



Ministry of Science and Higher Education of the Republic of Kazakhstan
L.N. Gumilyov Eurasian National University

Faculty of Information Technology
Department of Information Systems

Deepfake

Done by: Yerassyl Iskakov

CHECKED BY: PROF. ZHUKABAYEVA T.K.

WHAT IS A DEEPFAKE?

Deepfake technology is a type of artificial intelligence used to create convincing fake images, videos and audio recordings. The term describes both the technology and the resulting bogus content and is a portmanteau of deep learning and fake.

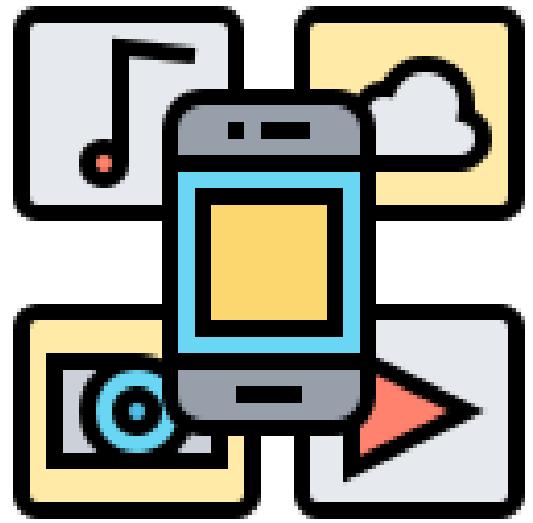
Deepfakes often transform existing source content where one person is swapped for another. They also create entirely original content where someone is represented doing or saying something they didn't do or say.

Deep learning + Fake = Deepfake

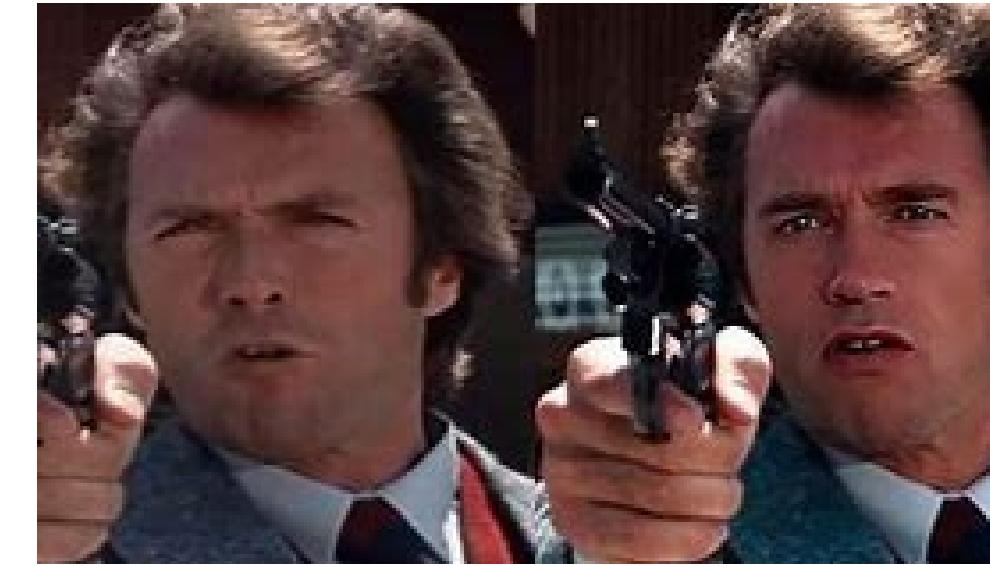


Example

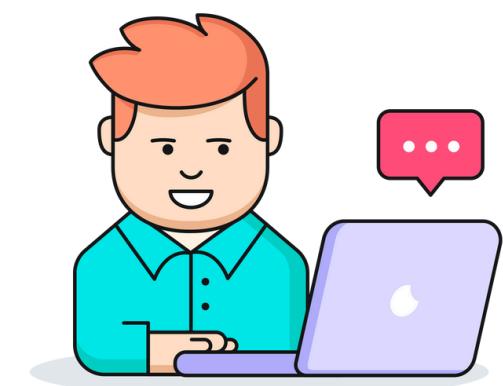
APPLICATIONS OF DEEPFAKE



Entertainment



FilmoGraphy



Education



METHODS TO DETECT DEEPFAKES



Which one is deepfake?

