June 10, 2019

Anti-Spoof Detection for In-Screen Fingerprint Sensors

Vishwath Mohan

James Brooks Miller

Anti-Spoof Detection for In-Screen Fingerprint Sensors

Abstract:

User authentication prior to accessing contents of a secured device or container can be achieved in many ways, including textual passwords, picture passwords, locks, keys, or other codes. Many devices also allow for biometric authentication using fingerprint scanners, iris scanners, facial recognition, or the like for increased security and simplified user experience. In concept, a biometric scanner eliminates all but a single individual from obtaining access to the device or container. Nevertheless, many biometric scanners can be fooled, tricked, or spoofed. For example, an unauthorized user can bypass some fingerprint scanners obtaining a latent fingerprint, manipulating a copy of the latent print, and presenting the copy to the fingerprint scanner, which can result in unauthorized access to the device or container. Indeed, improvements in scanning technology and manipulation software have increased the potential for forged fingerprint production. Fingerprint scanners, especially those in smart device displays, can be improved by illuminating a finger, or a purported finger, with multiple differing wavelengths of light as an integral component of fingerprint verification.

Keywords:

In-screen fingerprint sensor, under-screen fingerprint sensor, below-screen fingerprint sensor, under-display fingerprint sensor, user equipment, mobile device, smartphone, organic light emitting diode display, OLED, light emitting diode display, LED, spoof detection, fraud detection, false detection, hack detection, visible light, infrared.

Background:

Many movies, books, television programs, and other stories include a scene in which either a nefarious troublemaker or a resourceful protagonist "lifts" a fingerprint of a target from an unattended object, such as a glass, a mirror, or a screen. The nefarious troublemaker or resourceful protagonist then uses this lifted fingerprint to access a biometrically secured system by impersonating the target. No longer the subject matter of fictional writing and production, biometric access and biometric impersonation continue to become both more helpful and more problematic as more and more devices include biometric security and access systems. For example, personal smartphones, home-security systems, safety-deposit boxes, and many other locations containing intimate and private data, belongings, and information, often feature some type of biometric-recognition component. The nefarious troublemaker or the resourceful protagonist may often repurpose other technological advancements, such as scanners, printers, cameras, and display screens, to engage in sophisticated techniques that used to be reserved for espionage-like specialists to bypass or spoof biometric recognition and security systems.

Description:

User authentication prior to accessing contents of a secured device or container can be achieved in many ways, including textual passwords, picture passwords, locks, keys, or other codes. Many devices also allow for biometric authentication using fingerprint scanners, iris scanners, facial recognition, or the like for increased security and simplified user experience. In concept, a biometric scanner eliminates all but a single individual from obtaining access to the device or container. Nevertheless, many biometric scanners can be fooled, tricked, or spoofed. For example, an unauthorized user can bypass some fingerprint scanners obtaining a latent fingerprint, manipulating a copy of the latent print, and presenting the copy to the fingerprint

scanner, which can result in unauthorized access to the device or container. Indeed, improvement in scanning technology and manipulation software have increased the potential for forged fingerprint production. Fingerprint scanners, especially those in smart device displays, can be improved by illuminating a finger, or a purported finger, with multiple differing wavelengths of light as an integral component of fingerprint verification.

For simplicity, this publication presents techniques to improve the security performance of a fingerprint reader used in a biometric security system of a device, such as a tablet computing device or a smartphone. Nevertheless, the techniques discussed herein can also be applied in additional biometrically-based scanning authentication systems.

An unauthorized user may lift or otherwise misappropriate a fingerprint in many different ways. For example, consider the following scene in a bar, as illustrated in Figure 1.

Figure 1

Here, a man sits at the bar enjoying a glass of wine. To his left, a woman joins him at the bar. The man may choose to casually turn to his left and engage the woman in conversation. In

so doing, he turns away from his glass of wine. While the man is occupied in conversation with the woman, the man leaves his wine glass, and a fingerprint on the wine glass, unattended. A nefarious troublemaker interested in lifting the man's fingerprint may seize the opportunity and sit at the unoccupied stool to the right of the man.

