Increase YourSkills

DEEPFAKES

How Artificial Intelligences Abuse Our Trust

TABLE OF CONTENTS

WHAT ARE DEEPFAKES?

A look at what is behind
this form of artificial intelligence

Deepfake [ˈdiːpˌfeɪ̯k] – a neologism made up of “deep learning” and “fake”.

It describes a method of manipulating images, videos or audio formats using artificial intelligence so that the human eye or ear can hardly distinguish the fakes as such. Deepfakes are created with the help of neural networks – such as GAN. If fed with a sufficiently large data set, these networks can predict what other data of the same type might look or sound like.

WHAT IS GAN?

GAN – short for Generative Adversarial Networks – is a network consisting of two algorithms. One algorithm forges an image (forger) while the other algorithm tries to detect the forgery (investigator). If the investigator succeeds in identifying the forgery, the forger learns from it and constantly improves. This process is also called deep learning.

THE DANGERS OF DEEPFAKES

The technology – which began in 2014 – has steadily expanded and improved. By 2017, the technology reached the point where the first videos could be produced. This led internet users to exploit deepfakes to manipulate pornographic content, which was first made available on the internet platform Reddit. These videos consisted of celebrities depicted in compromising situations.
According to a study by Sensity (then known as Deeptrace), 96% of all deepfake videos in 2019 were pornographic and exclusively concerned women.

With time, more and more YouTube channels were created to deceive people. From 2018 to 2020, the number of fake videos doubled every six months, reaching more than 85,000 in December 2020. Fakes of politicians, actors and other public figures began to see the light of day.

Hao Li, a deepfake expert, has warned that we will soon no longer be able to identify deepfakes as fakes. The problem, however, is not the technology itself but the lack of means to recognise these fakes.

The truth in this statement was revealed in a programming competition initiated by Facebook AI in 2019. The group developed a dataset of 124,000 videos, eight face-modification algorithms and associated research papers. But even the best competitors only achieved a detection rate of just over 65%.

There have been numerous cases worldwide that demonstrate the power of deepfake technology, with many of these examples having a political motivation behind them.

There have been numerous cases worldwide that demonstrate the power of deepfake technology, with many of these examples having a political motivation behind them.

One particularly frightening example involved X Gonzáles, a strong advocate for stricter gun laws in the USA. Gonzáles is a survivor of the Parkland school massacre and gained international recognition for her emotional speech at a memorial service following the event. Opponents of further gun legislation defamed Gonzáles in a video depicting her tearing up the American Constitution. In the original video, she tears up a target.

HOW ARE DEEPFAKES CREATED?

From A (Avatarify) to Z (Zao)

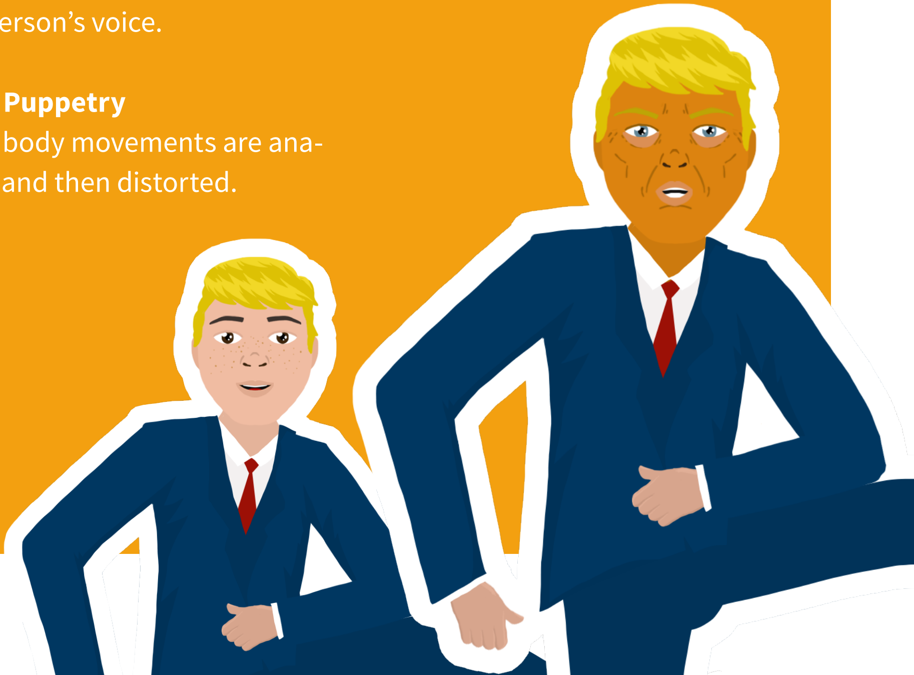
Types of Deepfake

Face Swapping
This involves the swapping of the heads of two people.

Voice Swapping
This involves the manipulation of a person's voice.

Body Puppetry
Here, body movements are analysed and then distorted.

Facial Expressions
This method goes hand in hand with voice swapping. Facial expressions and gestures are adapted to match a particular subject.



Deepfake Apps

DeepFaceLab
According to the app's developers, 95% of all deepfake videos are generated with DeepFaceLab. The app makes it possible to swap faces or entire heads, modify a person's age or adjust the lip movements of strangers.

Zao
This extremely popular app, which originates from China, creates deepfake videos in seconds. So far, however, the app is only available in China or for those with a Chinese phone number.

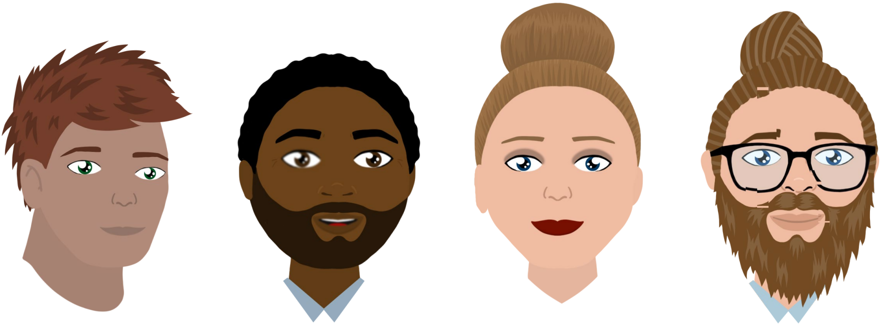
FaceApp
This app offers numerous functions such as rejuvenation or ageing, adding beards, make-up, tattoos, hairstyles or even the ability to change a person's gender.

Avatarify
With this application, users can create live deepfakes in video chats. The technology can recreate facial movements such as eye blinks and mouth movements in real-time, thus achieving realistic imitations. However, a powerful graphics card and other additional tools are required to run the installation.

RECOGNISING DEEPFAKES

Unmasking a deepfake is not always easy. First, always check the context of the video or image and consider whether the context makes sense. The FBI has also published a list that highlights specific characteristics of deepfakes. This list includes, but is not limited to:

- Visual indicators such as distortions, deformations or inconsistencies.
- Noticeable head and body movements
- Distinct visual distortions, usually in pupils and earlobes
- Visual artefacts in the image or video
- Distinct eye spacing/placement of the eyes
- Synchronisation problems between facial and lip movements and associated sound
- Indistinct or blurred backgrounds



HOW TO REACH US:

Katharinenstraße 21, 04109 Leipzig

Phone: +49 341 249 116 71

www.increaseyourskills.com/en

info@increaseyourskills.com

JOIN US

– AND GET STARTED!