COMMONLIT

Name: _____ Class: _____

Biometrics: New IDs that are uniquely you

Forget fingerprints: In the near future, eyebrows or heartbeats may become your new IDs

By Sharon Oosthoek
2014

Police and law enforcement have historically used fingerprints to identify suspects and prosecute criminals. But now, using new technology and the science of biometrics, scientists have developed a different, and potentially more advanced, way of identifying people. As you read, take notes on how this technology works, and how it can be used beneficially.

[1] On April 18, 2013, the Federal Bureau of Investigation (FBI) released blurry photos of two suspects at the scene of the Boston Marathon bombing.[1] Marios Savvides and his team quickly tried to identify them.

"fingerprint" by CCOA is licensed under CC BY-ND 2.0.

Savvides works at Carnegie Mellon University in Pittsburgh, Pa., as a scientist specializing in pattern recognition and signal processing. He creates special software that can identify people in digital images. As he and his fellow experts began sifting through the FBI pictures, they faced a challenge. Even the best picture of one of the suspects "was extremely low-resolution," Savvides recalls. "It was blurred, off-angle and he was wearing a hat."

Still, the team worked through the night. Using their experimental face-recognition software, they enhanced the photo. In the morning, they sent it off to the FBI. By that time, law enforcement already had identified the two suspects. "Still, after the fact, we saw our reconstruction was pretty darn good," Savvides says.

Today, he is working to make the software even better. To do this, he and his team are using something called biometrics. It's a relatively new field of technology, Savvides notes. The name explains it all: "*Bio* means life," he says. "*Metrics* is about measuring." So biometrics measures features or characteristics — individually or in combination — that are unique to some person. No one else will share exactly the same features.

[5] Fingerprints probably represent the best-known example of a feature useful in biometrics. Others include the iris (the colored muscle in the eye) and the face. Biometrics engineers are looking to find still more. Any feature of the body with a unique shape, size, texture or pattern — and that can be read by biometric technologies — potentially can be used to identify someone.

1. The Boston Marathon bombing was a terrorist attack, followed by subsequent related shootings, that occurred when two pressure cooker bombs exploded during the Boston Marathon on April 15, 2013.

Rapidly and accurately identifying people is useful. The police sometimes use biometric technology to ID criminals, disaster victims and missing children. Bank tellers may use biometrics to verify the identity of anyone attempting to withdraw money from an account. Because of the usefulness of biometric technology, governments are starting to include fingerprint and other biometric data in driver's licenses, ID cards and passports.

Research on biometrics is advancing rapidly. Here we meet researchers behind three teams developing new ways to ID people. Their work is leading to the creation of electronic devices and security systems that one day may recognize us almost instantly and effortlessly.

Lego lessons

Savvides' specialty is facial biometrics. He creates step-by-step instructions, called algorithms, for a computer program to follow. The instructions tell the computer how to fill in the parts of a face that either don't show up in a photo or are too low-quality and blurry to recognize.

"Let's say the face is made up of Lego blocks," says Savvides. "You can create an algorithm that knows which Lego blocks to use at what location." For instance, the first line in a set of mathematical instructions written by Savvides might tell the program to place two small, dark green blocks in the center. They would represent the eyes. The second line might tell the computer to add 103 large light beige blocks in an oval pattern around the edge. These blocks would represent the outline of the head. The result will be the building plan for a simple biometric signature of the face.

[10] Using a powerful computer, Savvides designed one algorithm that can enhance a small and blurry face. It automatically generates a larger and more detailed image. He taught the computer program to do this by having it compare thousands of matched pairs of faces. Each pair included one blurry image and one sharp image of the same face.

Now, when Savvides scans a new blurry face into his computer, his algorithm applies the lessons it had learned earlier from analyzing those thousands of matched pairs of photos. In short order, the program pops out a sharpened version of the once-blurry face.

The enhanced version may not be an exact likeness of the person in the photo. Still, it's usually close. Certainly, it can be close enough for police to use in comparing against clearer photos of possible suspects.

