Video manipulation technology poses danger to future elections

April 18 2019, by Brian Huchel

Credit: CC0 Public Domain

A video on social media shows a high-ranking U.S. legislator declaring his support for an overwhelming tax increase. You react accordingly because the video looks like him and sounds like him, so certainly it has be him.

Not necessarily.

The term "fake news" is taking a much more literal turn as new technology is making it easier to manipulate the faces and audio in videos. The videos, called deepfakes, can then be posted to any social media site with no indication they are not the real thing.

Edward Delp, director of the Video and Imaging Processing Laboratory at Purdue University, says deepfakes are a growing danger with the next presidential election fast approaching.

"It's possible that people are going to use fake videos to make fake news and insert these into a political election," said Delp, the Charles William Harrison Distinguished Professor of Electrical and Computer Engineering. "There's been some evidence of that in other elections throughout the world already.

"We've got our election coming up in 2020 and I suspect people will use these. People believe them and that will be the problem."

The videos pose a danger to swaying the court of public opinion through social media, as almost 70 percent of adults indicate they use Facebook, usually daily. YouTube boasts even higher numbers, with more than 90 percent of 18- to 24-year-olds using it.

Delp and doctoral student David Güera have worked for two years on video tampering as part of a larger research into media forensics. They've worked with sophisticated machine learning techniques based on artificial intelligence and machine learning to create an algorithm that detects deepfakes.

Late last year, Delp and his team's algorithm won a Defense Advanced Research Projects Agency (DARPA) contest. DARPA is an agency of

the U.S. Department of Defense.

"By analyzing the video, the algorithm can see whether or not the face is consistent with the rest of the information in the video," Delp said. "If it's inconsistent, we detect these subtle inconsistencies. It can be as small as a few pixels, it's can be coloring inconsistencies, it can be different types of distortion."

"Our system is data driven, so it can look for everything – it can look into anomalies like blinking, it can look for anomalies in illumination," Güera said, adding the system will continue to get better at detecting deepfakes as they give it more examples to learn from.

The research was presented in November at the 2018 IEEE International Conference on Advanced Video and Signal Based Surveillance.

Deepfakes also can be used to fake pornography video and images, using the faces of celebrities or even children.

Delp said early deepfakes were easier to spot. The techniques couldn't recreate eye movement well, resulting in videos of a person that didn't blink. But advances have made the technology better and more available to people.

News organizations and social media sites have concerns about the future of deepfakes. Delp foresees both having tools like his algorithm in the future to determine what video footage is real and what is a deepfake.

"It's an arms race," he said. "Their technology is getting better and better, but I like to think that we'll be able to keep up."

Provided by Purdue University