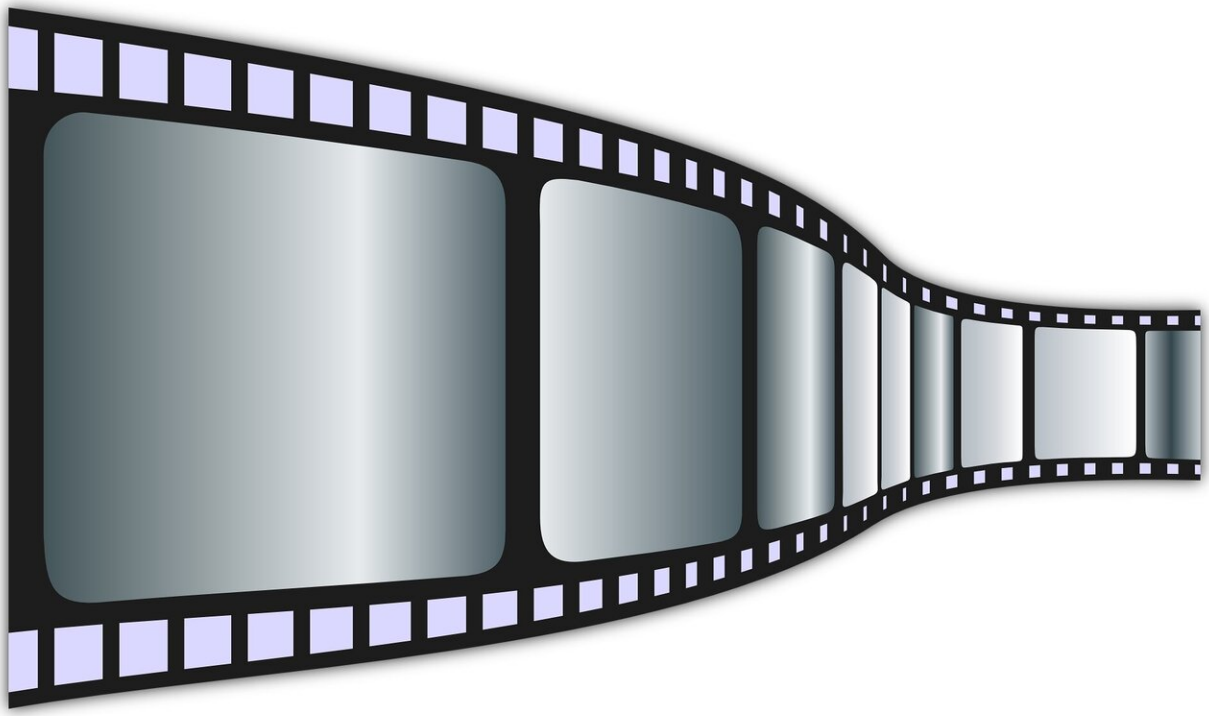
Wait, is that video real? The race against deepfakes and dangers of manipulated recordings

May 13 2019, by Dalvin Brown, Usa Today



Credit: CC0 Public Domain

It used to take a lot of time and expertise to realistically falsify videos. Not anymore.

For decades, authentic-looking video renderings were only seen in big-budget sci-fi movies films like "Star Wars." However, thanks to the rise in artificial intelligence, doctoring footage has become more accessible than ever, which researchers say poses a threat to national security.

"Until recently, we have largely been able to trust audio (and) video recordings," said Hany Farid, professor of computer science at Dartmouth College. He said that advances in machine learning have democratized access to tools for creating sophisticated and compelling fake video and audio.

"It doesn't take a stretch of the imagination to see how this can be weaponized to interfere with elections, to sow civil unrest or to perpetrate fraud," Farid said.

With the 2020 presidential election looming and the U.S. defense agency worried about doctored videos misleading voters, lawmakers and educational institutions are racing to develop software that can spot and stop what's known as deepfakes before they even hit the internet.

Deepfakes

Broad concern around the idea the video forgeries began making headlines in late 2017 when computer software was used to superimpose celebrities into porn by using computer software.

One of the best-known examples was created by director Jordan Peele's production company in 2018. The video shows former President Barack Obama warning people not to believe everything they see on the internet.

However, it's not actually Obama talking. It's Peele ventriloquizing the former president.