"We have a long way to go before we start trusting computers 100 percent," says Savvides. "We still want humans involved in making the final identification."

He has used the same compare-and-match technique to teach a computer to turn a two-dimensional[2] photo of a face into a three-dimensional one. That means instead of seeing a face just from a single angle, law enforcement officials now can rotate and turn that head on a computer screen. This allows them to view the face from any angle — including the same angle as the face in some photo. Now the police can make a 2-D view of this rotated face and see if it matches the person in the original photo.

2. **Two-dimensional** ***(adjective):*** (or 2-d) something that is portrayed on a planar surface, meaning it has height and width, but no depth. A photo, for instance, is a two-dimensional representation of something in the three-dimensional world.

[15] Savvides even has a strategy for taking into account how faces change as people age. Imagine the police are looking for a young man missing since childhood. The only photograph they have was taken when a boy was just 12. Now he is 25 — and police think they have spotted him in a recent photo.

Savvides' research shows that eyes and eyebrows stay the same over time, so he asks the computer to match just those features in the two pictures. Since the computer is not looking at the entire face, any match may not be foolproof. But it could narrow down the number of candidates.

And if the photos reveal a clear image of the iris, a computer will have even better luck in matching the man to his 12-year-old self. The colored muscle surrounding the pupil of the eye is much more detailed. It also is unique — and won't have changed as the boy grew into a man.

In fact, the pattern of light reflected by the iris never changes. That is why its pattern forms the basis of some security locks. (The technology often shows up in movies and television programs.)

Putting your heart into it

Biometric programs that rely on facial features are among the most common ways to identify people. But Foteini Agrafioti and Karl Martin are developing a system that would work even if no part of the body were visible. You might say they are taking biometrics to heart. Their technology works by measuring a heart's electrical patterns.

[20] In 2011, the two engineers created a wristband called Nymi (NEE-me) that measures the electrical signals created by its wearer's heart. The signals match the rhythm of the heartbeat. And these are unique to each of us. That makes them useful as a sort of biometric password — the type that can allow someone to log onto a computer. No need to remember a complicated password that contains a string of letters, numbers and other symbols.

The engineers came up with the idea when they were getting their PhDs — Agrafioti in electrical and computer engineering, and Martin in engineering science — at the University of Toronto, in Ontario, Canada.

Their wristband includes sensors that read the electrical signal a heart gives off each time it beats. That reading is called an electrocardiogram, or ECG. It's the same test that hospitals use to monitor a patient's heart.

The ECG measures the shape of a heart's electrical signal. When your heart beats fast — such as after a run — the signal will constrict and repeat faster. But its shape stays the same.

When you sit down to work, the wristband can wirelessly transmit that shape to your computer. There, a computer program can compare the pattern to one previously stored on its hard drive. Only if the two match will the computer log you on. And you stay logged on until you take off the wristband — or walk away.

[25] In 2011, Agrafioti and Martin founded a company in Toronto called Bionym to sell the wristbands. Sales should start late in 2014. The $79 wristbands are being designed for use with tablets, cell phones and computers.

In the future, the engineers hope their wristband will open all sorts of doors — literally — for wearers. One day it might allow homeowners to unlock the door to their house or their car. It even could be used to withdraw cash from an ATM.

Martin says the goal is to create a single wearable item to replace all the smart cards, keys and passwords people now use. All of these tools allow us to let technology know who we are, Martin says. "It's not only easier, but also more interesting to create a single technology that a person can wear on their body" to replace all of those separate objects.

And finally, stealing the wristband would do a thief no good. That's because it is someone's heartbeat, not the wristband, that would actually unlock something.

'Fingerprints' from blood vessels

But using a heartbeat to identify someone is a relatively new form of biometrics. Fingerprints have a much longer history. Police have relied on them to help catch criminals for at least a century.

[30] The ridges on our fingertips create unique patterns that don't change, even as we age. These ridges contain tiny pores through which we sweat. That means each time we touch something, we leave behind a little sweat in the pattern of that print.

