They developed what?!? #Deepfake

Maxime Raafat

Computational Science & Engineering, ETH Zurich 2021

What is deepfake?

Deepfake: emerging AI driven method for synthetic media content creation, wherein a generator fits someone's facial attribute or other features onto another's.

Main applications

- Video or audio manipulation for entertainment use cases (e.g., the film industry). An inspiring example is shown in the bottom right video[1]
- Virtual bot improvement (e.g., voice assistants such as Apple's Siri)
- Voice (or potentially vision) recovery for mute (resp. blind) people

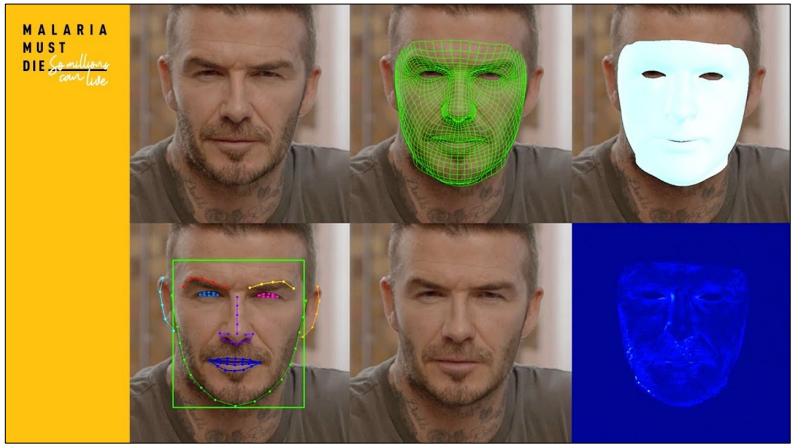
How are they developed : usually through GANs (Generative adversarial networks), algorithms consisting of 2 neural networks training against each other and improving each other alternately.
One (generative) network generates a new image sample, the other (discriminative) network tries to determine whether the image is real or fake. Both networks train until the discriminator can't tell fake from real. By design, GANs are extremely powerful and allow to create digital content undiscernible from reality.

The ethical issues

In the last few years, deepfakes have started being accessible to the general public through open-source libraries, and have therefore shown disastrous consequences on society, by harming individual's privacy and identity and by changing our perception of reality.

In 2020, nonconsensual pornography made up 96% of deepfakes deployed on the Internet, disproportionally targeting women[2] (thus violating all 4 key components of the (bio-)ethical principlist approach).

Access to seemingly unlimited information and cheap computational power gives anyone the ability to create fully new false information.



Deepfake, at what cost?

Misuse of technology: technology is often the result of human curiosity and does not necessarily fulfill a need. Although fueling the span of our comprehension, innovation can however have undesired and negative outcomes. Identity stealing, cybercrime or "revenge porn" are drastic side effects of technology being in wrong hands; the beneficial applications of deepfake might therefore not justify its development in the first place.

How to prevent deepfake misuse

- Implementation of measures and regulations, penalizing deepfakes misuse if not employed under certain conditions
- Development of fake-information detectors (ironically, again through the help of AI)
- Inform and sensitize the population through an educational system or advertising campaigns

Conclusion

Ethical by design: although ethical interrogations might seem to inhibit research and development in the first place, their purpose rather serve the involved stakeholders by highlighting the flaws or aspects to improve in any kind of technology.

Despite having disastrous side effects, algorithms similar to deepfake could lead to very different results with revolutionary effects on society.

References

[1] Malaria Must Die (2019, April 9), David Beckham speaks nine languages to launch Malaria Must Die Voice Petition. Retrieved from https://www.youtube.com/watch?v=QiiSAvKJlHo

[2] Sally Adee (2020, April 29), What Are Deepfakes and How Are They Created? Spectrum. Retrieved from https://spectrum.ieee.org/tech-talk/computing/software/what-are-deepfakes-how-are-they-created

ETH zürich