MATHEMATICAL MOMENTS

Unmasking Deepfakes

You're probably thinking, "Steve Buscemi doesn't usually wear red when he goes sleeveless, does he?" Indeed, this image is not real. It's from a computer-generated video known as a *deepfake*. Due to the increase in computing power and improvements in machine-learning, deepfake videos are now, unfortunately, both easier to make and harder to identify. All is not lost, though. Just as computers, with human guidance, create deepfakes, together they can detect them, too. Current approaches use many techniques, including geometry (of head and lip movements), linear algebra (to detect discrepancies that arise from transforming one face to another), and probability (to measure the chance that a video isn't real) to identify fake videos. Yet the most important weapon in this battle against fraud may be not taking everything at value.

Researchers are now working on a more robust method to foil fakers. The method uses the bits of a video file to assign a mathematically encrypted number to that file, which serves as its digital signature. The signature becomes part of a blockchain similar to what is used in digital currency to authenticate transactions and detect manipulations. Any manipulating of the video will change the bits of the original file but not its original signature, so that the new file's signature won't match that of the original. With this validation method in place, accessing a deepfake will generate an alert, similar to what pops up when you're trying to access an unsecure website, so you'll know that what you see isn't what you ought to get.

Image: Screen grab from video by VillainGuy.

For More Information: "Protecting World Leaders Against Deep Fakes," by Agarwal, Farid, Gu, He, Nagano, and Li, 2019.

Listen Up!

MM/146

AMS
American Mathematical Society

The ***Mathematical Moments*** *program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.*

www.ams.org/mathmoments