When investigating a crime, police often look for fingerprints. Investigators can capture an image of a print by taking a picture of it. Or they can transfer a print to a piece of sticky tape. Later, if a fingerprint lifted from the scene of a crime matches one on file, police know that person was at the scene. Then they can start investigating whether that person might be the criminal.

Using fingerprints to identify someone has its limits. It can be hard to get a good print from people who have worn down the skin on their fingers after years of working with rough materials, such as brick or stone. It also can be hard to get good fingerprints from young children. Their ridges are just too tiny and narrow.

Rob Rowe has designed a hand-held fingerprint scanner that solves these problems. An optical physicist, Rowe studies light and how it interacts with things.

The scanner looks like a tall computer mouse with a finger-shaped pad on top. When someone places a finger on the pad, different colors of light illuminate it from below.

[35] Each color (wavelength[3]) of light travels harmlessly through the skin into the finger. The light travels all the way to the blood vessels. Those vessels scatter and absorb the light in different ways, depending on the wavelength of light that had been used.

3. A wavelength is the distance between one peak and the next in a series of waves, or the distance between one trough and the next. Visible light — which, like all electromagnetic radiation, travels in waves — includes wavelengths between about 380 nanometers (violet) and about 740 nanometers (red). Radiation with wavelengths shorter than visible light includes gamma rays, X-rays and ultraviolet light. Longer-wavelength radiation includes infrared light, microwaves and radio waves.

As each wavelength of light bounces back to the scanner, it creates a pattern tracing out the blood vessels within the finger. The scanner then puts together all those separate images to produce a single, master pattern.

"It turns out blood vessels and other structures below the skin have the same shape as the fingerprint on the surface of the finger," says Rowe, who helped found a company to sell the scanners. So an image of those vessels is just as good as a fingerprint, if not better.

Beyond law enforcement

VaxTrac is an organization based in Washington, D.C. It works around the world to help poor and developing countries do a better job of vaccinating[4] children. In 2013, it started using Rowe's fingerprint scanner in the West African country of Benin.

Health workers there have so far scanned the fingers of more than 20,000 children. The kids are not suspected of crimes. Instead, their prints reveal whether they already have received vaccines against life-threatening diseases.

[40] The fingerprint scanner sends a message to a central computer. Inside the computer, a database contains information about what vaccines a child has received and when. The "username" for each medical file is the child's fingerprint. Health officials tap into this file, using the fingerprint scanner, to accurately identify which children still need vaccinating — and which don't.

"Without a record of a child's vaccination, we usually re-vaccinate them," says VaxTrac project manager Meredith Baker. "Using the scanner, we don't waste vaccine."

Using biometrics to keep kids healthy, log onto electronic devices and catch criminals are important applications. But all three teams already are looking to other uses. They want to refine their research for use in exciting new applications.

Savvides, for example, dreams of smart robots that do our bidding, before we even ask.

"We eventually want to use facial recognition in robots that can identify who you are. How cool would it be to have a robot that could say, 'Hi Marios, how are you doing today?'" It also would know your every preference. After recognizing you, a robot butler could let you into your house, adjust the air temperature and put on your favorite music.

[45] "That's how I see biometrics being used in the future," he says. "It may seem far away. But some day it will happen."

4. A vaccine is a biological mixture that resembles a disease-causing agent. It is given to help the body create immunity to a particular disease.

Text-Dependent Questions

Directions: For the following questions, choose the best answer or respond in complete sentences.

1. PART A: Which TWO of the following best identify the main ideas of this article? [RI.2]
   A. Fingerprints are still the most accurate way to identify a person.
   B. Blood vessels have the same structure as fingerprints.
   C. Biometric features are slightly different in everyone.
   D. Biometrics is the measurement of life.
   E. Biometric technology can help in areas of security, privacy, and health.
   F. Children in West Africa desperately need vaccines.