Figure 2 illustrates a close-up view of the wine glass sitting on the bar to the right of the man. As illustrated in Figure 2, the man left a clear fingerprint on the glass. Unbeknownst to the man, the nefarious troublemaker pulls out a now ubiquitous and almost unnoticed smart phone equipped with a high-resolution camera. In a causal manner, the nefarious troublemaker can snap a photograph of the glass seen in Figure 2, while pretending to take a selfie or otherwise view content on the smartphone.

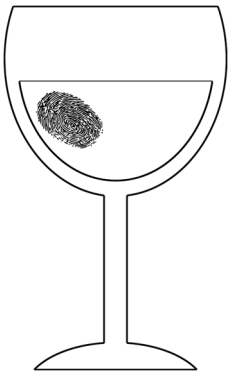

Figure 2

While sitting at the bar, the nefarious troublemaker can process the photograph of the fingerprint using any number of commercially available or free photo-manipulation application software on their smartphone. Such photo-manipulation application software may perform sophisticated manipulation techniques to isolate, highlight, and enhance the photo of the fingerprint. Within a few short moments, the nefarious troublemaker can possess a reliable, accurate, and functional copy of the man's fingerprint, which can be used to impersonate the man

and attempt to gain access the man's smartphone, a home-security system, or other biometrically-secured device or location.

Feeling emboldened by their success, the nefarious troublemaker attempts to access a smartphone or a tablet of the man, which also reside on the bar, while the man continues to engage in conversation with the woman to his left. Figure 3 illustrates a tablet computing device that includes a fingerprint authentication system integrated into the lower-right corner of the display. If able to access the tablet computing device, the nefarious troublemaker may remove or access information, install some form of malware or other unauthorized software, corrupt information, reset the device to factory settings, or any number of untoward and disruptive actions.

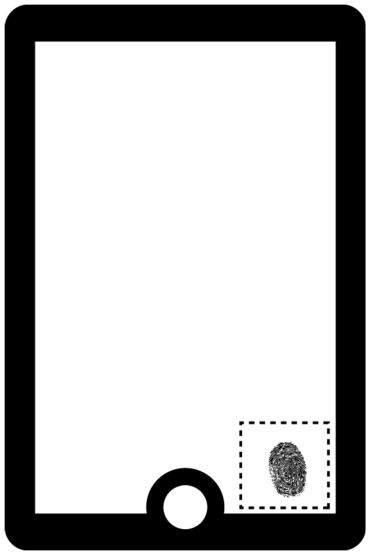

Figure 3

The nefarious troublemaker can present the stolen fingerprint in a number of ways, including printing out a copy on physical paper or displaying the lifted fingerprint on their own smartphone display screen and setting their smartphone on the lower-right corner of the tablet computing device. Other, more-sophisticated techniques of recreating the lifted fingerprint may also be used.

The nefarious troublemaker, however, does not know that the tablet computing device of the man includes an anti-spoofing security system, as illustrated in Figure 4.

