May 2021

Accounting for Screen Protectors on Smartphones that Utilize an Under-Display Fingerprint Sensor

Firas Sammoura

Omar Sze Leung

Accounting for Screen Protectors on Smartphones that Utilize an Under-Display Fingerprint Sensor

Abstract:

This publication describes techniques and apparatuses to increase biometric security and enhance user experience by accounting for an installation or removal of a screen protector on a smartphone that utilizes an under-display fingerprint sensor (UDFPS) embedded under a display screen. The installation or the removal of the screen protector is detected by the smartphone utilizing the UDFPS, the display screen, or other sensors embedded under the display screen (e.g., an optical proximity sensor).

After detecting the installation or the removal of the screen protector, the smartphone then determines whether a user attempting to gain access to the smartphone is a verified user or an unverified user. To do so, the smartphone prompts the user to utilize an alternative (to biometric) verification process. If the smartphone, using the alternative verification process, determines that the user is a verified user, the smartphone deletes a first enrolled fingerprint image used to match one or more verify fingerprint image(s). Lastly, the smartphone prompts the verified user to start a new enrollment process to capture and save a second enrolled fingerprint image. The smartphone uses the second enrolled fingerprint image to match any future verify fingerprint images until another installation or removal of a screen protector is detected.

Keywords:

Under-display fingerprint sensor, UDFPS, fingerprint sensor, screen protector, smartphone, display screen, biometric security, fingerprint image, enrolled image, verify image

Background:

Computing devices (e.g., a smartphone) often include a fingerprint identification system that enables a user to safeguard their smartphone, application, function, or peripheral using biometric data (e.g., a fingerprint) of the user's finger, thumb, palm, and so forth. A fingerprint identification system may include an under-display fingerprint sensor (UDFPS) embedded under the display screen of the smartphone. To protect the display screen from damage, some users may temporarily or permanently install a screen protector. Meanwhile, other users may use their smartphones without a screen protector.

Screen protectors alter the quality of a fingerprint image by lowering a signal-to-noise ratio (SNR) and/or introducing other undesired effects (e.g., increasing optical and/or acoustic scattering). In addition, a user may install a screen protector that is not approved by a smartphone manufacturer. Furthermore, the user may enroll a fingerprint image before installing a screen protector, and the smartphone uses the enrolled fingerprint image to match one or more verify fingerprint images after the user installs the screen protector, or vice versa. As a result of the installation or the removal of the screen protector after enrollment, the qualities of the enrolled fingerprint image and the verify fingerprint image may not match, for example, due to different SNRs. The mismatch in the qualities of the fingerprint images may increase a false-rejection rate (FRR), a false-acceptance rate (FAR), a spoof-acceptance rate (SAR), and/or an imposter-acceptance rate (IAR) when the user utilizes the UDFPS to access their smartphone. The high FAR, the high SAR, and/or the high IAR may decrease biometric security. For example, an attacker can take advantage of the high FAR, the high SAR, and/or the high IAR to access and/or corrupt the smartphone, in part, by installing or removing a screen protector.

Description:

This publication describes techniques and apparatuses that account for screen protectors, or a lack thereof, on smartphones that utilize a UDFPS. Specifically, accounting for an installation or removal of a screen protector that improves biometric security by lowering the FAR, the SAR, and/or the IAR and improves a user's experience with the smartphone by lowing the FRR, as is illustrated in Figures 1A, 1B, 2A, 2B, and 3.

