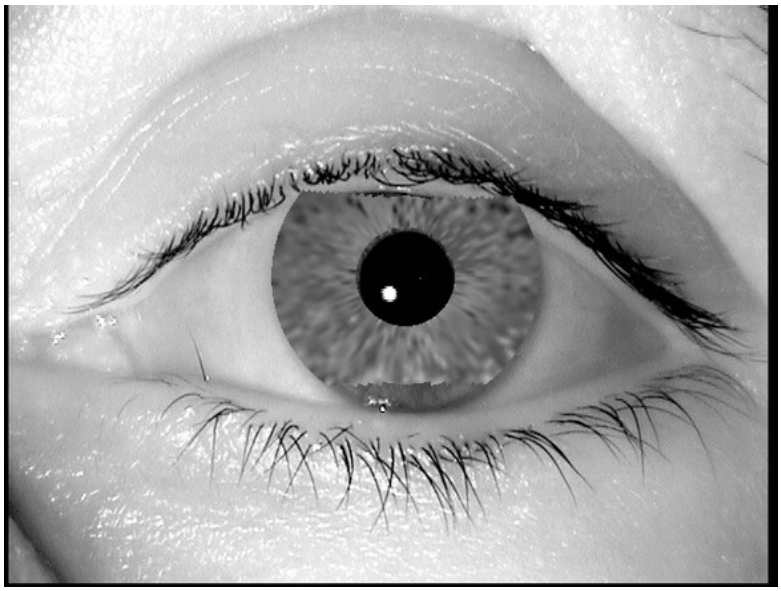
KIM ZETTER SECURITY 07.25.12 06:00 AM

REVERSE-ENGINEERED IRISES LOOK SO REAL, THEY FOOL EYE-SCANNERS



Researchers reverse-engineered iris codes to create synthetic eye images that tricked an iris-recognition system into thinking they were authentic. Can you tell if this is the real image or the synthetic one? ALL IMAGES COURTESY OF JAVIER GALBALLY

LAS VEGAS – Remember that scene in *Minority Report* when the spider robots stalk Tom Cruise to his apartment and scan his iris to identify him?

Things could have turned out so much better for Cruise had he been wearing a pair of contact lenses embossed with an image of someone else's iris.

New research being released this week at the Black Hat security conference by academics in Spain and the U.S. may make that possible.

The academics have found a way to recreate iris images that match digital iris codes that are stored in databases and used by iris-recognition systems to identify people. The replica images, they say, can trick commercial iris-recognition systems into believing they're real images and could help someone thwart identification at border crossings or gain entry to secure facilities protected by biometric systems.

The work goes a step beyond previous work on iris-recognition systems. Previously, researchers have been able to create wholly synthetic iris images that had all of the characteristics of real iris images – but weren't connected to real people. The images were able to trick iris-recognition systems into thinking they were real irises, though they couldn't be used to impersonate a real person. But this is the first time anyone has

subjects, creating the possibility of stealing someone's identity through their iris.

"The idea is to generate the iris image, and once you have the image you can actually print it and show it to the recognition system, and it will say 'okay, this is the [right] guy,'" says Javier Galbally, who conducted the research with colleagues at the Biometric Recognition Group-ATVS, at the Universidad Autonoma de Madrid, and researchers at West Virginia University.

Is this real? OR IS THIS?

IS THIS REAL?

Iris-recognition systems are rapidly growing in use around the world by law enforcement agencies and the commercial sector. They're touted as faster, more sanitary and more accurate than fingerprint systems. Fingerprint systems measure about 20-40 points for matching while iris recognition systems measure about 240 points.

Schipol Airport in the Netherlands allows travelers to enter the country without showing a passport if they participate in its Privium iris recognition program. When travelers enroll in the program, their eyes are scanned to produce binary iris codes that are stored on a Privium card. At the border crossing, the details on the card are matched to a scan taken of the cardholder's eye to allow the person passage.

Since 2004, airports in the United Kingdom have allowed travelers registered in its iris-recognition program to pass through automated border gates without showing a passport, though authorities recently announced they were dropping the program because passengers had trouble properly aligning their eyes with the scanner to get automated gates to open.

Google also uses iris scanners, along with other biometric systems, to control access to some of its data centers. And the FBI is currently testing an iris-recognition program on federal prison inmates in 47 states. Inmate iris scans are stored in a database managed by a private firm named BI2 Technologies and will be part of a program aimed at quickly identifying repeat offenders when they're arrested as well as suspects who provide false identification.

When someone participates in an iris-recognition system, his or her eyes are scanned to create iris codes, which are binary representations of the image. The iris code, which consists of about 5,000 bits of data, is then stored in a database for matching. The iris code is stored instead of the iris image for security and privacy reasons.

