Ultrasound fingerprint scanners amplify security

Acoustic waves offer 3D print mapping for phones and computers.

Boer Deng

02 July 2015

Christophe Van Biesen/Getty Images

Most fingerprint scanners map a person's unique pattern of ridges and whorls using tiny capacitors.

Smartphones, laptops and payment systems are among the technologies that can be unlocked by fingerprints instead of typed passcodes. But these security systems can be fooled by dirt and grease.

In a paper[1] published on 29 June in *Applied Physics Letters,* engineer David Horsley of the University of California, Davis, and his colleagues describe a system that can read a fingerprint with greater depth than standard devices, and is less prone to malfunctioning during everyday use.

The team says that its technology, which relies on ultrasound, can be incorporated easily into consumer electronics. “We think our approach has a number of benefits,” says Horsley.

Most scanners used in consumer electronic devices today recognize the ridges and valleys of a print by mapping the pattern of voltages generated by a finger pressed against the scanner. When the ridges of a pressed digit contact tiny capacitors on a dedicated chip sensor, the devices produce a certain voltage; where there is a valley, there is no contact and they generate a different voltage.

The pattern of these variations allows the scanner to recognize the fingerprint. But moisture and grime can cause the circuit to close in the wrong places, rendering prints illegible.

The sound of one finger tapping

The ultrasound technology in Horsley's scanning method limits such vulnerability. When a user puts his or her finger to the print-reading chip, an ultrasonic pulse bounces against it. The chip is coated with a layer of aluminium nitride, which can convert mechanical stress to electric energy or vice versa.

When the ultrasonic pulse bounces back off the fingerprint, ridges and valleys return different patterns of stress, which can then be converted into electrical signals. By measuring the bounce from the ultrasound for longer period of time, the scanner can also sense the depth of the ridges and valleys.

The researchers tested their system using a model fingerprint made from a polymer.

Increasingly, engineers believe that scanners capable of reading such 3D prints will enhance security. “If you can sense deeper characteristics, not just the shape, of a fingerprint, you can better tell the difference between what’s real or not,” says Rob Rowe, vice-president of development at security-technology firm HID Biometrics in Albuquerque, New Mexico.

Ultrasound consumer electronics scanners have previously proved difficult to manufacture: lead zirconate titanate, a compound often used for this application, must be heated to some 800 °C before it can be deposited onto a circuit. This process can harm the semiconductors and circuitry at the core of an electronic device.

Some engineers are working on improving other forms of fingerprint recognition. Rowe’s firm, for example, works on scanners that use multiple wavelengths of light to scan beneath the skin. And Horsley hopes that the aluminium nitride used in his system will avoid manufacturing hurdles, because the material is already used in other parts of chip-making.

At least one manufacturer already seems to have worked out how to make ultrasonic fingerprinting workable. In March, Qualcomm, a mobile-technologies company based in San Diego, California, unveiled a demonstration of its own ultrasonic scanner. However, little is known about how the device is made.

Nature | doi:10.1038/nature.2015.17904

References

1. Lu, Y. *et al. Appl. Phys. Lett.* **106**, 263503 (2015).