This Startup Wants to Bring Face Recognition to All Kinds of Smartphones

Most of us aren't going to shell out for an iPhone X, but we can still log in with our faces.

By Rachel Metz

October 4, 2017

ZOOMLOGIN

ZOOMLOGIN

Unlike passwords, your face is unique—a simple fact that may make it an invaluable authenticator in the near future for everything from stock trading to video games as biometrics become increasingly common (and powerful) on smartphones.

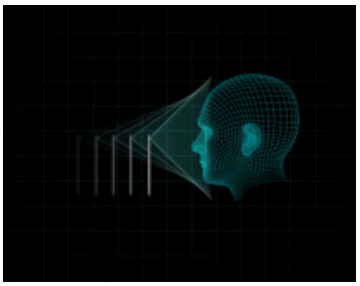
Yet while some companies, like Apple, believe the best way to do this is with sensors like an infrared camera to map your face in 3-D—something that, for now, continues to limit the technology to high-end phones—a small Las Vegas startup is trying to bring a software-only take on 3-D face recognition to all kinds of smartphones.

FaceTec's Zoom technology uses a different tactic than the one Apple uses to determine if you are a human (rather than, say, a photo or a video of one) and, in fact, the phone's rightful owner. It pays attention to the distortion that

FACETEC EXHIBIT 2050
JUMIO v. FACETEC
IPR2025-00109

occurs as you move your face closer to the phone's camera, and analyzes how the distortion in images taken when you want to get into, say, a stock trading app, compare to that in images already stored on the phone.

Related Story



Related Story

The move toward alternatives to the password has been happening for years now, and biometric technologies like fingerprint and iris scanning and facial recognition have long been creeping into smartphones—sometimes without much success. However, facial recognition in particular is becoming more popular, and Apple's inclusion of face recognition in its highest-end iPhone, which ships out in November, may help companies such as FaceTec gain a toehold in the market by making the feature seem more desirable (see "10 Breakthrough Technologies 2017: Paying with Your Face").

FaceTec has been working on its face authentication for nearly four years, says CEO Kevin Alan Tussy, and hopes companies such as banks and payment services will add it to their apps (it's free for smaller businesses, educational companies, and nonprofits). A couple of banks are currently conducting pilot tests using it, and the company offers its software tools to developers to use, too.

