PCBB

BID® Daily Newsletter

Jul 7, 2022

The Big Picture on Synthetic Image Fraud

cyber security fraud protection

Summary: Synthetic images have become so sophisticated that people and facial recognition systems are no longer able to tell the difference between AI-generated faces and real ones.

More than four decades into her career, music legend Ella Fitzgerald experienced a resurgence in popularity after agreeing to become the spokesperson for a 1972 television advertising campaign for Memorex blank cassette tapes. The ad series kicked off with Fitzgerald singing so high that her voice breaks a glass, followed by a recording of her voice breaking another glass and then a third glass breaking from the song followed by the famous tagline “Is it live… or is it Memorex?” The campaign was so successful that it ran for several years in multiple versions, always ending with the recognizable tagline hyping the fact that Memorex’s cassette quality was so good it was nearly impossible to discern a live performance by Fitzgerald from a recording.

The idea of being unable to tell the difference between a live performance and a cassette recording seems somewhat amusing, given the massive improvements in the quality of sound recording since the 1970s. The inability to tell the difference between real and fake photos, however, is far less entertaining when it comes to advancements in synthetic image quality. Synthetic images created by artificial intelligence have advanced to a point where not only can they fool the average person, they can successfully fool the facial recognition software that financial institutions and other organizations rely on to confirm a person’s identity.

A Clear Picture. Synthetic images have become so convincing that when asked to tell the difference between photos of real human faces and fake ones, people are wrong more than 50% of the time. Faces created by generative adversarial networks have become so realistic that, even when given tips on things to look for to spot faces generated by artificial intelligence, there’s virtually no improvement in people’s ability to discern between phony faces and real photographs. Even more concerning, when asked to rate the trustworthiness of a set of real and phony faces, AI-generated faces rank 8% more trustworthy.

Beyond the ability to fool people, AI-generated faces are now able to trick the very software designed to protect people’s identities. Ace shots pulled from deep fake videos – videos where a real person’s face is replaced by an AI-generated face that is similar looking – are able to fool Amazon’s facial recognition program 68% of the time and Microsoft’s 78%.

Focusing on Prevention. From still images to videos, there is no shortage of fraudulent ways that criminals are finding to use synthetic. They are creating phony passports and other identification documentation to craft false identities or to take over the identity of real people. As more and more institutions rely on selfie identification software as a way to authenticate the identity of individuals opening new accounts, such fraud is only likely to increase.

Though AI-based security measures, such as facial recognition programs are themselves continuously becoming more sophisticated, there isn’t yet any one foolproof way for community financial institutions (CFIs) to protect against such fraud. Given this reality, your institution should be aware of the risks and take every measure possible to keep your security measures up to date with the latest advancements. It’s equally important to make sure that your employees are aware of developments on this front, don’t become overly reliant on facial recognition software programs, and remain diligent in dual verification methods.

One preventative measure gaining traction that your institution should be aware of and keep an eye on is known as controlled capture, a technology that relies on the metadata that exists in apps with built-in camera functions to identify the location and time that an image was captured—information that is absent in artificial images. Controlled capture is being developed by the Coalition for Content Provenance and Authentication, along with technology companies.

Picture a customer’s face: is it real or is it AI-generated? A new challenge to double check.

PCBB PODCAST: EXCITING, NEW & INFORMATIVE

PCBB’s podcast, Banking Out Loud has launched! We provide informational, unbiased, and candid conversations and discussions in each episode on an array of banking topics, including CECL, artificial intelligence, and real-time payments. Check out our podcast episodes today.

ECONOMY & RATES

Rates As Of: 07/07/2022 09:16AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	1.90	0.18	1.84
6M	2.62	0.11	2.43
1Y	2.83	0.05	2.45
2Y	3.05	0.09	2.31
5Y	3.05	0.01	1.79
10Y	3.00	-0.02	1.49
30Y	3.18	-0.01	1.28

FF Market	FF Disc	IORB
1.58	1.75	1.65
SOFR	**Prime**	**OBFR**
1.54	4.75	1.57

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.