When that person then later goes before an iris-recognition scanner - to obtain access to a facility, to cross a border or to access a computer, for example - their iris is scanned and measured against the iris code stored in the database to authenticate the person's identity.

It's long been believed that it wasn't possible to reconstruct the original iris image from an iris code stored in a database. In fact, B12 Technologies says on its web site that biometric templates "cannot be

short, biometrics can be thought of as a very secure key: Unless a biometric gate is unlocked by using the right key, no one can gain access to a person's identity."

But the researchers showed that this is not always the case.

AND THIS?

WHAT ABOUT THIS?

Their research involved taking iris codes that had been created from real eye scans as well as synthetic iris images created wholly by computers and modifying the latter until the synthetic images matched real iris images. The researchers used a genetic algorithm to achieve their results.

Genetic algorithms are tools that improve results over several iterations of processing data. In this case, the algorithm examined the synthetic images against the iris code and altered the images until it achieved one that would produce a near identical iris code as the original iris image when scanned.

"At each iteration it uses the synthetic images of the previous iteration to produce a new set of synthetic iris images that have an iris code which is more similar (than the synthetic images of the previous iteration) to the iris code being reconstructed," Galbally says.

It takes the algorithm between 100-200 iterations to produce an iris image that is "sufficiently similar" to one the researchers are trying to reproduce.

Since no two images of the same iris produce the same iris code, iris recognition systems use a "similarity score" to match an image to the iris code. The owner of the scanner can set a threshold that determines how similar an image needs to be to the iris code to call it a match.

The genetic algorithm examines the similarity score given by the recognition system after each iteration and then improves the next iteration to obtain a better score.

"The genetic algorithm applies four ... rules inspired in natural evolution to combine the synthetic iris images of one iteration in such a way ... that they produce new and better synthetic iris images in the next generation – the same way that natural species evolve from generation to generation to adapt better to their habitat but in this case it is a little bit faster and we don´t have to wait millions of years, just a few minutes," Galbally says.

Galbally says it takes about 5-10 minutes to produce an iris image that matches an iris code. He noted, though, that about 20 percent of the iris codes they attempted to recreate were resistant to the attack. He thinks this may be due to the algorithm settings.

Once the researchers perfected the synthetic images, they then scanned them against a commercial iris recognition system, and found that the scanner accepted them as matching iris images more than 80

Neurotechnology.

VeriEye's algorithm is licensed to makers of iris-recognition systems and recently ranked among the top four in accuracy out of 86 algorithms tested in a competition by the National Institute of Standards and Technology. A Neurotechnology spokeswoman said there are currently 30-40 products using VeriEye technology and more are in development.

The iris codes the researchers used came from the Bio Secure database, a database of multiple kinds of biometric data collected from 1,000 subjects in Europe for research use by academics and others. The synthetic images were obtained from a database developed at West Virginia University.

After the researchers had successfully tricked the VeriEye system, they wanted to see how the reconstructed images would fare against real people. So they showed 50 real iris images and 50 images reconstructed from iris codes to two groups of people – those who have expertise in biometrics those who are untrained in the field. The images tricked the experts only 8 percent of the time, but the non-experts were tricked 35 percent of the time on average, a rate that is very high given there is a 50/50 chance of guessing correctly. It should be noted that even with their high rate of error, the non-expert group still scored better than the VeriEye algorithm.

The study assumes that someone conducting this kind of attack would have access to iris codes in the first place. But this might not be so hard to achieve if an attacker can trick someone into having their iris scanned or hacks into a database containing iris codes, such as the one that B12 technologies maintains for the FBI.

BI2 states on its web site that the iris images in its database are "encrypted using strong cryptographic algorithms to secure and protect them," but the company could not be reached to obtain details about how exactly it secures these images. Even if BI2's database is secure, other databases containing iris codes may not be.

(From left-right) A young Geoff Ramsey, Gustavo Sorola and Burnie Burns record dialogue for Red vs. Blue Image: Rooster Teeth

SOLUTION: THE PICTURE AT THE TOP OF THE POST IS A SYNTHETIC IRIS IMAGE. IN THE FIRST SET OF IMAGES BELOW THAT, THE ONE ON THE LEFT IS REAL, THE OTHER SYNTHETIC. IN THE SECOND SET OF IMAGES, THE ONE ON LEFT IS REAL, THE ONE ON RIGHT SYNTHETIC. AND THIS FINAL ONE? AUTHENTIC. LOOK HARD, AND YOU CAN EVEN SEE THE CONTACT LENS SURROUNDING THE IRIS.

#CYBERSECURITY

VIEW COMMENTS