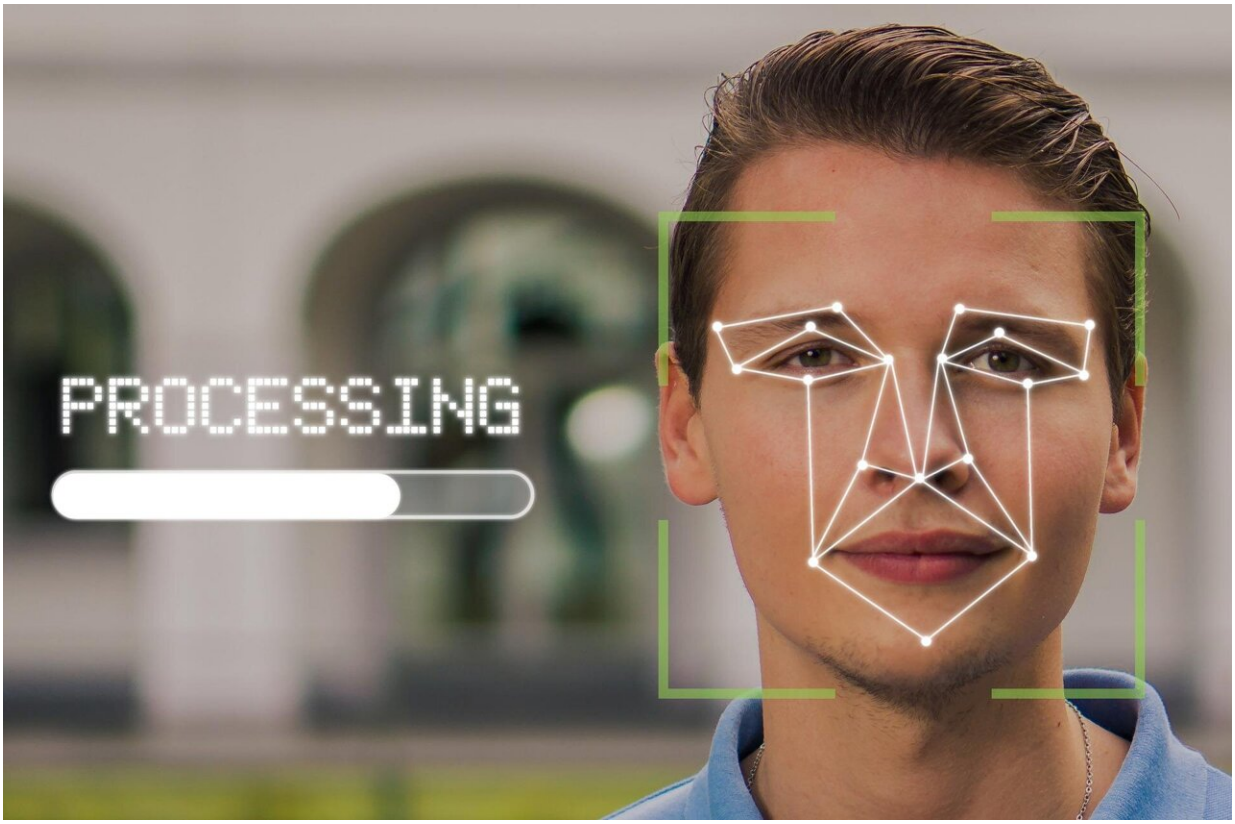
Deepfakes expose vulnerabilities in certain facial recognition technology

August 12 2022, by Jessica Hallman



Credit: Pixabay/CC0 Public Domain

Mobile devices use facial recognition technology to help users quickly and securely unlock their phones, make a financial transaction or access medical records. But facial recognition technologies that employ a

specific user-detection method are highly vulnerable to deepfake-based attacks that could lead to significant security concerns for users and applications, according to new research involving the Penn State College of Information Sciences and Technology.

The researchers found that most application programming interfaces that use facial liveness verification—a feature of facial recognition technology that uses computer vision to confirm the presence of a live user—don't always detect digitally altered photos or videos of individuals made to look like a live version of someone else, also known as deepfakes. Applications that do use these detection measures are also significantly less effective at identifying deepfakes than what the app provider has claimed.

"In recent years we have observed significant development of facial authentication and verification technologies, which have been deployed in many security-critical applications," said Ting Wang, associate professor of information sciences and technology and one principal investigator on the project. "Meanwhile, we have also seen substantial advances in deepfake technologies, making it fairly easy to synthesize live-looking facial images and video at little cost. We thus ask the interesting question: Is it possible for malicious attackers to misuse deepfakes to fool the facial verification systems?"

The research, which was presented this week at the USENIX Security Symposium, is the first systemic study on the security of facial liveness verification in real-world settings.

Wang and his collaborators developed a new deepfake-powered attack framework, called LiveBugger, that enables customizable, automated security evaluation of facial liveness verification. They evaluated six leading commercial facial liveness verification application programming interfaces provided. According to the researchers, any vulnerabilities in

these products could be inherited by the other apps that use them, potentially threatening millions of users.

Using deepfake images and videos secured from two separate data sets, LiveBugger attempted to fool the apps' facial liveness verification methods, which aim to verify a user's identity by analyzing static or video images of their face, listening to their voice, or measuring their response to performing an action on command.

The researchers found that all four of the most common verification methods could be easily bypassed. In addition to highlighting how their framework bypassed these methods, they propose suggestions to improve the technology's security—including eliminating verification methods that only analyze a static image of a user's face, and matching lip movements with a user's voice in methods that analyze both audio and video from a user.

"Although facial liveness verification can defend against many attacks, the development of deepfake technologies raises a new threat to it, about which little is known thus far," said Changjiang Li, doctoral student of information sciences and technology and co-first author on the paper. "Our findings are helpful for vendors to fix the vulnerabilities of their systems."

The researchers have reported their findings to the vendors whose applications were used in the study, with one since announcing its plans to conduct a deepfake detection project to address the emerging threat.

"Facial liveness verification has been applied in many critical scenarios, such as online payments, online banking and government services," said Wang. "Additionally, an increasing number of cloud platforms have begun to provide facial liveness verification as platform-as-a-service, which significantly reduces the cost and lowers the barrier for companies

to deploy the technology in their products. Therefore, the security of facial liveness verification is highly concerning."

Provided by Pennsylvania State University