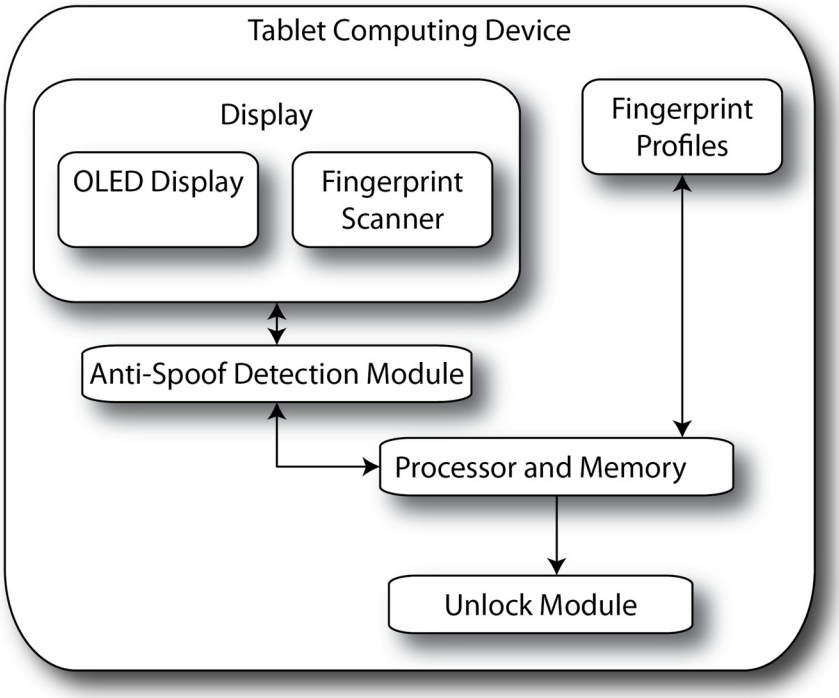

Figure 4

The fingerprint scanner of the tablet computing device does not operate in isolation. The fingerprint scanner works in conjunction with organic light emitting diode (OLED) components of the display and an anti-spoof detection module to compare any received fingerprints with established fingerprint profiles prior to unlocking the tablet computing device.

Unlike some fingerprint scanners, which rely entirely on ambient light or scan entirely in black and white, the fingerprint scanner of the tablet computing device scans the presented fingerprint under the illumination of the OLED display or a separate illuminator (*e.g.*, a light-emitting diode). For example, as illustrated in Figure 5, the display can illuminate the presented finger or fingerprint in the primary colors of red, green, or blue or a combination thereof.

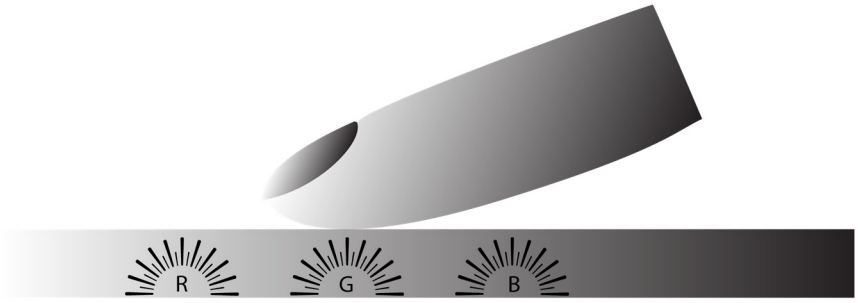

Figure 5

In addition to what is shown in Figure 5, the display can also use other wavelengths of light, such as infrared, in conjunction with the red, green, and blue elements illustrated in Figure 5. The display illuminates the finger by presenting the light in succession, in a cycle, or in predetermined patterns. The anti-spoof detection module can analyze the fingerprint under each of the various light combinations or under multiple combinations of light.

An OLED display can vary the illumination patterns very quickly, which may not even be noticed by a user attempting to access the tablet computing device because the light emitted by the display in fingerprint illumination and verification harmonizes with light already emitted by the display.

Once illuminated, the fingerprint scanner can analyze the received light. The fingerprint scanner can be tailored to conduct image analysis in a broad spectrum of light that matches the output characteristics of the display or other illumination device. A spoofed fingerprint printed on paper or a fingerprint displayed on a screen of another device cannot reflect light in the same manner as a real human finger because of differences in color, skin tone, skin texture, moisture, or geometry. Indeed, all these physical factors can be incorporated into a stored fingerprint profile against which any received fingerprints are compared. Any substantial deviation from the stored

fingerprint profile indicates a spoof attempt, which can result in the anti-spoofing security system actively preventing the tablet computing device from being unlocked.

Additionally, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable collection of user information (*e.g.*, information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user. The user may also choose to not use a biometric scanner to unlock the device. Instead, the user may choose another security feature, such as a username and a password, to unlock their device.

As the number of devices featuring biometric-authentication systems increases, so will the opportunities for untoward individuals to seek unauthorized access to the biometrically-secured devices. In concept, a biometric-authentication system prevents all but a single individual from obtaining access. Fingerprint scanners, especially those in smart device displays, can be improved by illuminating a finger, or a purported finger, with multiple differing wavelengths of light as an integral component of fingerprint verification.

Reference:

[1] Shenzhen Goodix Technology Co., Ltd. and Shenzhen Huiding Technology Co Ltd. Under-screen optical sensor module for on-screen fingerprint sensing. US Pub. 2017/0220838, filed January 31, 2017, and published July 3, 2017.

[2] Jones, Eric, Paul Wickboldt, Patrick Smith, Young Seen Lee, Alvin Jee, Richard Andrew Klenkler, and Bob Lee Mackey. Optical fingerprint sensor under a display. US Pub. 2017/0220844, filed June 30, 2016, and published July 3, 2017.