2. PART B: Which TWO sentences from the article best support the answers to Part A? [RI.1]
   A. "Fingerprints probably represent the best-known example of a feature useful in biometrics." (Paragraph 5)
   B. "Any feature of the body with a unique shape, size, texture or pattern … potentially can be used to identify someone." (Paragraph 5)
   C. "It can be hard to get a good print from people who have worn down the skin on their fingers after years of working with rough materials, such as brick or stone." (Paragraph 32)
   D. "Health officials tap into this file, using the fingerprint scanner, to accurately identify which children still need vaccinating…" (Paragraph 40)
   E. "Using biometrics to keep kids healthy, log onto electronic devices and catch criminals are important applications." (Paragraph 42)
   F. "We eventually want to use facial recognition in robots that can identify who you are." (Paragraph 44)

3. Which of the following best describes the relationship between the Boston Marathon bombing and biometrics? [RI.3]
   A. Because of the newly developed biometric technology, the FBI was able to quickly identify two suspects.
   B. The blurry photos released by the FBI after the bombing prompted researchers to improve their early biometric software.
   C. Because biometric technology was unavailable at the time, the Boston Marathon bomber remains at large.
   D. The Boston Marathon bombing made researchers aware of how biometric technology is sometimes useless and ineffective.

4. Which statement best states how the author conveys her purpose for writing the article? [RI.6]
   A. The author presents her opinions on why biometric technology is helpful.
   B. The author presents various researchers who are using biometric technology in a variety of ways.
   C. The author provides evidence that supports the claim that old methods of identification are unhelpful.
   D. The author presents the progress she has made in the field of biometrics.

5. PART A: In paragraph 40, the text says, “the ‘username’ for each medical file is the child’s fingerprint.” Which of the following best explains the meaning of this statement? [RI.4]
   A. The child’s vaccination record is labeled with a picture of their fingerprint.
   B. The child’s vaccination record also contains information about their fingerprint.
   C. The child’s fingerprint is the only way they can be vaccinated.
   D. The child’s vaccination record is directly linked to their fingerprint.

6. PART B: Which detail from the text best supports the answer for Part A? [RI.1]
   A. “"It turns out blood vessels and other structures below the skin have the same shape as the fingerprint on the surface of the finger...”” (Paragraph 37)
   B. “Health workers there have so far scanned the fingers of more than 20,000 children.” (Paragraph 39)
   C. “Health officials tap into this file, using the fingerprint scanner, to accurately identify which children still need vaccinating — and which don’t.” (Paragraph 40)
   D. “‘Without a record of a child’s vaccination, we usually re-vaccinate them,’ says VaxTrac project manager Meredith Baker.” (Paragraph 41)

7. Which TWO of the following quotes from the text best summarize the benefits of Rob Rowe’s fingerprint scanner? [RI.1]
   A. "When investigating a crime, police often look for fingerprints... Later, if a fingerprint lifted from the scene of a crime matches one on file, police know that person was at the scene." (Paragraph 31)
   B. "It can be hard to get a good print from people who have worn down the skin on their fingers... It also can be hard to get good fingerprints from young children" (Paragraph 32)
   C. "An optical physicist, Rowe studies light and how it interacts with things." (Paragraph 33)
   D. “When someone places a finger on the pad, different colors of light illuminate it from below.” (Paragraph 34)
   E. “As each wavelength of light bounces back to the scanner, it creates a pattern tracing out the blood vessels within the finger.” (Paragraph 36)
   F. "'It turns out blood vessels and other structures below the skin have the same shape as the fingerprint on the surface of the finger,' ... So an image of those vessels is just as good as a fingerprint, if not better." (Paragraph 37)

8. How does Savvides’ Lego explanation help explain how his biometric algorithm works? [RI.5]

_____

_____

_____

_____

_____

_____

_____

Discussion Questions

Directions: Brainstorm your answers to the following questions in the space provided. Be prepared to share your original ideas in a class discussion.

1. What are some other examples of ways that biometrics might be used in the future? List all of your ideas.

2. In paragraphs 43-45, Savvides describes a future in which machines collect data about our personal habits and preferences. What do you think about this kind of technology? Do you think it will improve our lives? Explain your answer.

3. What are some positive uses for biometrics? Are there any potential drawbacks? Explain your answer.