- Unusual or awkward facial positioning.
- Unnatural facial or body movement.
- Unnatural coloring.
- Videos that look odd when zoomed in or magnified.
- Inconsistent audio.
- People who don't blink.

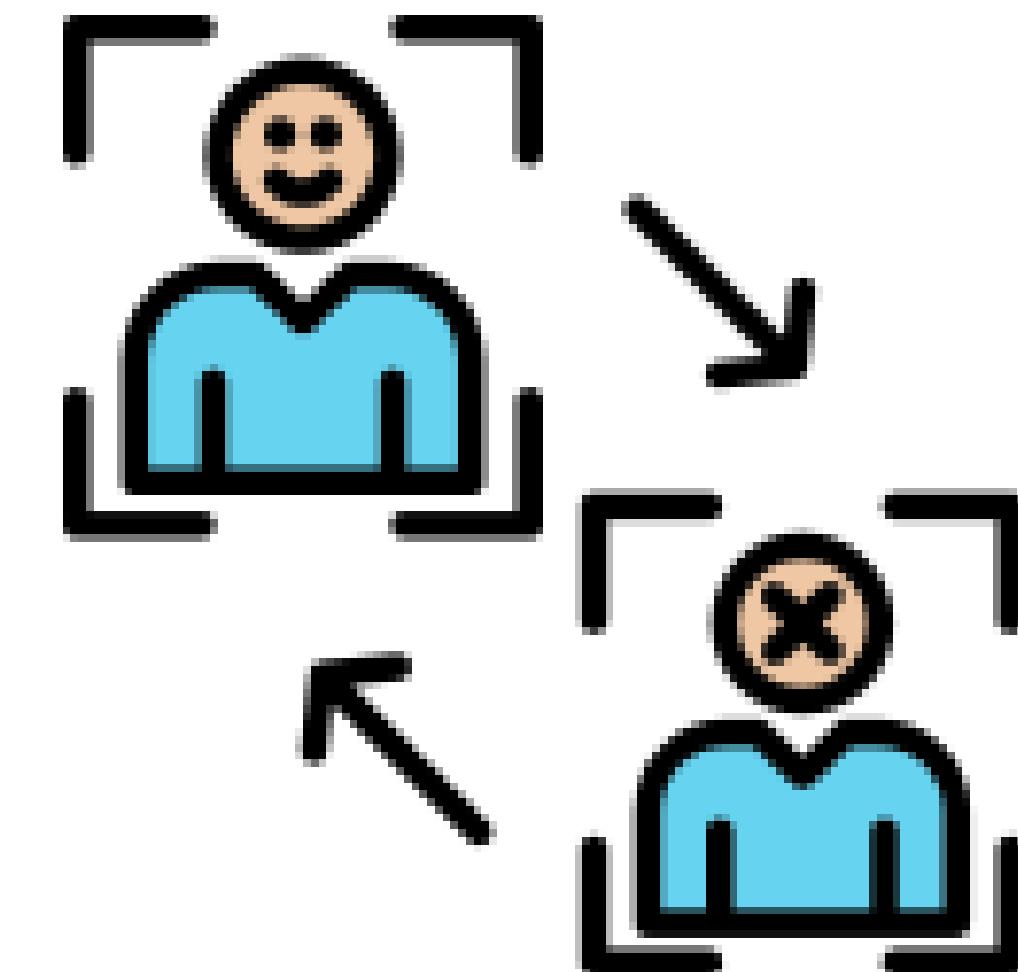
- Tiny deviations in the reflected light in the eyes of the subject.
- The aging of the skin doesn't match the aging of the hair and eyes.
- Glasses either have no glare or have too much and the glare angle stays the same despite the person's movements.

DEEPFAKE TECHNIQUES AND TECHNOLOGIES

- Source video deepfake – alters a person's face, movements, or speech in an existing video.
- Face swap – replaces one person's face with another in a video.

Technologies to create

1. GAN neural network technology uses generator and discriminator algorithms to develop all deepfake content.
2. Convolutional neural networks analyze patterns in visual data. CNNs are used for facial recognition and movement tracking.
3. Autoencoders are a neural network technology that identifies the relevant attributes of a target such as facial expressions and body movements, and then imposes these attributes onto the source video.
4. Natural language processing is used to create deepfake audio. NLP algorithms analyze the attributes of a target's speech and then generate original text using those attributes.
5. High-performance computing is a type of computing that provides the significant necessary computing power deepfakes require.
6. Video editing software isn't always AI-based, but it frequently integrates AI technologies to refine outputs and make adjustments that improve realism.

