Rodney's Take

May 13, 2024

Where Are the Heroes?

Months ago, I told you about how someone had recorded a few minutes of my son's voice and used it to simulate my son further on audio. The fraudster then called me on the phone and, using the audio to pose as my son, said he'd been in an accident and needed cash. The deception would have worked, had I not called my son's wife to verify my son's whereabouts before sending the money. It was a really good fake.

Now, the people who make such things, for good or ill, are getting better. They can steal someone's identity not only on audio but also on video, and they will do this… for a fee.

Jonathan Yang paid $1,350 to have an AI company replicate his deceased uncle on video calls. Yang's family gave the AI company some pictures and video of Yang's uncle to use for training the computer. Now, Yang's grandmother gets video calls three times a year on Chinese holidays in which the simulated "uncle" lets her know he won't make it home. Yang's grandmother is 93. The family thinks news of her son's death would devastate her.

It's easy to see how such technology could be the next big thing in fraud, just as audio fraud was for me. The problem lies in recreating natural movements and conversations. To do that, you need a lot of material with which to work. Yang paid $1,350 to get a quick video call three times a year. Getting a longer call would require a massive dump of raw material and computer resources to get it right… at least it would today.

What about tomorrow? Computers steadily get cheaper, and it seems someone has a phone out at every family gathering, taking pictures and video. As computers learn more, all someone would need to mimic a person successfully is enough video and audio, and employers and stores are generating just that. My youngest graduated college in 2021, during the "COVID year." She took her last 10 classes online. During exams, she and her classmates were required to have their cameras on. The college used a software package to track eye movements and facial features to try to ferret out cheating. The software now is commonly used for online courses. I wonder if (or, rather, *where*) a person or group with bad intentions has breached such databases, to match hours of facial expressions with names and audio files.

I'm looking for the white hats. I've read too much about what bad things are possible. Unless they can spend a lot of money—and can find lots of video footage of the target (Watch out, politicians and social influencers!)—bad

guys can't create seamless video fakes yet. So far, fraudulent videos are easy to spot, much like AI-written articles. But costs fall and expertise improves. While some companies are working to spot fakes, who is going to help individuals? My fear is that by the time we have such defenses, fraud will be even more rampant.

The government of India, a nation of 1.4 billion people, created a biometric database of almost everyone in the country to fight corruption in aid distribution. In the Western world, we use our faces to open or close our phones. The problem is not in protecting our devices or accounts, it's when bad guys use personal data to pretend that they are people we trust.

Some friends of mine have a security word each family member knows that they use to detect fraud. It's a low-tech solution to a high-tech problem. I fear that we're going to be overburdened with security questions, like, "What was the first name of your grandmother on your maternal side?" I hate those things today. Imagine how my daughter will feel when I'm asking her those questions when she wants to borrow a few hundred bucks?

I think the answer may be using biometrics to verify whether callers (on audio or video) are who they say they are, but who would maintain the database? Do you want that group, whomever they are, to have your data? As an early Gen-Xer, my answer is, "!@#$% no!" As for my kids, well, they think the government knows everything about them anyway.

Somehow, that doesn't make me feel better.

Rodney

Got a question or comment? You can contact us at info@hsdent.com