Warning: The video below includes coarse language to make its point and may not be suitable for young viewers.

Since then, the Department of Defense, through the Defense Advanced Research Projects Agency (DARPA), began developing ways to detect when a video is a deepfake.

A spokesperson for the agency said in March that while many video manipulations are performed for fun, others are much more dangerous as they can be used to spread propaganda and misinformation.

The organization is seeking to develop online flags and filters that stop manipulated content from being uploaded to the internet.

It only takes about 500 images or 10 seconds of video to create a realistic deepfake, according to Siwei Lyu, a researcher who is working with the Defense Department to develop software to detect and prevent the spread of deepfakes.

Lyu said that anyone who posts photos on social networking sites like Instagram is at risk of being deepfaked.

Software solutions

The first piece of software Lyu and his team of researchers at the University of Albany introduced last year could spot a deepfake video in the blink of an eye, literally, by analyzing how often the simulated faces blink—or don't.

"We discovered the subjects (in deepfake videos) do not blink very much, and sometimes not at all," Lyu said. "We then asked why does this happen."

The researchers found that the software used to make deepfakes often depends on photos available on the internet. There aren't many photos available of high profile people with their eyes closed, so the animated subjects in the fake videos don't blink, Lyu said.

As the makers of deepfakes began to catch wind of the new software, the researchers developed other methods to spot deepfakes like using algorithms that detect unnatural movements between faces and heads as well as software that analyzes footage for the loss of subtle details.

"The skin on the deepfake-generated face tends to be overly smooth, and some of the hair and teeth details will be lost," Lyu said. "If you look at the teeth more closely, they look more like a whole white block rather than individual teeth."

Researchers at the University of Washington are also experimenting with deepfake technology. The school figured out how to turn audio clips into a lip-synced video of the person speaking those words in 2017.

Criminalization

Late last year, Sen. Ben Sasse (R-Neb.) introduced a bill to Congress that would punish people for the malicious creation and distribution of deepfakes. The bill, which was introduced the day before the government shutdown, flew under the radar and died. But Sasse's office plans to reintroduce it.

USA Today reached out to Sasse for more information.

The senator said in a recent interview with radio host Glenn Beck that the "perfect storm of deep fakes" is coming soon.

The state of New York introduced a bill in 2018 that would punish

people who create digital videos of subjects without their consent.

Despite the concerns over the hypothetical dangers, abuse of deepfakes has yet to be seen outside of adult videos. The Verge published a report in March that questions whether technology for swapping faces is even a major threat seeing as though it has been widely available for years.

Lyu said that he's doubtful that deepfakes can start a war, and it is unlikely that they will have a long-lasting effect on society as people become increasingly aware of the phenomenon.

Lyu suggested that people may even become desensitized by them.

Perception-altering technology was used in April to break down language barriers in a global malaria awareness campaign featuring David Beckham.

The charity Malaria No Moreposted a video on YouTube highlighting how it used deepfake tech to effectively lip-sync the video of Beckham with the voices of several other people.

To create the 55-second ad, the nonprofit used visual and voice-altering tech to make Beckham appear multilingual. His speech begins in English, then transitions to eight other languages through dubbing.

Today, we live in a world in which millions of real people follow computer-generated influencers on social media and don't even know it at the same time governments have worked to develop animated news anchors that have human-like movements.

One of the clearest examples of real humans adapting to unreal computer-generated people is Lil Miquela, a digitally created "it-girl" with 1.5 million followers on Instagram that she interacts with via direct

messages.

Despite what's in her photo captions, she's not "daydreaming" or partying at Coachella. She's fake, but her followers don't care. They like and comment on her pictures as if she's a real person.

AI generated humans have also begun showing up on television.

The Chinese government-run news agency Xinhua began testing out AI news anchors in 2018, a move it claims as the first in the world.

At first glance, the virtual newsman appears to be an ordinary person with facial expressions and movements that correspond with his speaking voice.

But seconds into the video, it's apparent that he's not real.

"I will work tirelessly to keep you informed as texts will be typed into my system uninterrupted," the news anchor said monotonically in an introductory video. "The development of the media industry calls for continuous innovation and deep integration with the international advanced technologies."

The agency's first fake female news anchor went live in February and she appears to be even more realistic.