Mini Review
Volume 12:2, 2023

Journal of Telecommunication System and Management

ISSN: 2167-0919 Open Access

Survey on Fake Data Generation and Detection in Telecommunications

Moras Haker*

Department of Network and Computer Security, University of New York, New York, USA

Abstract

Deep learning advances and the availability of free, large databases have enabled even non-technical people to manipulate or generate realistic facial samples for both benign and malicious purposes. Deep fakes are face multimedia content that has been digitally altered or created synthetically using deep neural networks. The paper begins by describing readily available face editing apps as well as the vulnerability of face recognition systems to various face manipulations. The following section of this survey provides an overview of recent deep fake and face manipulation techniques and works. Four types of deep fake or face manipulations are specifically discussed: identity swap, face re-enactment, attribute manipulation, and entire face synthesis.

Keywords: Digital face manipulations • Digital forensics • Multimedia manipulations

Introduction

It is estimated that 1.8 billion images and videos are uploaded to online services each day, including social and professional networking sites. However, 40% to 50% of these images and videos appear to be manipulated for benign or adversarial purposes. Human face image/video manipulation, in particular, is a serious issue endangering the integrity of information on the Internet and face recognition systems, as faces play a central role in human interactions and biometrics-based person identification. As a result, plausible manipulations in face samples can severely undermine trust in digital communications and security applications. Deep Fakes are multimedia files that have been digitally altered or created synthetically using deep learning models. Deep fakes are expected to take current disinformation and misinformation sources to the next level, which could be exploited by trolls, bots, conspiracy theorists, hyper partisan media, and foreign governments; thus, deep fakes could be fake news 2.0. Deep fakes can be used for productive purposes such as realistic dubbing of foreign video films or historical figure reanimation for educational purposes. Deep fakes can also be used for destructive purposes, such as blackmailing or damaging a person's reputation with fake pornographic videos, manipulating elections, creating warmongering situations, inciting political or religious unrest with fake speeches, causing financial market chaos, or identity theft. It is easy to see that the number of malevolent deep fake exploitations vastly outnumbers the benevolent ones [1,2].

Literature Review

Additionally, open challenges and potential future directions (e.g., robust deep fake detection systems against adversarial attacks using multistream and filtering schemes) in this evolving field of deep fakes are highlighted. The primary goals of this article are to supplement previous survey papers with recent advances, to provide the reader with a more in-depth understanding of the deep fake creation and detection domain, and to use this article as ground truth to develop novel algorithms for deep fake and face manipulation generation and detection systems. There is a dearth of work on the interpretability and dependability of the deep fake detection framework. Most deep-learning-based deep fake or face manipulation detection methods in the literature do not explain why the final detection outcome occurred. It is primarily because deep learning techniques are a black box in nature. Deep fake or face manipulation detectors currently available only provide a label, confidence percentage, or fake ness probability score, but not an insight description of the results. Such a description would be useful in understanding why the detector made a particular decision. Deep fake or face manipulation can also be used for either benign or malicious purposes. Nonetheless, current deep fake or face manipulation detection techniques can't tell the difference [3].

Numerous methods for detecting deep fake and face manipulation

A systematic analysis, however, reveals that the majority of them have low generalisation capability, i.e., their performances plummet when they encounter a novel deep fake/manipulation type that was not used during the training stage, as demonstrated in. Prior research also viewed deep fake detection as a reactive defence mechanism rather than a battle between attackers (i.e., deep fake generation methods) and defenders (i.e., deep fake detection methods). As a result, there is a significant disconnect between academic deep fake solutions and real-world scenarios or requirements. For example, the preceding works typically lag in terms of system robustness against adversarial attacks, decision explain ability, and real-time mobile deep fake detection and there are numerous methods for detecting deep fake and face manipulation.