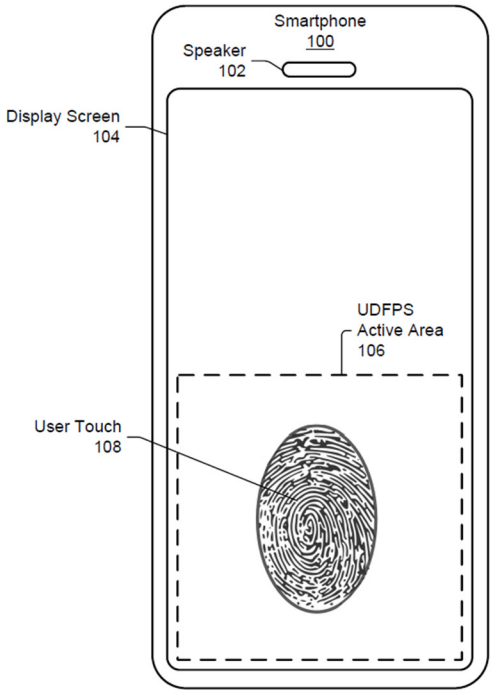

Figure 1A

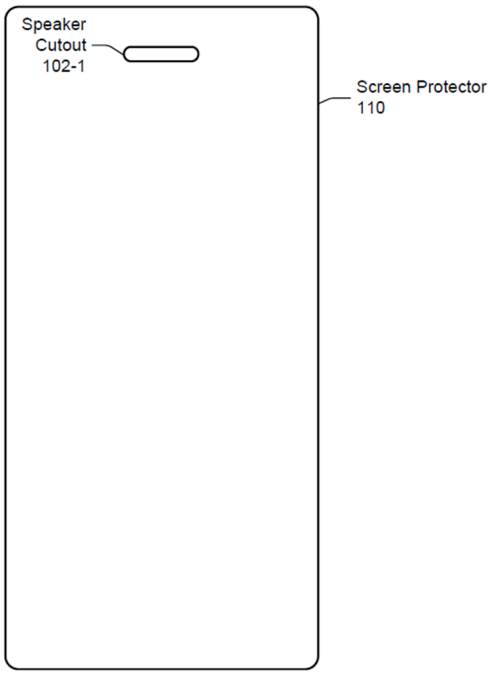

Figure 1B

Figure 1A illustrates a top view of a smartphone 100 with a speaker 102, a display screen 104, and a UDFPS embedded under the display screen 104. A UDFPS active area 106 (illustrated with dashed lines) captures a fingerprint image as the user touches the display screen 104 (illustrated as a user touch 108). The fingerprint image captured by the smartphone 100 (of Figure 1A) without a screen protector 110 (of Figure 1B) may have a considerable signal-to-noise ratio (SNR). Capturing a verify fingerprint image (also referred to as a verify image) with a considerable SNR to be matched to an enrolled fingerprint image (also referred to as an enrolled

image) also with a considerable SNR, helps lower a false-rejection rate (FRR), a false-acceptance rate (FAR), a spoof-acceptance rate (SAR), and/or an imposter-acceptance rate (IAR).

Throughout this disclosure, a "verify fingerprint image" is a fingerprint image used for authentication during a fingerprint verification process. On the other hand, an "enrolled fingerprint image" is an image that the smartphone 100 captures during an enrollment process, for example, when the user first sets up the smartphone or an application. Also, as described herein, an "enrolled template" can be a mathematical representation of the enrolled image.

Figure 1B illustrates a top view of the screen protector 110. The screen protector 110 may be adhered on the front side (display screen side) of the smartphone 100 and, as illustrated in Figures 1A and 1B, covers an area larger than the display screen 104. To avoid covering the speaker 102, the screen protector 110 includes a speaker cutout 102-1. The screen protector 110 and other example screen protectors (not illustrated) may or may not be designed and built by the manufacturer of smartphone and may or may not be compatible with the smartphone 100. Specifically, these screen protectors may have different physical, acoustic, and/or optical specifications (e.g., thickness, transmittance), which may adversely affect the quality of a fingerprint image captured by the UDFPS.

For example, assume the user enrolls a fingerprint image (enrolled image) during the enrollment process shortly after purchasing a smartphone with a UDFPS. Later, the user may install a screen protector. After installing the screen protector, using the UDFPS, the user captures verify images to access the smartphone. However, if the smartphone compares the verify images captured after installing the screen protector to the enrolled image captured before the installation of the screen protector, the smartphone may determine the existence of a mismatch in the qualities of the images, as is illustrated in Figures 2A and 2B.

