11
EVERYTHING IS FAKE

HOW AI SYSTEMS CAN MANIPULATE

Funny, these fake photos. But also scary when you cannot trust your own eyes anymore, right?

Technically, this is possible with ==artificial neural networks==. First, many images, audio, or video recordings of you and the person you want to replace are analyzed: What facial or voice characteristics do you have? It is important to examine many different facial expressions, lighting conditions, and recording conditions or sound sequences with different recording qualities so that the AI system knows as accurately as possible what the face looks like in different situations.

Then the AI system ==compares the original and your recordings== in order to adjust your recordings so that they ==can be placed on the originals.== How this works is explained in more detail in Station 25 (photo box). The more often the AI system does this and the more data it has available, the more realistic the results will be. The learning process works best with a GAN (Generative Adversarial Network), where one AI system creates the fakes and a second AI system has to expose them. In this way, the AI systems learn from each other, as each wants to be better than the other.

Even blurry photos can be used to create deep-fakes.

11 EVERYTHING IS FAKE
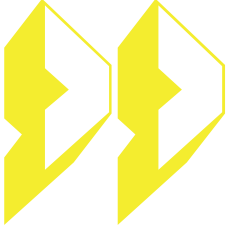
Creating deepfakes has advantages:

People who have never learned to read or who are blind can use these AI systems to have content read aloud to them in their own or a familiar voice. Someone who has lost their voice due to an accident can use an assistive system with their own voice. Famous artists can guide visitors through their exhibitions and talk about their work themselves. Imagine William Byrd telling you about Parthenia or Shakespeare reading from Macbeth. Wouldn't that be cool?

Elvis is alive! At least in this deepfake performance on America's Got Talent.

But there are also many dangers:

How would you feel if a picture appeared in the class chat showing you at an event you never attended? How would your grandmother react if she received a video from you via messenger asking her for money, even though you did not record or send the video? What if dictators manipulate video recordings to win elections or even start wars? Is democracy then in danger? And what can we do about it?
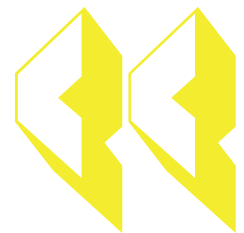
In the video, Barack Obama is clearly recognizable. But it is not the former US president who calls his successor Donald Trump a „complete fool". It is a comedian.

11 EVERYTHING IS FAKE

In some countries, the distribution of deepfakes is already punishable by law, and it is also being discussed in Europe. Violations of personal rights or copyrights are already prohibited.

But what can you do specifically?

Be vigilant and try to detect deepfakes!

Often the transitions between the inserted part and the real image are blurred. Faces and their contours can also be faulty. If the lighting and colors of the templates do not match, the AI system has to improvise. However, since it has only been trained to manipulate faces, it often has problems with the backgrounds, which leads to errors there (wrong shadows, objects in unnatural places, etc.). In videos, you can pay attention to the eyes. If they seem to be looking into the distance or if the person blinks frequently or rarely, this could be a sign that it is a fake. Audio fakes, on the other hand, are usually almost perfect. While humans use filler words, change the pace of their speech, or do not always speak fluently, an AI system must first learn these irregularities.
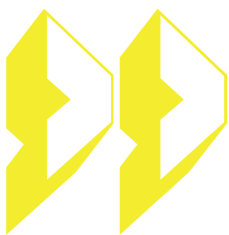
> As long as an AI system is still learning, we humans have the opportunity to expose it because of its mistakes.
> If you are not sure whether the information is real or fake, always try to find other sources that also contain the information.

11
EVERYTHING IS FAKE

SOURCES

Graphik "Deepfakes lassen sich sogar mit unscharfen Fotos erstellen."

> https://the-decoder.de/geschichte-der-deepfakes-so-rasant-geht-es-mit-ki-fakes-voran

Deepfake Video Barak Obama

> https://youtu.be/cQ54GDm1eL0

Deepfake Performance America's Got Talent

> https://youtu.be/_pwpdc6oqaE

SOCURCES EVERYTHING IS FAKE - APP

All Deepfake videos and pictures were created at https://facehub.live