Fake videos could influence the 2024 presidential election—a cybersecurity researcher explains situation deepfakes

July 17 2023, by Christopher Schwartz

Credit: Unsplash/CC0 Public Domain

Imagine an October surprise like no other: Only a week before Nov. 5, 2024, a video recording reveals a secret meeting between Joe Biden and

Volodymyr Zelenskyy. The American and Ukrainian presidents agree to immediately initiate Ukraine into NATO under "the special emergency membership protocol" and prepare for a nuclear weapons strike against Russia. Suddenly, the world is on the cusp of Armageddon.

While journalists could point out that no such protocol exists and social media users might notice odd video-gamelike qualities of the video, others might feel that their worst fears have been confirmed. When Election Day comes, these concerned citizens may let the video sway their votes, unaware that they have just been manipulated by a situation deepfake—an event that never actually happened.

Situation deepfakes represent the next stage of technologies that have already shaken audiences' perceptions of reality. In our research at the DeFake Project, my colleagues at the Rochester Institute of Technology, the University of Mississippi, Michigan State University and I study how deepfakes are made and what measures voters can take to defend themselves from them.

Imagining events that never happened

A deepfake is created when someone uses an artificial intelligence tool, especially deep learning, to manipulate or generate a face, a voice or—with the rise of large language models like ChatGPT—conversational language. These can be combined to form "situation deepfakes."

The basic idea and technology of a situation deepfake are the same as with any other deepfake, but with a bolder ambition: to manipulate a real event or invent one from thin air. Examples include depictions of Donald Trump's perp walk and Trump hugging Anthony Fauci, neither of which happened. The hug shot was promoted by a Twitter account associated with the presidential campaign of Trump rival Ron DeSantis.

An attack ad targeting Joe Biden's 2024 campaign published by the Republican National Committee was made entirely with AI.

At the DeFake Project, our research has found that deepfakes, including situations, are typically created by some mixture of adding one piece of media with another; using a video to animate an image or alter another video, dubbed puppeteering; conjuring a piece of media into existence, typically using generative AI; or some combination of these techniques.

To be clear, many situation deepfakes are made for innocent purposes. For example, Infinite Odyssey Magazine produces fake stills from movies that were never produced or could never have existed. But even innocent deepfakes give reason for pause, as in the case of near-believable fake photographs depicting the Apollo Moon landing as a movie production.

Deepfaking an election

Now put yourself in the position of someone trying to influence the upcoming election. What are the possible situations you might want to create?

For starters, it would matter whether you wanted to tilt voting toward or away from a specific outcome. Maybe you would portray a candidate acting heroically by pulling a pedestrian out of the way of a speeding car or, conversely, doing something offensive or criminal. The format of the situation deepfake would also matter. Instead of a video, it could be a photograph, maybe with the blur and angles that simulate a smartphone camera or the forged logo of a news agency.

Your target audience would be key. Rather than aiming for the general electorate or a party's base, you might target conspiracy theorists in key voting districts. You could portray the candidate or their family

members as engaging in a satanic ritual, participating in a festival at the exclusive and controversial Bohemian Grove, or having a secret meeting with an extraterrestrial.

If you have the ambition and capabilities for it, you could even try to deepfake the election itself. In June 2023, Russia's television and radio stations were hacked and broadcast a full mobilization order by a deepfake of Russian President Vladimir Putin. While this would be more difficult to do in a U.S. election, in principle any news outlet could be hacked to broadcast deepfakes of their anchors announcing the wrong results or a candidate conceding.

Defending reality

There are a variety of technological and psychological ways to detect and defend against situation deepfakes.

On the technological front, all deepfakes contain some evidence of their true nature. Some of these tells can by seen by the human eye—like overly smooth skin or odd lighting or architecture—while others may be detectable only by a deepfake-hunting AI.

We are building DeFake's detector to use AI to catch the telltale signs of deepfakes, and we are working to try to have it ready in time for the 2024 election. But even if a sufficiently powerful deepfake detector like ours cannot be deployed by Election Day, there are psychological tools that you, the voter, can use to identify deepfakes: background knowledge, curiosity and healthy skepticism.

If you encounter media content about a person, place or event that seems uncharacteristic, trust your background knowledge. For example, in a recent hoax of a fire at the Pentagon, the building shown looks more square than pentagonal, which could be a giveaway.

However, try not to rely entirely on your background knowledge, which could be mistaken or patchy. Never be afraid to learn more from reliable sources, like fact-checked news reports, peer-reviewed academic articles or interviews with credentialed experts.

Additionally, be aware that deepfakes can be used to take advantage of what you are inclined to believe about a person, place or event. One of the best ways to deal with this is to simply be aware of your biases and be a bit guarded about any media content that seems to confirm them.

Even if it becomes possible to create perfect situation deepfakes, how believable their subject matter is, is likely to remain their Achilles' heel. So, with or without a technological solution, you still have the power to defend the election from the influence of fake events.

Provided by The Conversation

Citation: Fake videos could influence the 2024 presidential election—a cybersecurity researcher explains situation deepfakes (2023, July 17) retrieved 14 May 2024 from https://techxplore.com/news/2023-07-fake-videos-presidential-electiona-cybersecurity.html