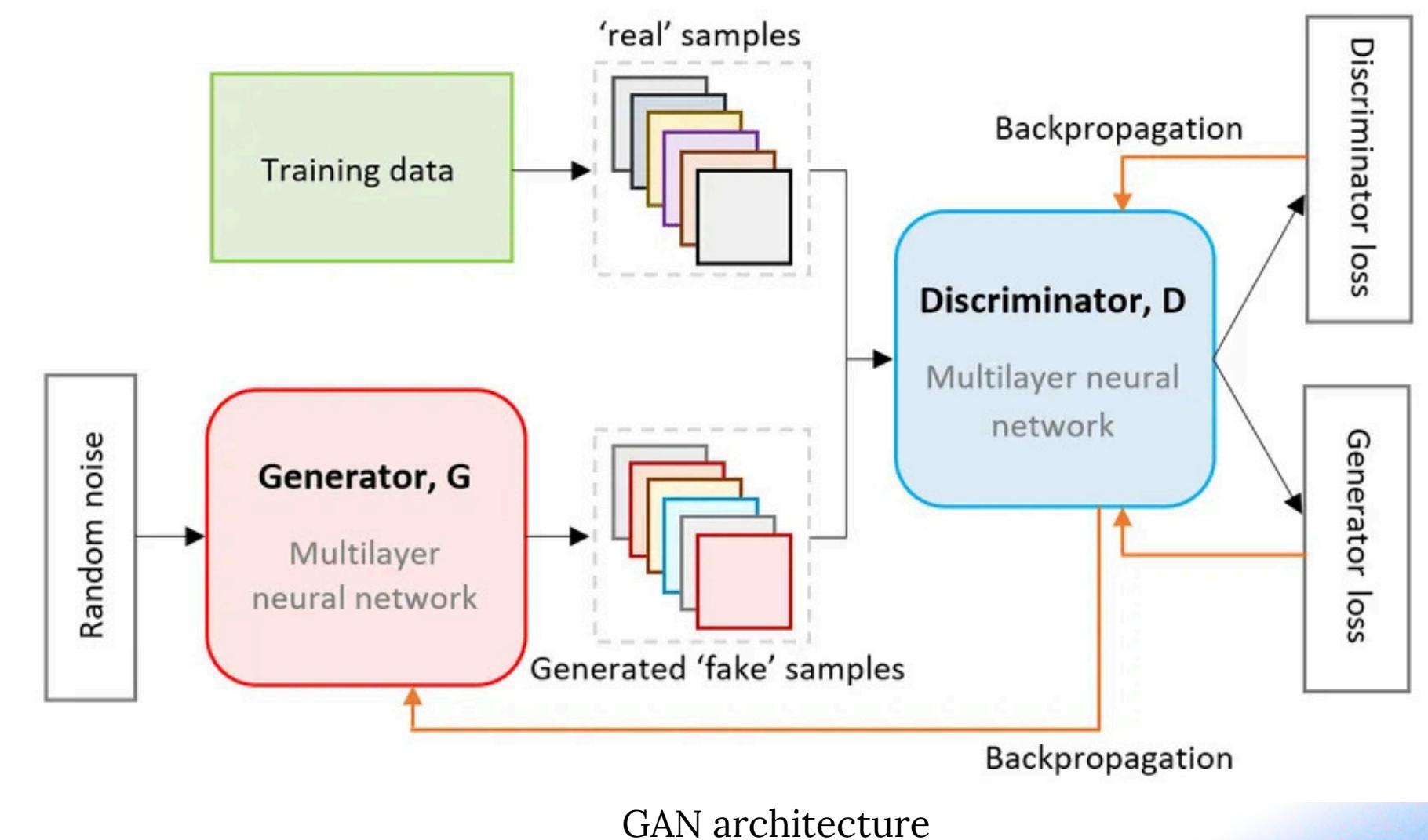


HOW DEEPFAKES WORK?

- Uses two AI algorithms – Generator (creates fake content) and Discriminator (detects flaws).
- Trained using Generative Adversarial Networks (GANs) – GAN refines deepfakes by learning patterns from real images and videos.

