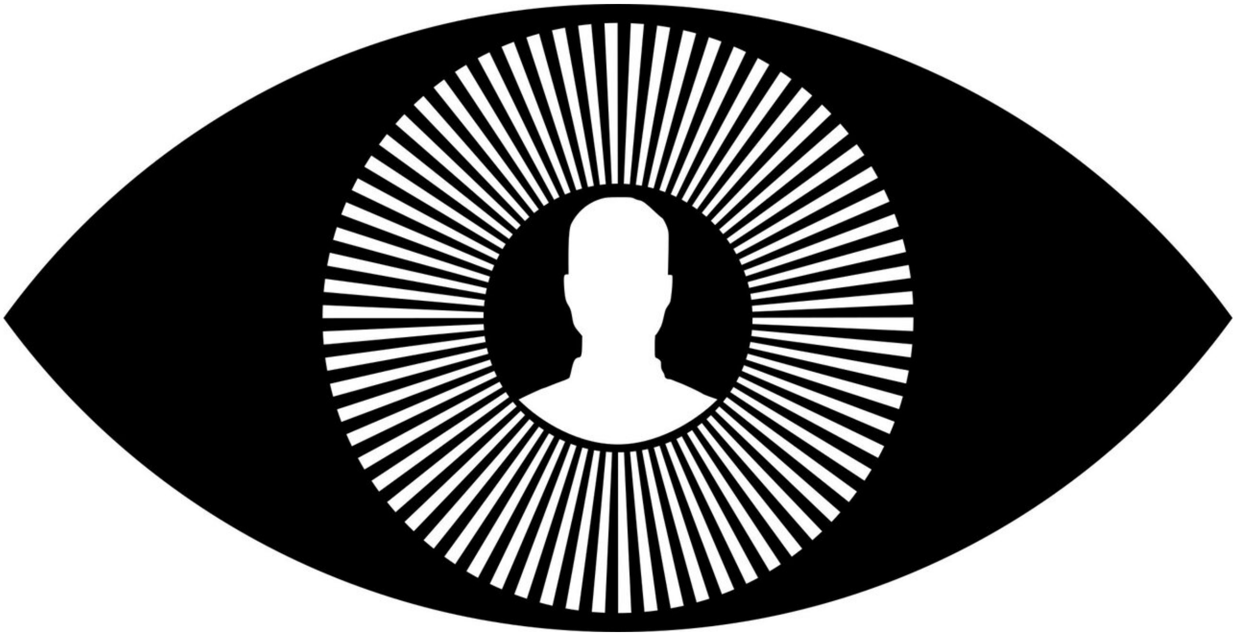
TechXplore

Sleuths with masks trick facial recognition systems

December 17 2019, by Nancy Cohen



Credit: CC0 Public Domain

Researchers are not kidding: Facial recognition technology was not having a good year, between sensitive critics who generally bristle over AI making calls on anything and scientists who specifically point out questionable accuracy ratings.

The latest findings are from a San Diego AI company Kneron who are out to promote their own facial recognition smarts and sent out researchers to test out facial recognition from China to the Netherlands. The results suggest there is possibly an industry-wide issue of substandard facial recognition technologies.

Patently Apple commented that "Masks and simple photographs are enough to fool some facial recognition technology, highlighting a major shortcoming in what is billed as a more effective security tool."

The company's goal was simple: Let's see how well facial recognition technology is doing by putting it to the test.

The sleuths wore masks of other people's faces and used photos to spoof a biometric self boarding system at Schiphol Airport. Other places tested? Border crossings. And more.

As for the masks: These were not exactly the masks you find in mall joke shops next to rubber spiders.

Patently Apple: In stores, "the Kneron team used high quality 3-D masks" to deceive payment systems in order to make purchases.

Kneron acknowledged, said Jeff Roberts in *Fortune*, that such fraud was unlikely to be widespread "because the ones used in the experiment were obtained from specialty mask makers in Japan."

> All it takes to fool facial recognition at airports and border crossings is a printed mask, researchers found https://t.co/42ymWrzYZI #fintech #biometrics pic.twitter.com/n294lfUUmw
>
> — Chris Gledhill (@cgledhill) December 13, 2019

According to the Dec. 12 article in *Fortune*, Schiphol Airport, We Chat, and AliPay did not respond to requests for comment about the effectiveness of their facial recognition technology.

Fabienne Lang, *Interesting Engineering*, was one of a number of tech watchers who wrote about the who, what and where as they set out to trick the systems.

They fooled mobile payment tablets. They duped a facial recognition system at a border crossing in China. They tested a passport control gate at Amsterdam's Schiphol Airport systems in the Netherlands. Schiphol, the Netherlands' largest airport? Schiphol, one of the busiest airports in Europe?

The widely quoted story in *Fortune* reported on their going though rail stations in China where commuters use facial recognition to pay their fare and board trains, using a photo on a phone screen.

BiometricUpdate.com similarly reported that Kneron testers say they defeated payment systems from AliPay and WeChat with high quality 3-D masks, and used images on phone screens to defeat payment and boarding systems at Chinese rail stations.

Reports said that Apple face recognition technology failed to fool.

(Regarding Apple, PYMNTS said that "Neither a mask nor a photograph could fool even the oldest iPhone with the technology, the iPhone X, during the test.")

Kneron's CEO Albert Liu was quoted in *Fortune*, as saying that "The technology is available to fix these issues but firms have not upgraded it. They are taking shortcuts at the expense of security."

Back in September, Kneron was celebrating adoption of its "Facial

Recognition Solution" by public banks of Taiwan. The technology was to be allied to door security and attendance management systems.

The company, said *Fortune*, is creating "Edge AI." Roberts said the tool does the job of recognizing individuals on devices rather than though cloud-based services.

Citation: Sleuths with masks trick facial recognition systems (2019, December 17) retrieved 2 May 2024 from https://techxplore.com/news/2019-12-sleuths-masks-facial-recognition.html