"BRAINPRINT" BIOMETRIC ID HITS 100% ACCURACY

Could an EEG-based system be the perfect biometric key for really high security situations?

Psychologists and engineers at Binghamton University in New York say they've hit a milestone in the quest to use the unassailable inner workings of the mind as a form of biometric identification. They came up with an electroencephalograph system that proved 100 percent accurate at identifying individuals by the way their brains responded to a series of images. But EEG as a practical means of authentication is still far off.

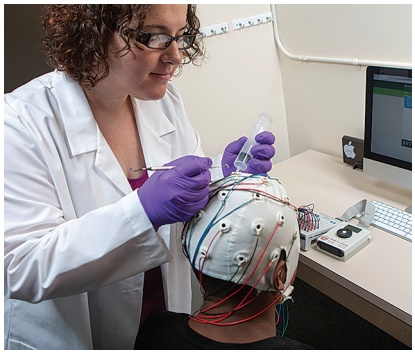
Many earlier attempts had come close to 100 percent accuracy but couldn't completely close the gap. "It's a big deal going from 97 to 100 percent because we imagine the applications for this technology being for high-security situations," says Sarah Laszlo, the assistant professor of psychology at Binghamton who led the research with electrical engineering professor Zhanpeng Jin.

Perhaps as important as perfect accuracy is that this new form of ID can do something fingerprints and retinal scans have a hard time achieving: It can be "canceled."

Fingerprint authentication can be reset if the associated data is stolen, because that data can be stored as a mathematically transformed version of itself, points out Clarkson University biometrics expert Stephanie Schuckers. However, that trick doesn't work if it's the fingerprint (or the finger) itself that's stolen. And the theft part, at least, is easier than ever. In 2014 hackers claimed to have cloned German defense minister Ursula von der Leyen's fingerprints just by taking a high-definition photo of her hands at a public event.

Several early attempts at EEG-based identification sought the equivalent of a fingerprint in the electrical activity of a brain at rest. But this new brain biometric, which its inventors call CEREBRE, dodges the cancelability problem because it's based on the brain's responses to a sequence of particular types of images. To keep that ID from being permanently hijacked, those images can be changed or re-sorted to essentially make a new biometric passkey, should the original one somehow be hacked.

CEREBRE, which Laszlo, Jin, and colleagues described in *IEEE Transactions in Information Forensics and Security*, involves presenting a person wearing an EEG system with images that fall into several categories: foods people feel strongly about, celebrities who also evoke emotions, simple sine waves of different frequencies, and uncommon words. The words and images are usually black and white, but occasionally one is presented in color because that produces its own kind of response.



OPEN YOUR MIND: Binghamton University professor Sarah Laszlo prepares to peer into the peculiarities of a person's brainwaves.

Each image causes a recognizable change in voltage at the scalp called an event-related potential, or ERP. The different categories of images involve somewhat different combinations of parts of your brain, and they were already known to produce slight differences in the shapes of ERPs in different people. Laszlo's hypothesis was that using all of them—several more than any other system—would create enough different ERPs to accurately distinguish one person from another.

The EEG responses were fed to software called a classifier. After testing several schemes, including a variety of neural networks and other machine-learning tricks, the engineers found that what actually worked best was a system based on simple cross correlation.

In the experiments, each of the 50 test subjects saw a sequence of 500 images, each flashed for 1 second. "We collected 500, knowing it was overkill," Laszlo says. Once the researchers crunched the data they found that just 27 images would have been enough to hit the 100 percent mark.

The experiments were done with a high-quality research-grade EEG, which used 30 electrodes attached to the skull with conductive goop. However, the data showed that the system needs only three electrodes for 100 percent identification, and Laszlo says her group is working on simplifying the setup. They're testing consumer EEG gear from Emotiv and NeuroSky, and they've even tried to replicate the work with electrodes embedded in a Google Glass, though the results weren't spectacular, she says.

For EEG to really be taken seriously as a biometric ID, brain interfaces will need to be pretty commonplace, says Schuckers. That might yet happen. "As we go more and more into wearables as a standard part of our lives, [EEGs] might be more suitable," she says.

But like any security system, even an EEG biometric will attract hackers. How can you hack something that depends on your thought patterns? One way, explains Laszlo, is to train a hacker's brain to mimic the right responses. That would involve flashing light into a hacker's eye at precise times while the person is observing the images. These flashes are known to alter the shape of the ERP.

"The awesome part of this—the crazy science-fiction part—is to see if the attitude of the hacker changes to be more like" the target of the hack, she says.

—SAMUEL K. MOORE

JONATHAN COHEN/BINGHAMTON UNIVERSITY