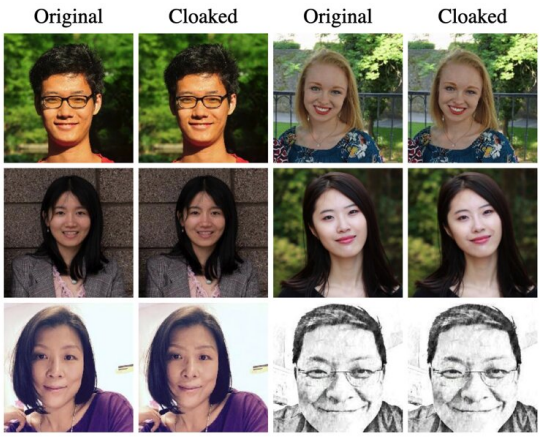
Image cloaking tool thwarts facial recognition programs

5 August 2020, by Peter Grad



Credit: University of Chicago

Researchers at the University of Chicago were not happy with the creeping erosion of privacy posed by facial recognition apps. So they did something about it.

They developed a program that helps individuals fend off programs that could appropriate their images without their permission and identify them in massive database pools.

Fawkes, named after the fictional anarchist who wore a mask in the "V for Vendetta" comics and film, makes subtle pixel-level alterations on images that, while invisible to the naked eye, distort the image enough so that it cannot be utilized by online image scrapers.

"What we are doing is using the cloaked photo in essence like a Trojan Horse, to corrupt unauthorized models to learn the wrong thing about what makes you look like you and not someone else," Fawkes co-creator Ben Zhao, a computer science professor at the University of Chicago, said. "Once the corruption happens, you are continuously protected no matter where you go or are seen."

The advent of facial recognition technology carried with it the promise of great benefits for society. It helped us protect our data and unlock our phones, organized our massive photo collections by matching names with faces, made air travel more tolerable by cutting the wait at ticket and baggage check-ins and is helping the visually impaired recognize facial reactions in social situations with others.

There are obvious advantages for law enforcement who use facial recognition to detect and catch bad actors, track transactions at ATMs, and find missing children.

It is also helping businesses crack down on thefts, tracking student attendance in schools, and, in China, allowing customers to leave their credit cards behind and pay for meals with just a smile. And the National Human Genome Research Institute is even using facial recognition with a near 100-percent success rate to identify symptoms of a rare disease that reveals itself in facial changes.

But concerns abound as well. With few federal regulations guiding the use of such an invasive technology, abuse is inevitable. The FBI has compiled a database exceeding 412 million people. Some, to be sure, are criminals. But not all. The notion of an increasingly surveilled population suggests to many the slow erosion of our privacy and, along with it, possibly our freedoms and rights. A society increasingly scrutinized under the watchful eye of Big Brother evokes images of totalitarian societies, imagined, as in "1984," and real, as in North Korea.

Concerns have been raised about the consequences of misidentification, especially in situations involving serious crime, as well as the capacity for abuse when corrupt governments or rogue police agents have such tools at hand. Also,

facial recogition programs can sometimes be wrong. Recent troubling studies have found recognition programs have particular problems with correctly identifying women of color.

Earlier this year, The *New York Times* reported on the controversial activity of Clearview AI, an app that claims to have compiled a database of more than 3 billion images from sources such as Facebook, YouTube and Venmo. All of this was done without permission of the subjects. Linked to a pair of reality-augmented eyeglasses, Clearview AI-equipped members of law enforcement and security agencies can walk down the street and identify anyone they see, along with their names, addresses and other vital information.

Credit: University of Chicago

The tool certainly can be used for good. Federal and state law enforcement officers, according to the Times, say the app helped solve murders, shoplifting crimes, identity theft, credit card fraud, and child sexual exploitation cases.

But there's a potential for abuse as well.

Eric Goldman, co-director of the High Tech Law Institute at Santa Clara University, told the Times, "The weaponization possibilities of this are endless. Imagine a rogue law enforcement officer who wants to stalk potential romantic partners, or a foreign government using this to dig up secrets about people to blackmail them or throw them in jail."

Researchers say Fawkes has stumped generally benign facial recognition systems used by Facebook, Microsoft and Amazon. Although Fawkes can successfully thwart Clearview AI recognition as well, its developers say they were not even aware of the program when they began their research.

"Our original goal was to serve as a preventative measure for Internet users to inoculate themselves against the possibility of some third-party, unauthorized model," the team recently stated in a FAQ sheet. "Imagine our surprise when we learned three months into our project that such companies already existed, and had already built up a powerful model trained from massive troves of online photos. It is our belief that Clearview AI is likely only the (rather large) tip of the iceberg."

The developers clearly defined how they measure success: "If we can reduce the accuracy of these models to make them untrustable, or force the model's owners to pay significant per-person costs to maintain accuracy, then we would have largely succeeded."

More information:
sandlab.cs.uchicago.edu/fawkes/

Fawkes: Protecting Privacy against Unauthorized Deep Learning Models, arXiv:2002.08327 [cs.CR]
arxiv.org/abs/2002.08327

APA citation: Image cloaking tool thwarts facial recognition programs (2020, August 5) retrieved 21 October 2020 from https://techxplore.com/news/2020-08-image-cloaking-tool-thwarts-facial.html