Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

#BN-46-Cyber and space as key enablers-Feb2021

DUAL-USE ASPECTS OF DEEPFAKE

Authors: Bita Afshar[1] and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Of particular interest in the domain of dual-use technologies is actually the dual-use aspects of deepfake technology. The advantages and disadvantages of employing deepfake are being investigated and analyzed.
- The consequences and potential threats due to the misuse of deepfake have been investigated and analyzed carefully. In addition, all the counteractive measures associated with different parts of the society such as government, private companies and sectors, and people are being studies, evaluated, and investigated.

CONTEXT

- The Deepfake phrase is a combination of two words “Deep learning” and “Fake”. Deepfake refers to a fake photo, video, voice, text, or story which is created by the powerful techniques of artificial intelligence and machine learning [1-2].
- Similar to other kinds of dual-use technologies, Deepfake technology provides benefits as well as threats. Since deepfake has a dual-use characteristic, the harmful application of this technology should be identified carefully and seriously [1-2].
- Deepfake technology can be employed in a number of beneficial applications including the film industry, healthcare, education, and entertainment. However, it is mostly and mainly known for its malicious usages [4]. A few examples of positive use of Deepfake are:
    - It can eliminate language barriers by synchronizing mouth and facial movements with the translated speech [3].
    - This technology has healthcare applications from producing virtual chemical molecules to generating fake brain MRI scans [3].
    - Art world can also benefit from this technology. Movie-making industry uses deepfake techniques for producing special and challenging effects [4].
- On the other hand, many specialists have raised alarms that deepfake will threaten the national security, democracy, and privacy since it has been mostly employed in spreading false and incorrect information such as [6]:
- The misuses can create political and religious tensions and conflicts among countries. One of the most concerning application of deepfake is fabricating politicians’ speech which can potentially raise serious political issues [6,7].
- It has the potential to manipulate election results or leads to chaos in financial and stock markets [1].
- It can change the outcome of a military engagement by generating fake satellite images and misguide military experts and commanders [1].
- Another serious concern is the impact of deepfake technology on the criminal justice system. Fake videos can be presented in the criminal trials as evidence and judges can be misguided and wrongly influenced [5].

CONSIDERATIONS

- To address potential risks of harmful deepfake applications, various public, official, and private organizations should collaborate with one another.
- To prevent harmful results of deepfake technology several advanced computational approaches are proposed such as Convolutional Neural Network and Recurrent Neural Network architectures [8,9].
  - There are certain unique characteristics which can support researchers to detect fake videos more easily. The differences between the spectral response graphs of genuine and fake videos can provide information for deepfake detection [9].
  - The Blockchain trust is another solution for increasing the accountability. In this approach multiple people, organizations and institutions with great reputation will approve the genuineness of information [10].
  - Embedding watermarks in images and videos is also another potential remedy and solution. To some extent data could be protected if a hidden watermark is devised on images or videos [11].
- The social media companies undeniable contributions to counteracting user's misinformation as private sectors can be achieved by instituting and enforcing information sharing policies [8].
  - Specifically, Facebook has started a new policy which bans publishing edited or synthesized videos that are created by artificial intelligence and cannot be easily recognized [12].
  - Twitter, Tik Tok, and Reddit are other platforms and social media that take a similar approach to prevent spreading of misinformation which have affected civic activities and operations such as elections [13,14].
- People should also be well-informed on the deepfake threats. If they have enough knowledge and media literacy not only they can recognize particular flaws in deepfake but also, they can take the responsibility of sharing the information [15].
- The significant role of law and policy makers in protecting individual cyber rights is undeniable. Generally, technology has a faster development rate and evolves at a higher rate than the associated laws that makes it vulnerable to be misused [16].
  - The Copyright Infringement, Defamation, Violation of Privacy, Appropriation of Personality, and Human Rights Complaints are a few examples of law violations that are applicable in producing deepfake [16].
  - Legal measures can be very crucial remedy for tackling these serious challenges, however, it is very complicated to control and guard the internet. For example, in China publishing deepfake and fake news is considered as a criminal offense [16,17].

RECOMMENDATIONS

- The advanced machine learning libraries that are developed by najor companies such as Google, Microsoft, and Amazon, to name a few, should not be made available to the public. These companies can provide access to these special machine learning libraries to university researchers, governments or authorized private companies.
- To establish an organization with special and unique software to validate the encrypted watermarks that appear in media and social platforms.
- Cyber utopia can be the final resolution to end all anonymous harmful unsecure activities. Each piece of information has been verified before its transmission. The user identity is associated with a real identity that implies in the virtual reality everyone has a valid and confirmed identity. Since every piece of information could be tracked from the origin to its final destination violating the stated rules, laws, and policies will be reduced significantly.

REFERENCES

1-Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2019). Deep learning for deepfakes creation and detection. *arXiv preprint arXiv:1909.11573*.

2-https://futurumresearch.com/research-notes/deepfake-technology-ecosystem/

3-https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/#166319812f84

4-Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, *9*(11).

5-https://qz.com/1660737/deepfakes-will-influence-the-2020-election/

6- Amritha Jayanti, Raina Davis, Chris Wiggins, Joan Donovan. (2020). Tech factsheets for policymakers. Deepfakes.

7-https://election.ctvnews.ca/how-deepfakes-could-impact-the-2019-canadian-election-1.4586847

8-https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/

9- Pishori, A., Rollins, B., van Houten, N., Chatwani, N., & Uraimov, O. (2020). Detecting Deepfake Videos: An Analysis of Three Techniques. *arXiv preprint arXiv:2007.08517*.

10-https://theconversation.com/deepfake-videos-could-destroy-trust-in-society-heres-how-to-restore-it-110999

11-https://www.axios.com/the-impending-war-over-deepfakes-b3427757-2ed7-4fbc-9edb-45e461eb87ba.html

12-https://www.washingtonpost.com/technology/2020/01/06/facebook-ban-deepfakes-sources-say-new-policy-may-not-cover-controversial-pelosi-video/

13-https://www.axios.com/deepfakes-big-tech-policy-facebook-reddit-tiktok-ca7a99b8-e571-4b0b-933a-27e4b2c0b0f7.html

14-https://www.cnbc.com/2020/02/04/twitter-unveils-new-rules-to-tackle-deepfakes-ahead-of-2020-election.html

15- Diakopoulos, N., & Johnson, D. (2019). Anticipating and addressing the ethical implications of deepfakes in the context of elections. *New Media & Society*, 1461444820925811.

16- Black, R., Tseng, P., & Wong, S. (2018). What can the law do about 'Deepfake'?. *McMillan Litigation and Intellectual Property Bulletin*.

17-https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality.