iPhone 5S fingerprint scanning: Thumbs up or down?

September 13 2013, by Wageeh Boles & Vinod Chandran

Say hello to your new iPhone passcode – so how do fingerprint scanners work? Credit: dhammza

Technology to acquire and use biometric data such as fingerprints has been around for several decades and has made its way from forensic investigation to laptop computers – and now, with this week's introduction of iPhone 5S, to smartphones.

Will it be useful and is it here to stay?

Biometric basics

Biometric systems capture biometric patterns (a person's identifying characteristics or traits) using a sensor, such as a camera or scanner.

There are two main phases of the process:

1. Enrollment phase: features are extracted from a sample (such as a fingerprint) to create a template for the user.

2. Verification phase: when a sample is later presented to the system, features of that sample are matched against the template. If the match is strong enough, the claim of identity is accepted – otherwise, it is rejected.

Implementations of such systems face many challenges because of variations and imperfection in the presentation of the pattern between enrolment and verification.

For example, with fingerprint scanners, a different part of the fingertip may be imaged and it may be rotated.

Besides, some people lose their fingerprint patterns because of burns, and working hands may sometimes be dirty. On top of these, the accuracy of a biometric such as a fingerprint is not anywhere near that of DNA analysis.

Sensor technology and algorithms have, however, improved tremendously over the past couple of decades. Costs have come down and computing power on phones has increased. Time may now be ripe for biometrics on personal devices.

Credit: CPOA

Picking up patterns

Apple iPhone 5S utilises new fingerprint scanning technology – using low frequency radiowaves to map the patterns in the inner dermis (the layer of the skin just below the outer layer, or epidermis, shown in the image below).

The scanned image of the fingerprint will be unaffected by damage to the outer skin layer.

Although patterns on the outer layer involve ridges, valleys and minutiae that can be easily copied from prints left on objects such as door handles or coffee cups and used to create artificial fingerprints, such attacks on security will be more difficult with new technology.

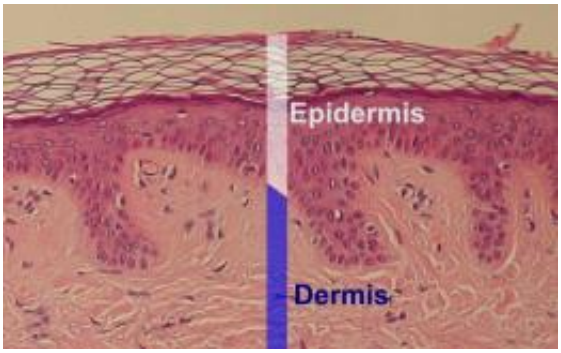
However, the false accept and false reject rates of the new fingerprint image, and the algorithm that Apple uses to verify identity with it, are not known. They can be expected to be equal or better than the use of a four-digit code (or one in 10,000).

Why use fingerprint scans?

A very good reason for fingerprint technology to find its way on the phone now is the need for increased security since smartphones are used to make online purchases. Many consumers prefer to turn off phone lock codes.

Fingertip based verification is done without any extra effort on the part of the consumer and is user-friendly. Transactions such as purchases from iTunes are completed using an identity code (such as the AppleID) and a corresponding password.

Entering the password usually takes a few seconds and the fingerprint verification could make it unnecessary to enter a password as frequently as it is required now without compromising on security.



Credit: Wikimedia Commons

Further, passwords entered in public places using the keypad, or as a traced pattern on the screen of a phone, are susceptible to be lost by "looking over the shoulder" and fingerprints are not revealed in the same manner.

Another reason for the use fingerprints on phones so much later than their use on laptops may be attributed to the availability of sufficient computing power on a phone.

Multiple users

Will the introduction of fingerprint scanners make it more difficult for members of the same family to share an iPhone?

Although published information about the fingerprint scanner on the iPhone indicates that it can store the prints of several fingers, it is not clear to us if it is possible to register more than one user on the system.

Fingerprints, like any other biometric data, cannot be replaced if stolen.

It is also not clear how much of the fingerprint – raw image data or templates or encrypted versions of these – will leave the device and be stored on a cluster or central server. Loss of such data can have serious consequences to security of financial assets and to privacy.

The use of multi-factor authentication and logging of transactions helps lower the risk to security. The risk to privacy is probably a small price to pay for having information right at your fingertips and completing transactions faster than a few keystrokes!

This article was originally published at The Conversation. Read the original article.

Provided by The Conversation