L.N. Gumilyov Eurasian National University
Faculty of Information Technology
Department of Information Systems

Deepfake

2025

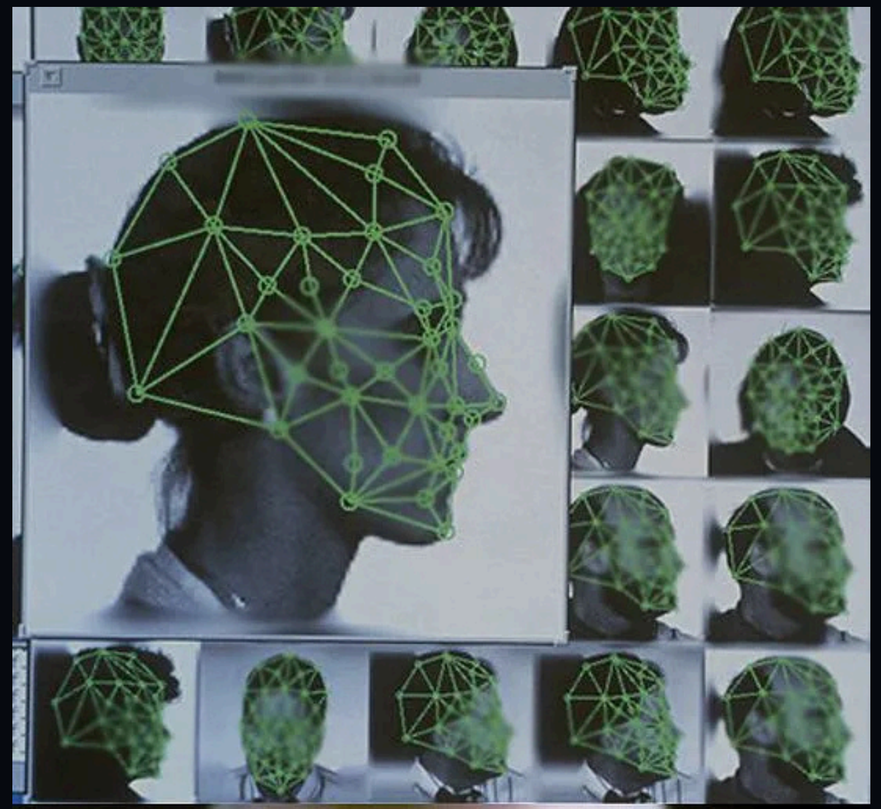
MUSTAFA ZHANSAYA

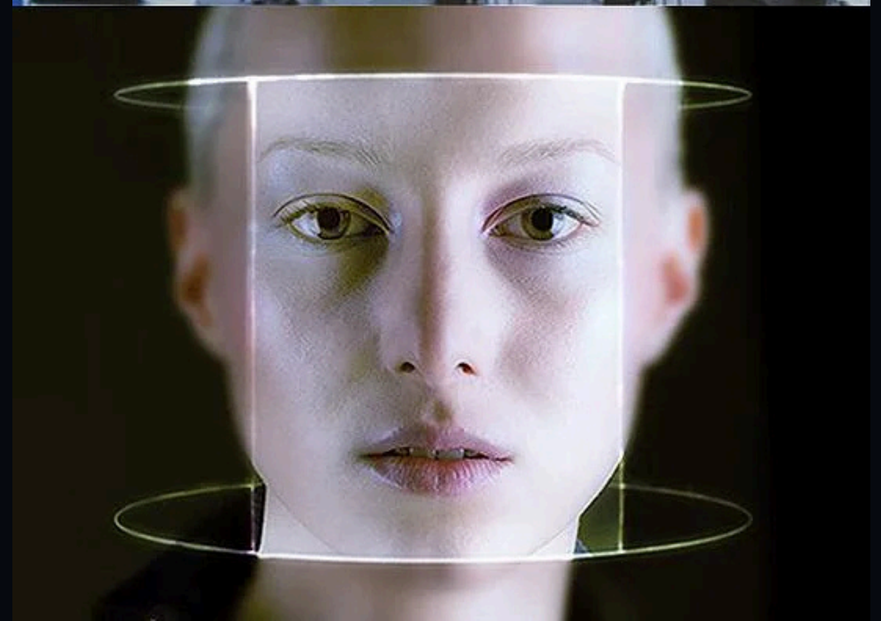
Deepfake is a state–of-the-art technology based on artificial intelligence that allows you to create fake media files such as images, videos, and audio with a high degree of realism. She uses deep learning to change a person's appearance, voice, and movements, making the manipulations almost invisible to the naked eye.

