May 2020

Spoof Detection in Optical Fingerprint Sensors Using Light Scattering

Firas Sammoura

Ion Bita

Spoof Detection in Optical Fingerprint Sensors Using Light Scattering

Abstract:

This publication describes methods, techniques, and apparatuses, implemented on a computing device, directed at detecting spoof fingerprints. In aspects, the addition of a quarter-wave polarizer above an optical fingerprint sensor, along with the utilization of a machine-learned algorithm, can enable a computing device to distinguish a spoof fingerprint from an authentic fingerprint.

Keywords:

Optical fingerprint sensor, biometric recognition systems, biometric authentication, fingerprint matching, authorized access, fingerprint residual, spoof detection, spoof fingerprint, fake fingerprint, spoof rejection, device unlock

Background:

Biometric recognition services provide computing device users personalized and convenient means by which to authenticate themselves and access their device. Fingerprint scanning, in particular, is a well-known and widely used service that enables quick and reliable user authentication on computing devices. The operations of this service, though often enigmatic to users, rely on fundamental principles of light and photography.

Figure 1, below, illustrates the standard implementation of optical fingerprint sensors in computing devices.

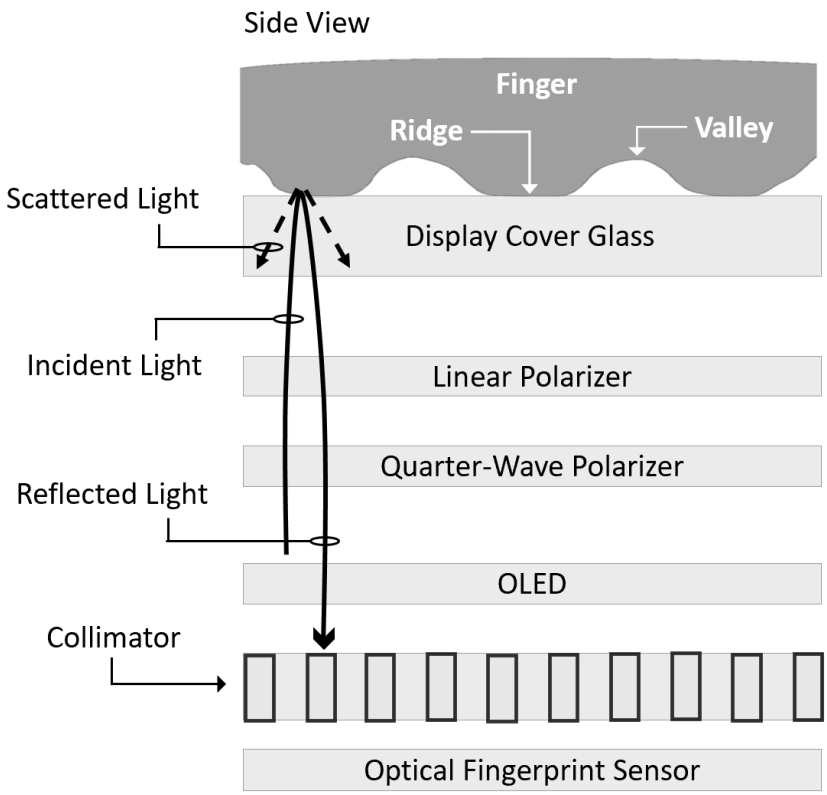

Figure 1

As illustrated, the optical fingerprint sensor is situated beneath a collimator, an organic light-emitting diode (OLED) layer, a quarter-wave polarizer, and a linear polarizer. Altogether, these components are housed under a display cover glass. Computing devices (*e.g.*, smartphones, laptops) may implement optical fingerprint sensors utilizing such a configuration.

During fingerprint authentication, computing devices may require users to place their finger on or above the display cover glass. In response, the OLED layer can illuminate the finger to capture a fingerprint image. Light incident at the skin surface experiences both reflection and scattering. The reflected light maintains identical polarization as the incident light, while the scattered light partially depolarizes. Utilizing the reflected light, the optical fingerprint sensor reconstructs an image of the fingerprint. A fingerprint matcher algorithm (*e.g.*, an algorithm developed to compare biometric identifiers in fingerprints) is then utilized to compare the

fingerprint to the enrolled fingerprint (*e.g.*, the fingerprint captured when security protocols were first initialized) and authenticate the user.

