THE FINANCIAL EXPRESS
www.financialexpress.com

21 September 2019

REEL OR REAL?

Accurately identifying disinformation

In this day and age of AI-based tech such as deepfake—one can easily produce or alter video content realistically—seeing should not necessarily be believing

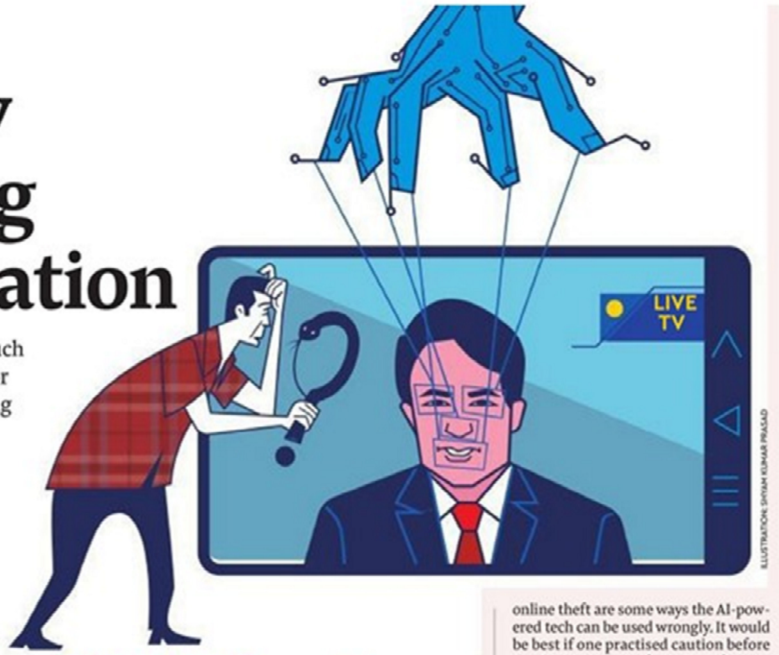

ILLUSTRATION: SHYAM KUMAR PRASAD

CHANDRAJIT BANERJEE

The author is director general, Confederation of Indian Industry. Views are personal

FOR THE LAST couple of years, India has been waging a silent battle against a growing epidemic of fake content that's being used to manipulate and deceive people. The problem is real and has serious repercussions as there is a tendency to amplify or act on the information that we have received, especially from sources that may be trusted by millions from all over the country. The content may look and sound real, and because it is trending on a global platform, authenticity verification is the last thing on anyone's mind.

Many of these fake videos are made with AI applications. Deepfake, for instance, is an AI-based technology through which one can produce or alter video content realistically. Through certain AI tools, one can morph or distort images, or create a scene or a dialogue that never happened. The list is endless.

The exponential growth of deepfakes is a grave concern, given that easily accessible open-source software and apps that can be downloaded free of charge allow pretty much anyone with a computer or a smart mobile device to create deepfakes. The threats posed by deepfakes are developing at an alarming rate.

Often, the target is a celebrity, public figure. But there have been instances where the general public has been targeted. For instance, women have had their faces morphed on pornographic content, which were then uploaded on the Internet. The data was obtained from their social media pages, which lacked the necessary privacy settings.

Another scenario where such tools can cause damage to individuals and businesses alike are deepfake audios. These audio fakes can be created by accessing publicly-available audio content and training the system in the voice modulations of particular individuals. Once an audio training model has been created, a simple text-to-speech software can help generate fake material.

Deepfakes provide means to impersonate a person or a group of people, leading to phishing, scams, frauds or espionage through traditionally secure contexts, like phone calls and video conferences. By perfectly replicating physical features of an individual, deepfakes make live impersonation fraud also easy.

Industry is an easy target for deepfakes due to the significant financial gain and due to the fact they stand to lose so much—reputation, profits, market valuation and customer loyalty. It is essential that companies invest in preparing their employees in advance, by educating them about this emerging threat and giving them the data identification tools to identify and tag the disinformation.

A security firm has already issued a warning of cyberattacks where deepfake audios have been used in the context of financial fraud on companies. At least three such incidents have been reported where the voice of the company CEO was used to call senior financial executives for urgent money transfers, resulting in a loss amounting to millions of pounds. When such techniques are already in use, the probability of the attack landing at one's doorstep increases drastically.

Consider a situation where an audio recording of a company's chairman is released of him purportedly claiming massive losses and the business no longer being sustainable. It can cause investors to lose confidence and the damage to the business could be far reaching. Combine this scenario with a video of the chairman making these statements before the opening of the stock market and the resultant economic loss to the company could be catastrophic. Even more worrisome is the possibility of an organisation using this fake technique to target its business rivals, where the repercussions could be extremely dangerous. Industry needs to come together to find a solution to this emerging AI-based threat.

Deepfakes can also be used in crimes against individuals—identity theft, blackmail through altered video/image, online theft are some ways the AI-powered tech can be used wrongly. It would be best if one practised caution before sharing important information after seeing video evidence because it could be a deepfake. It is also quite feasible that some individuals may claim real videos of themselves as being fakes, trying to give the powers that be the run around.

It's difficult for investigation agencies and the judiciary to grapple with the myriad issues arising out of deepfakes. Globally, research institutes and tech companies are conducting research to create programs that can red flag fake videos, pictures and audio clips. Several fact-checking and content-validation tools have been successful in this regard, but only to an extent. Forensic analysis techniques, rules of evidence and appropriate legislative tools would need to be examined afresh in light of this growing threat.

We need to create a public awareness campaign about such digitally-manipulated content. The general population should also be made aware and educated on the downsides of falling prey to fake content through mass awareness campaigns by the government. Indian tech companies should consider research and development to combat deepfakes.

A collaborative effort between the government, industry and academia to find effective solutions to this menace is imperative, and would go a long way in making India a more cyber-aware and secure country. Till such time India is well prepared to tackle this threat, seeing should not necessarily be believing.