Figure 2A

Figure 2B

Figure 2A illustrates a portion of an enrolled image that a smartphone may capture and store before the user installs a screen protector. For consistency, Figure 2B illustrates the same portion of a verify image that the smartphone captures after the user installs the screen protector. The captured verify image has a reduced signal-to-noise ratio (SNR), which reduces the captured verify image quality. The reduced SNR in the captured verify image of Figure 2B is illustrated as a lighter shade of grey of patterns and/or minutiae compared to the enrolled image of Figure 2A. Although not illustrated, in addition to the reduced SNR, the screen protector may introduce other undesired effects (e.g., optical and/or acoustic scattering), which may further reduce the quality of the captured verify image.

These undesired effects may result in either poor biometric security and/or improperly denying access to the user. Improperly denying access to the user adversely affects the user's experience and may be due to or measured by a high FRR, whereas poor biometric security may be due to or measured by a high FAR, a high SAR, and/or a high IAR. Although Figure 2A represents the enrolled image and Figure 2B represents the verify image in the above-mentioned scenario, it is to be understood that these undesired effects may result in either poor biometric security and/or improperly denying access to the user even in a reverse scenario. Considering the reverse scenario, assume the smartphone captures and stores the fingerprint image of Figure 2B after the user installs a screen protector. Later, the user may remove the screen protector. After

removing the screen protector, the user captures the fingerprint image of Figure 2A to access the smartphone. In this example, a higher-quality verify image compared to a lower-quality enrolled image may also result in a high FAR, a high FRR, a high SAR, and/or a high IAR.

By contrast, a smartphone 100 implementing the disclosed techniques and apparatuses enables and prompts the user to utilize enrolled and verify images of comparable qualities, as is further described with reference to Figure 3.

