

Deepfake Detection through Deep Learning

Prof. Chavan Sir¹, Jayesh S. Pathade², Prajwal D. Khandge³,

Nayan N. Khairnar⁴, Yuvraj N. Kamble⁵

Professor, Department of Computer Engineering¹

Students, Department of Computer Engineering^{2,3,4,5}

SKN Sinhgad Institute of Technology and Science, Kusgaon (BK), Pune, Maharashtra, India

Abstract: Deepfakes allow for the automatic generation and creation of (fake) video content, e.g. through generative adversarial networks. Deepfake technology is a controversial technology with many wide reaching issues impacting society, e.g. election biasing. Much research has been devoted to developing detection methods to reduce the potential negative impact of deepfakes. The results suggest that while deepfakes are a significant threat to our society, political system and business, they can be combatted via legislation and regulation, corporate policies and voluntary action, education and training, as well as the development of technology for deepfake detection, content authentication, and deepfake prevention. The study provides a comprehensive review of deepfakes and provides cyber security and AI entrepreneurs with business opportunities in fighting against media forgeries and fake news. Generations and the results were realistic. Moreover, we implemented a DeepFake Detector XceptionNet with minor modifications which achieved 95% accuracy on detecting DeepFakes. At last, we implemented a newly introduced technique in which the DeepFake generation is perturbed through which it can easily fool the deepfake detector..

Keywords: DeepFakes, Image Animation, DeepFakes Generations, Detection of DeepFakes, GANS, Adversarial Attacks, Fooling DeepFake Detectors

REFERENCES

- [1]. Deepfake Detection through Deep Learning, Deng Pan, Lixian Sun, Rui Wang, Xingjian Zhang, Richard O. Sinnott. 2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies https://www.researchgate.net/publication/348033118_Deepfake_Detection_through_Deep_Learning
- [2]. Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Nießner, "Face2face: Real-time face capture and reenactment of rgb videos," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 2387–2395
- [3]. A. Bansal, S. Ma, D. Ramanan and Y. Sheikh, "Recycle-GAN: Unsupervised Video Retargeting", Computer Vision – ECCV 2018, pp. 122-138, 2018. Available: <https://arxiv.org/pdf/1808.05174.pdf>. [Accessed 10 July 2020].
- [4]. Xunyu Pan, Xing Zhang, and Siwei Lyu, "Exposing image splicing with inconsistent local noise variances," in 2012 IEEE International Conference on Computational Photography, 2012, pp. 110.
- [5]. P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Two-stream neural networks for tampered face detection," in 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, 2017, pp. 1831-1839: IEEE.
- [6]. Blinking," in 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, 2018, pp. 1-7: IEEE.
- [7]. X. Yang, Y. Li, and S. Lyu, "Exposing deep fakes using inconsistent head poses," in ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019, pp. 8261-8265: IEEE.
- [8]. H. Li, B. Li, S. Tan, and J. Huang, "Detection of Deep Network Generated Images Using Disparities in Color Components," arXiv preprint :07276, 2018.
- [9]. S. McCloskey and M. Albright, "Detecting GAN-generated Imagery using Color Cues," arXiv preprint rXiv:08247, 2018.



IJARSCT

Impact Factor: **6.252**

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, November 2022