The term "Deepfake" combines two concepts: "deep learning" and "fake". The technology has both useful and malicious applications, from the film industry and digital avatars to spreading false information and threatening data security.

The concept of deepfakes (or deepfaking) can be traced back to efforts starting in the 1990s, when researchers used CGI in attempts to create realistic images of humans. The technology gained traction in the 2010s, when the availability of large datasets, developments in machine learning, and the power of new computing resources led to major advances in the field.

A true point of no return for deepfakes is attributed to the 2014 breakthrough in deep learning unveiled by Ian Goodfellow and his team. Goodfellow introduced the machine learning concept known as Generative Adversarial Network (GAN). Eventually, GAN would enable the next generation of highly sophisticated image, video, and audio deepfakes.





HOW IT WORKS

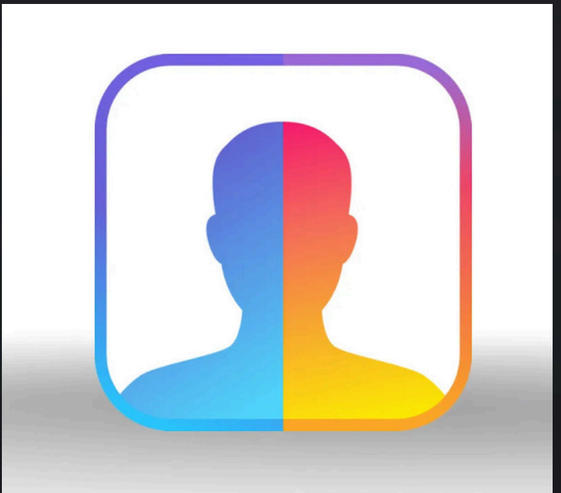
Deepfake technology utilizes machine learning algorithms trained on images or videos of a person. The primary mechanism behind it is Generative Adversarial Networks (GANs), which consist of two neural networks:

1. Generator – Creates fake images.
2. Discriminator – Evaluates their authenticity and helps improve their quality.

Key Steps in Creating a Deepfake:

- Data collection – The AI model is trained on a large number of photos and videos to accurately reproduce a person's appearance.
- Model training – The system analyzes facial features, voice, and movements to create a realistic fake.
- Video synthesis – The fake face is overlaid onto a video with another person, synchronizing it with expressions and voice.

💻 Popular Deepfake Software: FakeApp, DeepFaceLab, ZAO, Avatarify, Reface.



APPLICATIONS

Dangerous & Illegal Uses:

❌ Misinformation & Fake News – Creating false video statements of public figures.

❌ Fraud & Cybercrime – Identity theft and blackmail using fake videos.

❌ Political Manipulation – Spreading fake videos to influence public opinion.

ENTERTAINMENT & FILM INDUSTRY

- Replacing actors in movies (e.g., Paul Walker in Fast & Furious 7).
- Enhancing visual effects and de-aging characters.

SOCIAL MEDIA & MOBILE APPS

Apps like Reface, Avatarify, and FaceApp allow real-time face swapping.

MARKETING & ADVERTISING

- Personalized ads featuring virtual models.
- AI-generated influencers (e.g., Lil Miquela).

EDUCATION & SCIENCE

- Virtual teachers and historical figures in educational videos.
- Training professionals in medicine and law through simulations.

WAYS TO DETECT & PREVENT DEEPFAKE

AI Detection Tools – Companies develop AI-based tools to spot fakes (e.g., Microsoft Video Authenticator).