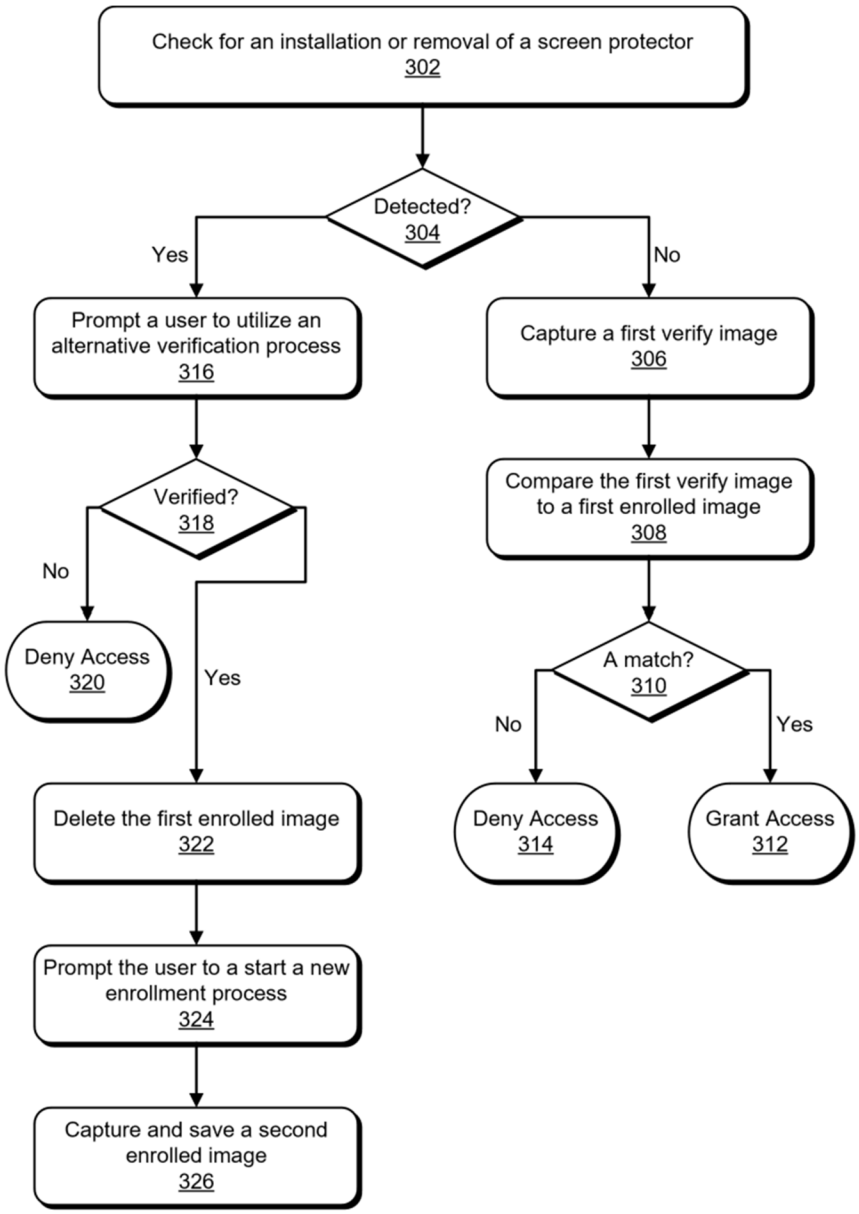

Figure 3

Figure 3 depicts a block diagram that helps describe how the smartphone 100 accounts for an installation or removal of a screen protector when a user utilizes the UDFPS embedded under the display screen 104 of the smartphone 100 to gain access to the smartphone 100.

At stage 302, the smartphone 100 checks for an installation or removal of a screen protector. For example, the smartphone 100 may use the UDFPS itself to check whether a screen protector has been removed or installed. The UDFPS may utilize ultrasonic technology (e.g., an ultrasonic sensor) or optical technology (e.g., a complementary metal-oxide-semiconductor (CMOS) image sensor) to capture a fingerprint image.

If the UDFPS utilizes ultrasonic technology, an associated ultrasonic transmitter sends ultrasonic waves through the display screen 104, or through the display screen 104 and the screen protector 110, and an associated ultrasonic receiver receives reflected ultrasonic waves. The ultrasonic transmitter and the ultrasonic receiver may be part of an ultrasonic transducer. The ultrasonic transducer can detect any changes from a baseline of the reflected ultrasonic waves. The baseline of the reflected ultrasonic waves may include a time-of-flight (ToF) measurement and/or other measurements. In general, the ToF is a measurement of the time it takes an object, a particle, or a wave (e.g., an acoustic wave, an ultrasonic wave, an electromagnetic wave) to travel a distance through a medium. Therefore, if the user or an unverified user installs or removes a screen protector, the ToF measurement either increases (when installing the screen protector) or decreases (when removing the screen protector) from the baseline of the reflected ultrasonic waves.

If the UDFPS utilizes optical technology (e.g., a CMOS image sensor), the CMOS image sensor can measure changes in a phase of a reflected light due to a change in a medium through which the reflected light travels. For example, the CMOS image sensor can detect a change in

reflectivity as a function of the wavelength of the light. The CMOS image sensor can do so by using a specific color (e.g., green, approximately 450 nanometers (nm) to 495 nm) or a spectrum of colors (e.g., a combination of red, green, and blue, approximately 450 nm to 750 nm). Alternatively or additionally, the UDFPS may also utilize a ToF measurement for the time it takes a pulse of light to travel through the display screen 104 versus the time it takes the pulse of light to travel the display screen 104 and the screen protector 110.

The smartphone 100 may also include an optical proximity sensor (not illustrated) embedded under the display screen 104. Like the UDFPS utilizing optical technology, the optical proximity sensor may utilize a ToF measurement to measure whether the user or an unverified user installs or removes a screen protector.