In recent years, the study of deep fake generation and detection has gained much more traction in the computer vision and machine learning communities. There are some review papers on the subject, but they are primarily concerned with deepfake or synthetic samples using generative adversarial networks. Furthermore, most survey articles were written from an academic perspective rather than a practical development perspective. They also did not cover the introduction of very recent face manipulation methods as well as new deep fake generation and detection techniques. As a result, this paper provides a concise but comprehensive overview from both theoretical and practical perspectives in order to provide the reader with an intellectual grasp and to facilitate the advancement of novel and more resilient techniques [4-6].

Discussion

Deep fakes, or AI-generated or digitally manipulated face samples, pose a significant threat to the dependability of face recognition systems and the integrity of information on the Internet. This paper provides an overview of recent advances in the generation and detection of deep fake and facial manipulation. Despite noticeable progress, several issues remain to be addressed in order to

***Address for Correspondence:** Moras Haker, Department of Network and Computer Security, University of New York, New York, USA, E-mail: haker231@gmail.com*

Received: 02 February, 2023, Manuscript No. jtsm-23-93231; **Editor assigned:** 03 February, 2023, Pre QC No. P-93231; **Reviewed:** 16 February, 2023, QC No. Q-93231; **Revised:** 21 February, 2023, Manuscript No. R-93231; **Published:** 28 February, 2023, DOI: 10.37421/2167-0919.2023.12.368

achieve highly effective and generalised generation and defence techniques. Thus, this article discussed some of the open challenges and research opportunities. Deep fake detection frameworks, which will require interdisciplinary research efforts in various domains such as machine learning, computer vision, human vision, psychophysiology, and so on, have a long way to go in the field. Overall, this survey could be used to develop novel AI-based algorithms for deep fake generation and detection. It is also hoped that this survey paper will inspire aspiring scientists, practitioners, researchers, and engineers to pursue deep fakes as a field of study.

Conclusion

One illustration gained from these 2 investigations is that the subtleties matter. Apparently minor contrasts in system can produce significant contentions. Contrasts in concentrate on plan, procedural technique, and factual examinations can cause stamped contrasts in concentrate on discoveries. As imagers, we can take an example from the playbook of our partners in interventional cardiology, who at a beginning phase had normalized definitions for clinical results and procedural achievement. Interestingly, we as imagers have not for the most part adopted this strategy. This lack is featured in the 2 examinations in this issue of JACC wherein a precise methodology with a beginning point in the coronal view will definitely bring about confounding discoveries that can be genuinely broke down yet not essentially demon.

Acknowledgement

None.

Conflict of Interest

There are no conflicts of interest by author.

References

1. Juefei, Xu, Felix Run Wang, Yihao Huang and Qing Guo, et al. "Countering malicious deepfakes: Survey, battleground, and horizon." *IJCV* 130 (2022): 1678-1734.
2. Huang, Wenjing, Shikui Tu and Lei Xu. "IA-FaceS: A bidirectional method for semantic face editing." *Neural Netw* 158 (2023): 272-292.
3. Segura, David, Emil J. Khatib, Jorge Munilla and Raquel Barco. "5G numerologies assessment for URLLC in industrial communications." *Sensors* 21 (2021): 2489.
4. Khalid, Waqas, Heejung Yu, Rashid Ali and Rehmat Ullah. "Advanced physical-layer technologies for beyond 5G wireless communication networks." *Sensors* 21 (2021): 3197.
5. Ranyal, Eshta, Ayan Sadhu and Kamal Jain. "Road condition monitoring using smart sensing and artificial intelligence: A review." *Sensors* 22 (2022): 3044.
6. He, Jiang and Paul K. Whelton. "Elevated systolic blood pressure and risk of cardiovascular and renal disease: overview of evidence from observational epidemiologic studies and randomized controlled trial." *Sensors* 138 (1999): 211–219.

How to cite this article: Haker, Moras. "Survey on Fake Data Generation and Detection in Telecommunications." *J Telecommun Syst Manage* 12 (2023): 368.