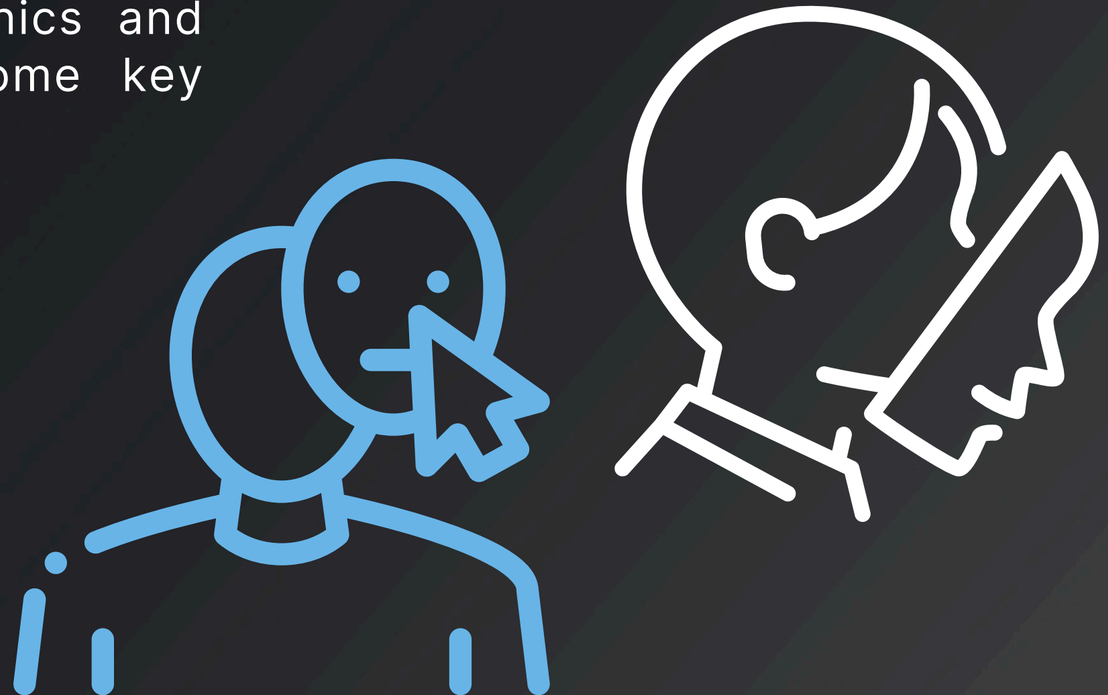
Legal Regulations – Some countries have introduced laws against malicious deepfake use.

Digital Watermarks – Implementing hidden markers in media files to verify authenticity.

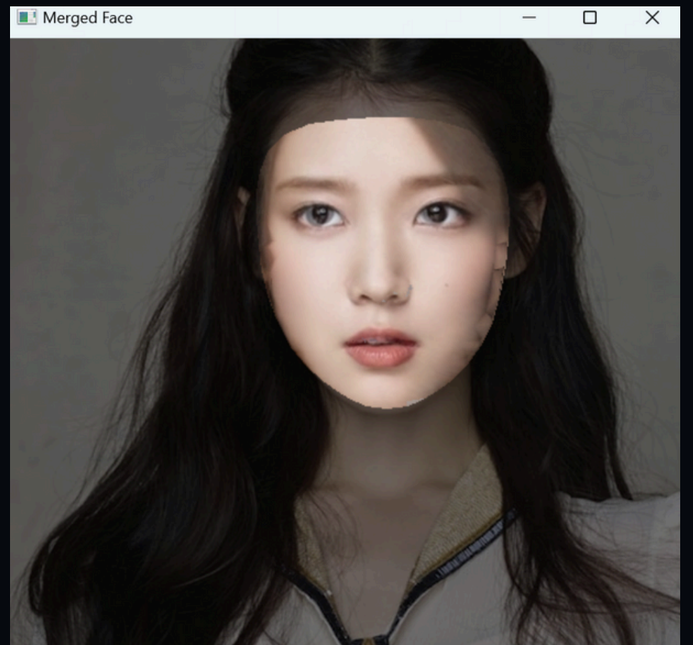
Public Awareness & Education – People should learn to recognize deepfake and critically assess media content.

CONCLUSION

The Deepfake technology is rapidly evolving, creating not only innovative opportunities but also significant challenges for society. It can be used to manipulate videos, audio, and images, posing threats to privacy, security, and trust in information. Combating its negative consequences requires stricter control, responsible usage, and the implementation of detection tools. Ethics and regulation of Deepfake technology must become key aspects of its development.



EXAMPLE



THANK YOU

FOR YOUR ATTENTION