In addition to sensors embedded under the display screen 104, the smartphone 100 may also utilize the display screen 104 to detect an installation or removal of a screen. In aspects, the display screen 104 may utilize organic light-emitting diode (OLED) technology, flexible OLED (FOLED) technology, active-matrix OLED (AMOLED) technology, or any other capacitive touchscreen technology. The smartphone 100 may create a baseline capacitance throughout the entire display screen or at a few select locations at the display screen. Any changes to the baseline capacitance may indicate whether the user or an unverified user installs or removes a screen protector.

In aspects, the smartphone 100 may also use the display screen 104 as a speaker by vibrating the display screen 104 to deliver sound. A resonance of the display screen 104 without the screen protector 110 differs from a resonance of the display screen 104 with the screen protector 110. As such, the smartphone 100 can monitor changes to a baseline resonance to check whether a screen protector was installed or removed. Also, the display screen 104 may utilize an

associated acoustic transmitter to send acoustic (audible) waves through the display screen, or the display screen and the screen protector, and an associated acoustic receiver can receive reflected acoustic waves. The acoustic transmitter and the acoustic receiver may be part of an acoustic wave transducer and can detect any changes from a baseline of the reflected acoustic waves. The baseline of the reflected acoustic waves may include a ToF measurement and/or other measurements.

At stage 304, the smartphone 100 determines whether a screen protector was installed or removed using any of the techniques and apparatuses described at stage 302. If the smartphone 100 does not detect an installation or removal of a screen protector, the smartphone 100, by utilizing the UDFPS, captures a first verify image at stage 306.

At stage 308, the smartphone 100 compares the first verify image to a first enrolled image (first enrolled template). Although not illustrated in Figure 3, if the first verify image has an SNR that differs by a threshold SNR compared to the first enrolled image, the smartphone 100 prompts the user to re-enroll, as is further described below. Therefore, in addition to, or alternatively of, the techniques and apparatuses described at stage 302, the smartphone 100 may also compare the quality of the first verify image to the quality of the first enrolled image to determine whether a screen protector was installed or removed.

Continuing with stage 308, if the quality of the first verify image is comparable to the quality of the first enrolled image, the smartphone 100 utilizes a fingerprint matching algorithm to compare the first verify image to the first enrolled image. As a result, at stage 310, the smartphone 100 determines whether the first verify image matches or mismatches the first enrolled image. If the first verify image matches the first enrolled image, at stage 312, the smartphone 100 grants

access to the user. If the first verify image mismatches the first enrolled image, at stage 314, the smartphone 100 denies access to the user.

Continuing with stage 304, if the smartphone 100 detects an installation or removal of a screen protector using any of the described techniques and apparatuses, at stage 316, the smartphone 100 prompts the user to utilize an alternative verification process (e.g., a username, a passcode, a password, a personal identification number (PIN), or a combination thereof). Using the alternative verification process, at stage 318, the smartphone 100 determines whether the user is a verified (e.g., owner of the smartphone) or an unverified user. If the user is an unverified user, the smartphone 100 denies access at stage 320. If the user is a verified user, the smartphone 100 may delete, deactivate, or phase out the first enrolled image at stage 322.

At stage 324, the smartphone 100 prompts the verified user to start a new enrollment process. The smartphone 100 may guide the user during the new enrollment process. Finally, at stage 326, utilizing the UDFPS, the smartphone 100 captures and saves a second enrolled image. The smartphone 100 uses the second enrolled image to verify any future verify images until another installation or removal of a screen protector is detected.

References:

[1] Patent Publication: US20200363516A1. Ultrasonic Sensor Array Control to Facilitate Screen Protectors. Priority Date: May 16, 2019.

[2] Patent Publication: US20170108961A1. Capacitive Detection of Screen Protector Removal in Mobile Communication Device. Priority Date: October 19, 2015.

[3] Patent Publication: US20190087621A1. Ultrasonic Biometric Sensing Device Integrated with Optics. Priority Date: August 09, 2017.