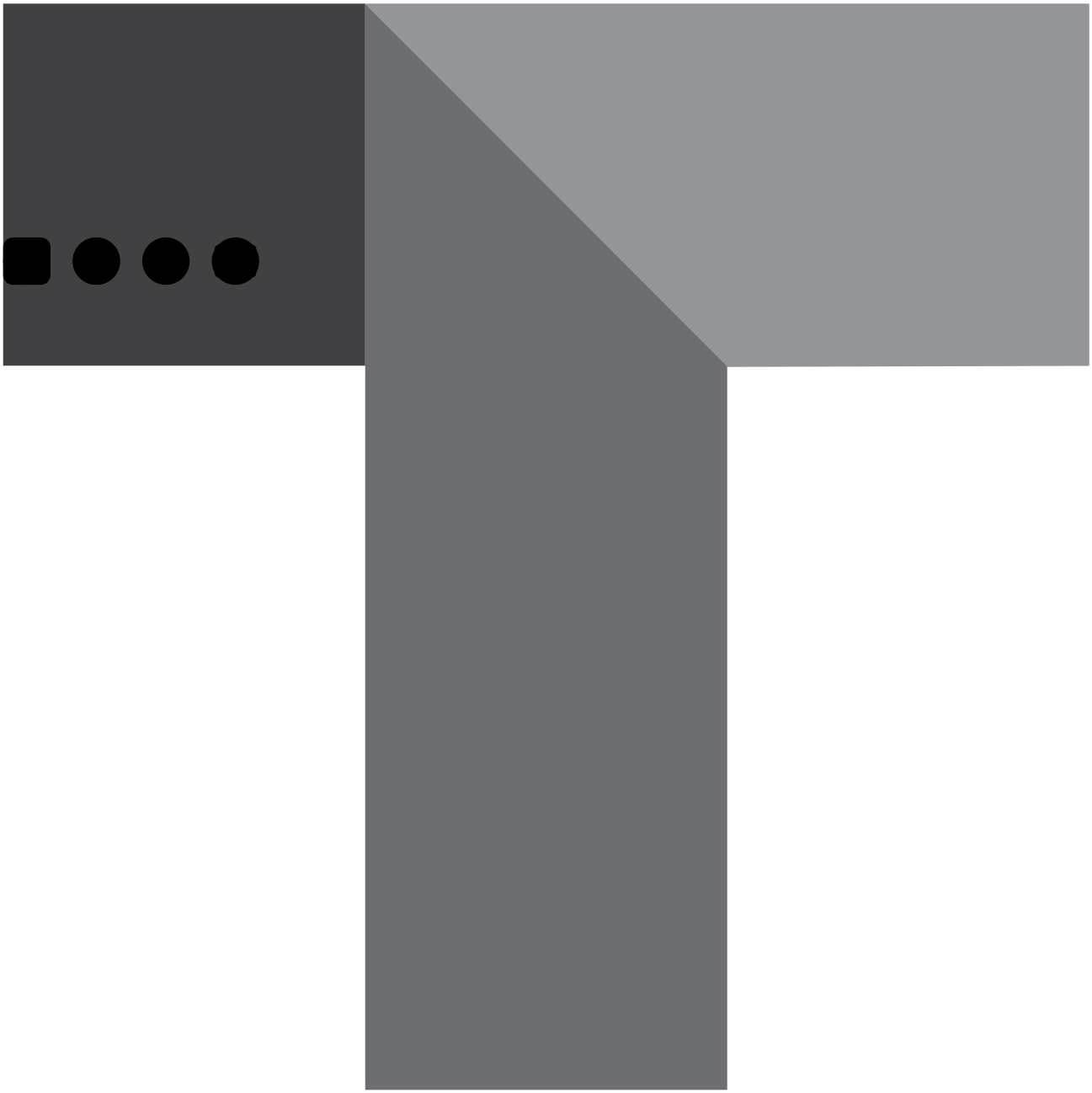
A demo app for Android and iOs called Zoom Login—which is just intended to take you through the enrollment and verification steps—gives a sense of how it works. To enroll, you take several rounds of selfies while holding the phone at two different depths (first, a bit more than a foot from your face, then several inches closer). To log in, you do the same thing once more, holding the phone in front of you, then closer. It even seems to work in the dark: in a pitch-black room the white around the edge of the display illuminated my face enough for it to log me in to the app.

Tussy says Zoom collects a handful of video frames and then sees how face features like the tip of your nose change as you move the camera lens closer. The software analyzes images of your face directly on the phone, and can be used on low-end smartphones, Tussy says.

Marios Savvides, director of the CyLab Biometrics Center at Carnegie Mellon University, says that FaceTec's method makes sense, and it should help deflect some spoofing attacks like those using photographs in an attempt to get into your phone. But he's not sure if it could prevent someone with a 3-D mask from accessing the handset (something Apple noted that it trained Face ID to avoid).

Tussy claims that the company's AI can determine whether a mask or mannequin head is trying to fool it. The accuracy of Zoom varies, depending on how it's configured, with a false acceptance rate ranging from one in 50,000 (the same as what Apple says it experiences with its Touch ID fingerprint sensor) to one in a million (what Apple says is the same chance of someone successfully spoofing you with Face ID).

Yet Rich Mogull, analyst and CEO at security research company Securosis, says that being totally software-based means “it would need additional hardware protection to achieve equivalent levels of security” to Apple’s face-scanning technology.

FaceTec can surely get its technology to work, he says, and it would be more secure than simple two-dimensional facial recognition.

“But I’d be shocked if it was as usable or secure as alternative methods we now see being adopted,” he adds.