifacts in the final Deepfake Videos, which a specialized deep neural network model can efficiently capture. We test our method using multiple sets of publicly available Deepfake Videos, demonstrating its practical efficacy.

As Deepfake's technology advances, we'll keep enhancing the detecting technique. Initially, we aim to assess and enhance the resilience of our detection technique in the face of numerous video compressions.Second, we would like to investigate a specific network structure for the detection of Deepfake movies in order to achieve more efficient detection than the predesigned network structure (such as resent or VGG) that we presently use for this task.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Chesney, B., Citron, D.: Deep fakes: a looming challenge for privacy, democracy, and national security. Calif. L. Rev. 107, 1753 (2019)

Dixon, H.B., Jr.: Deepfakes: More frightening than photoshop on steroids. Judges J. 58(3), 35–37 (2019

Neekhara, P., et al.: Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. arXiv preprint arXiv:2002.12749. (2020)

Thies, J., et al.: Face2face: real-time face capture and reenactment of RGB videos. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2387–2395 (2016)
Kim, H., et al.: Deep video portraits. ACM Trans. Graph. 37(4), 1–14 (2018)
Zhou, P., et al.: Two-stream neural networks for tampered face detection. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2017)
Dolhansky, B., et al.: The deepfake detection challenge (DFDC) preview dataset. arXiv preprint arXiv:1910.08854. (2019)
Amerini, I., et al.: Deepfake video detection through optical flow-based CNN. Proceedings of the IEEE International Conference on Computer Vision Workshops (2019)
Li, Y., Lyu, S.: Exposing deepfake videos by detecting face warping artifacts. arXiv preprint arXiv:1811.00656. (2018)
Dang, H., et al.: On the detection of digital face manipulation. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern recognition, pp. 5781–5790 (2020).
Güera, D., Edward, J.: Delp: Deepfake video detection using recurrent neural networks. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–6. IEEE (2018)
Zhao, Y., et al.: Capturing the persistence of facial expression features for deepfake video detection. In: International Conference on Information and Communications Security, pp. 630–645.Springer (2019)
Z. Lu, Z. Li, J. Cao, R. He, and Z. Sun. Recent progress of face image synthesis. arXiv:1706.04717, June 2017.
Dufour, N., Gully, A.: Deepfakes Detection Dataset (2019)
Carlini, N., Farid, H.: Evading deepfake-image detectors with white-and black-box attacks. arXiv preprint arXiv:2004.00622. (2020)