Source : www.thehindu.com Date : 2023-06-06

DEALING WITH DEEPFAKES

Relevant for: Security Related Matters | Topic: Challenges to internal security through Communication Networks

June 06, 2023 12:15 am | Updated 08:47 am IST

This image made from video of a fake video featuring former President Barack Obama shows elements of facial mapping used in new technology that lets anyone make videos of real people appearing to say things they’ve never said. | Photo Credit: AP

A deepfake is something that a machine has produced using deep learning and which contains false information. It pays to keep the definition of deepfakes, however vague, in front of us because of the way deepfakes distort reality and attempt to persuade us that something false is true.

On May 28, the wrestlers protesting peacefully in New Delhi were tackled to the ground, arrested, and boarded in a van to keep them from disrupting the inauguration of the Parliament building. Shortly after, a photo appeared to show four of the beleaguered wrestlers posing with wide smiles for a selfie in the van.

If you had believed the photo to be real, you might also have believed that the wrestlers had orchestrated a clash with the police and that they wanted to be photographed while being ‘roughed up’. This is what the person who created the photo may have intended. Though it emerged later that this photo had been morphed, and was not a deepfake, creating such visuals has become child’s play. Deepfaking is a significant ‘upgrade’ from photoshopping images as it transcends the limits of human skill. Here, machines iteratively process large amounts of data to falsify images and videos, sometimes in real time, and with fewer imperfections.

Deepfake images and videos thus have an unsettling legacy. People worldwide have already used the technology to create a video of Barack Obama verbally abusing Donald Trump, hack facial recognition software, manufacture ‘revenge porn’, etc. On May 22, a deepfake image purporting to show a towering column of dark smoke rising from the Pentagon received sober coverage from a few Indian television news channels. The image was soon found to have been machine-made.

As with other modern technologies set on the information superhighway, there is no way for us to go back to a time when people didn’t have the tools to falsify media elements at scale. Alongside deepfaked images and videos, we have chatbots that mimic intelligence, but we can’t tell the difference when they make a mistake. This leads some to believe certain information to be ‘true’ simply because a machine gave it to them.

Then again, these tools have also been used for good. Using deep learning, the ALS

Association in the U.S. founded a “voice cloning initiative” to restore the voices of those who had lost it to amyotrophic lateral sclerosis. Deep learning has also been adapted in comedy, cinema, music, and gaming. Experts have recreated the voices and/or visuals of visual artist Andy Warhol, celebrity chef Anthony Bourdain, and rapper Tupac Shakur, among others, enhancing our ability to understand, and even reinterpret, history (although some of these attempts haven’t been free of controversy).

As such, despite its potential to rupture the social fabric, deep learning is entirely redeemable, just like the kitchen knife or the nuclear reactor. The focus, in turn and as usual, must be on how we wield it. This is also the question that generative artificial intelligence like ChatGPT has been forcing us to ask. The major technology companies behind ChatGPT et al seem to have been driven by ‘can we do this?’ rather than ‘should we do this?’, although not without exceptions.

Our still-evolving experience with solar geoengineering offers a useful, if also imperfect, parallel. Solar geoengineering involves modifying the climate to be favourable over one part of the planet, by blocking sunlight, but which invariably has planet-wide consequences. Many scientists agree that this is dangerous and have called for a moratorium on the use of this technology and for international cooperation led, if required, by a treaty.

Clumsy though it may seem, deepfakes merit a similar response: laws that regulate its use and punish bad-faith actors, and keep the door open for democratic inputs to guide the future of such a powerful technology. A good starting point could be what political philosopher Adrienne de Ruiter wrote in 2021, which is to protect against the “manipulation of hyper-realistic digital representations of our image and voice.” This, she said, “should be considered a fundamental moral right in the age of deepfakes”. And a stepping stone for us, as individuals, is to become more scientifically, digitally, and public-spiritedly literate. Then, we will be able to look past an implausible photo and bring to light its concealed creator.

For now, among all the countries, China has responded strongest. It has banned deepfaked visuals whose creators don’t have permission to modify the original material and which aren’t watermarked accordingly. The success of this policy is no doubt assured by the country’s existing surveillance network. Every measure short of this requires at least an ampoule of self-restraint. And that is rooted in the kind of people that we are.

COMMents

SHARE

Artificial Intelligence / technology (general)

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END