Process of Deepfake Creation:

1. GAN learns patterns from real data (images, videos, or audio).
2. The generator creates a fake version.
3. The discriminator detects flaws and sends feedback.
4. The generator improves until the fake is highly realistic.



RISKS AND ETHICAL CONCERNS



Misinformation, Fake news



Fraud and Theft:



Privacy Issues

Scarlett Johansson warns of 'AI misuse' after fake Kanye video

A deepfake video purported to show Jewish celebrities including Johansson protesting about Kanye West.

Culture



AI Brad Pitt dupes French woman out of €830,000

Anne, 53, was subject to nationwide ridicule after a TV show revealed how she paid out huge sums to romance scammers pretending to be Brad Pitt.

Europe



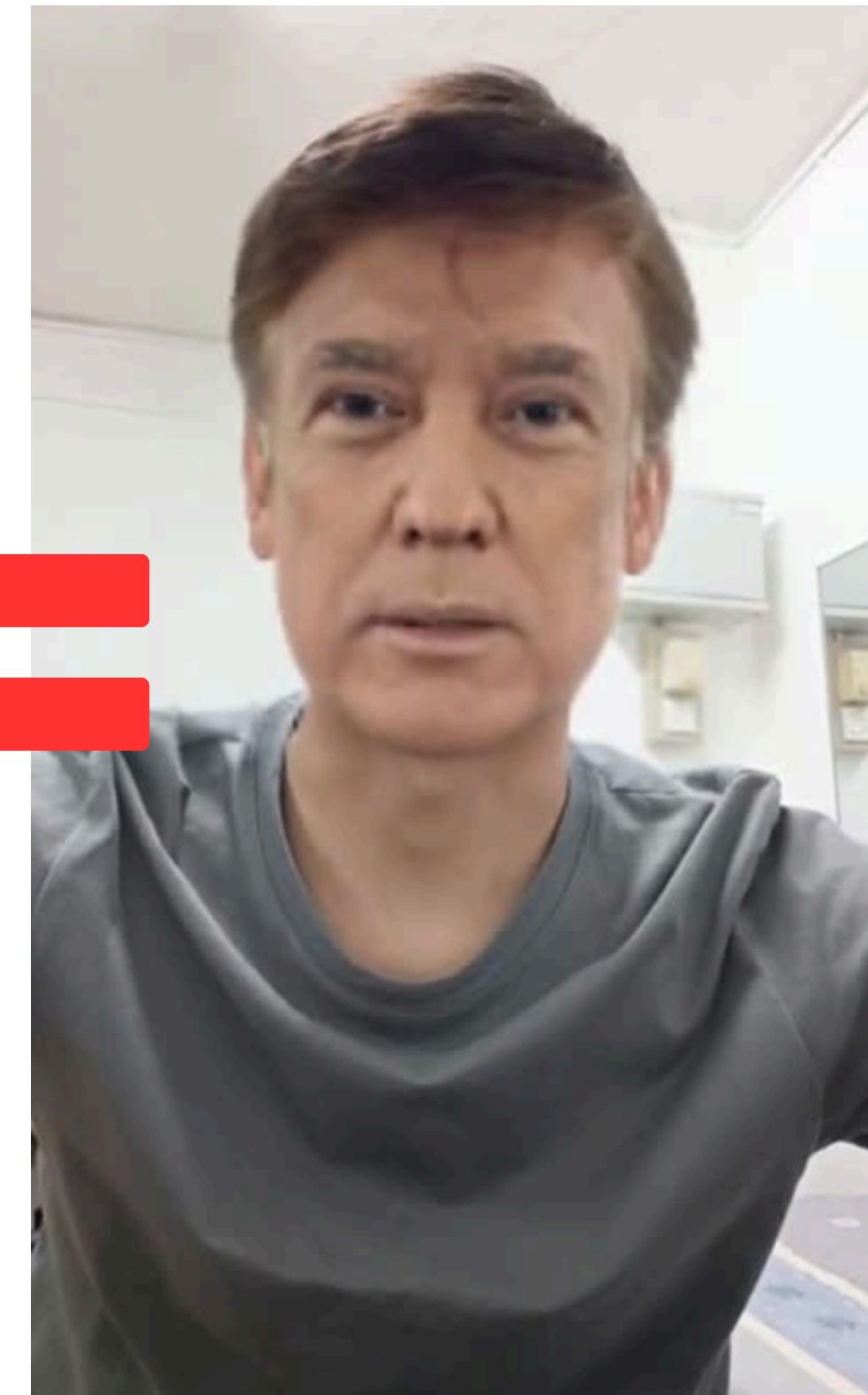
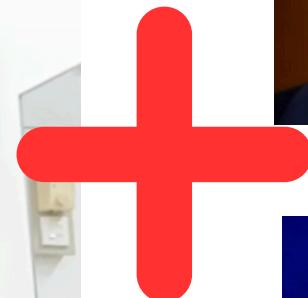
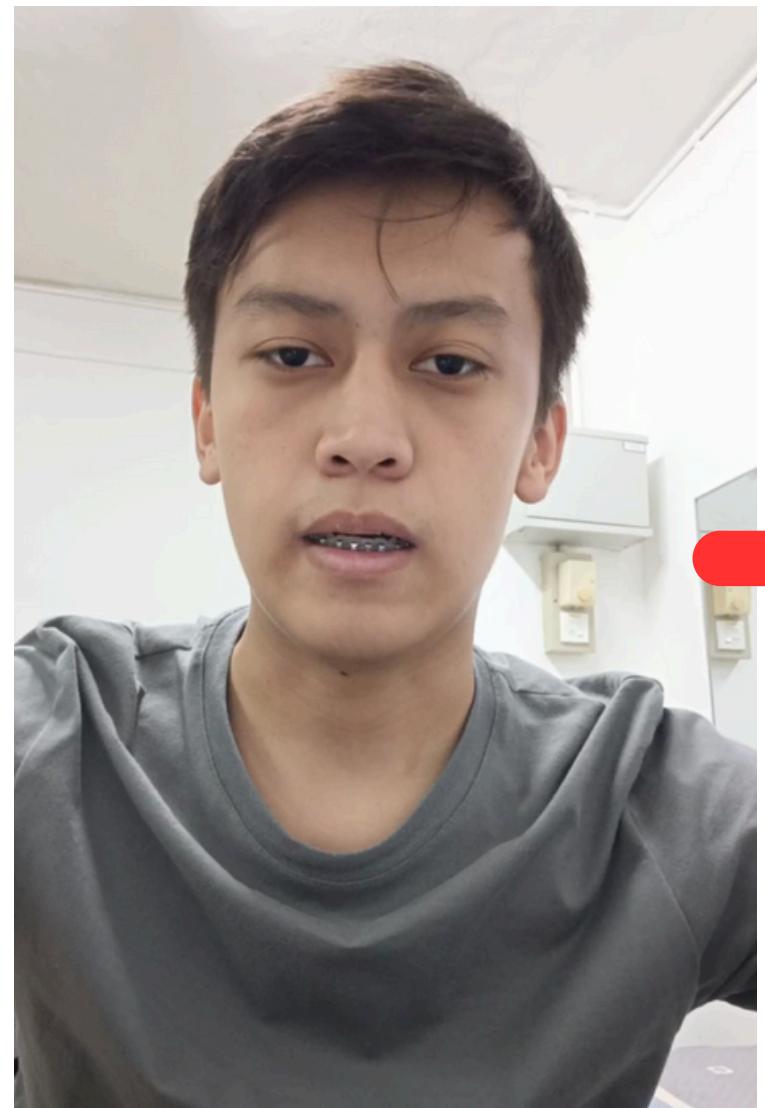
Governments not protecting press freedom, report says

Governments are failing to protect journalism from political attacks, according to Reporters Without Borders.

World



EXAMPLES



<https://huggingface.co/spaces/tonyassi/video-face-swap>

<https://github.com/Yerassyl04/CompVision>

CONCLUSION



Deepfake technology has revolutionized content creation by enabling hyper-realistic video and audio manipulation. While it offers innovative applications in entertainment, it also raises serious ethical concerns, including misinformation, fraud, and privacy risks. As deepfake technology continues to advance, stronger regulations, detection tools, and public awareness will be essential in mitigating its misuse. Balancing innovation with ethical responsibility is key to ensuring deepfakes are used for positive and constructive purposes.

REFERENCES

1. <https://spectrum.ieee.org/what-is-deepfake>
2. <https://www.bbc.com/news/topics/crm5plqk980t>
3. <https://www.techtarget.com/whatis/definition/deepfake>
4. <https://www.britannica.com/technology/deepfake>

THANKS FOR ATTENTION!

WHAT ?