Unfortunately, optical fingerprint sensors are vulnerable to spoof fingerprints: fingerprints that are replicas of authentic fingerprints. For example, an unauthorized user may acquire a user's fingerprints, digitize the lifted fingerprints, post-process them, and print them (*e.g.*, two-dimensional images or three-dimensional molds) to fool a fingerprint sensor and gain access to the user's computing device. As a result, fingerprint spoofs pose serious security and privacy concerns.

Therefore, it is desirable to identify fingerprint spoofs and reject unauthorized users. To this end, the addition of a quarter-wave polarizer above an optical fingerprint sensor, along with the utilization of a machine-learned algorithm, can enable a computing device to distinguish a spoof fingerprint from an authentic fingerprint.

Description:

This publication describes methods, techniques, and apparatuses, implemented on a computing device, directed at detecting spoof fingerprints. In aspects, the addition of a quarter-wave polarizer above an optical fingerprint sensor, along with the utilization of a machine-learned algorithm, can enable a computing device to distinguish a spoof fingerprint from an authentic fingerprint.

Figure 2, below, illustrates an additional quarter-wave polarizer implemented above an optical fingerprint sensor.

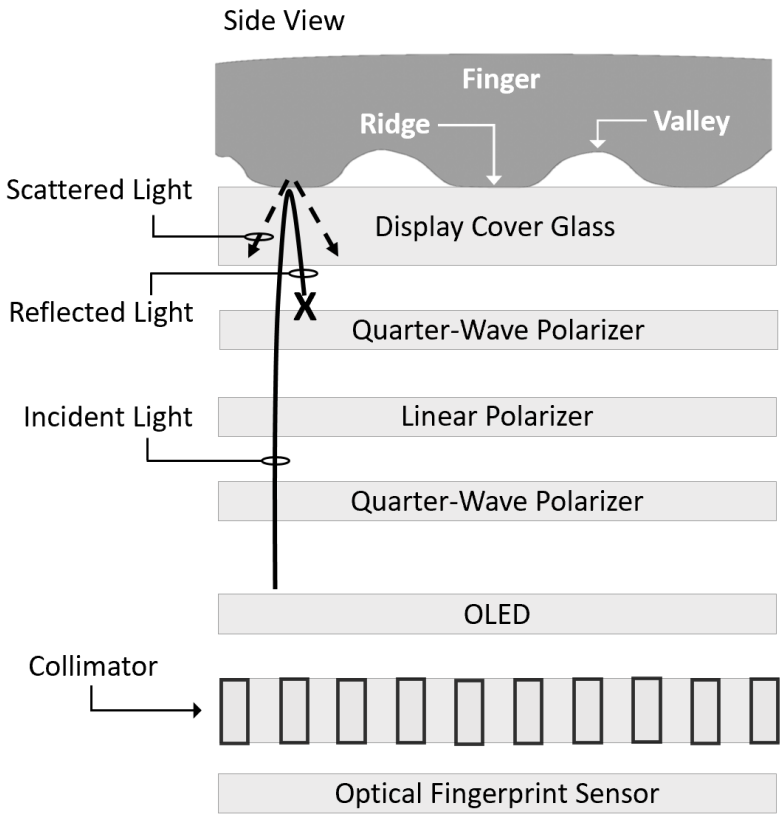

Figure 2

As illustrated, the optical fingerprint sensor is situated beneath a collimator, an OLED layer, a quarter-wave polarizer, a linear polarizer, and an additional quarter-wave polarizer. Altogether, these components are housed under a display cover glass.

During fingerprint authentication, a computing device (*e.g.*, smartphone, laptop) may require a user to place a finger on or above the display cover glass. In response, the OLED layer can illuminate the finger to capture a fingerprint image. Light incident at the skin surface experiences both reflection and scattering. The reflected light maintains identical polarization as the incident light, while the scattered light partially depolarizes. Due to the polarization of the reflected light, the additional quarter-wave polarizer obstructs the reflected light.

The addition of one or more quarter-wave polarizers above an optical fingerprint sensor are configurable in a variety of patterns. Figure 3A and 3B, below, illustrate just two patterns that the additional quarter-wave polarizer(s) may be configured.

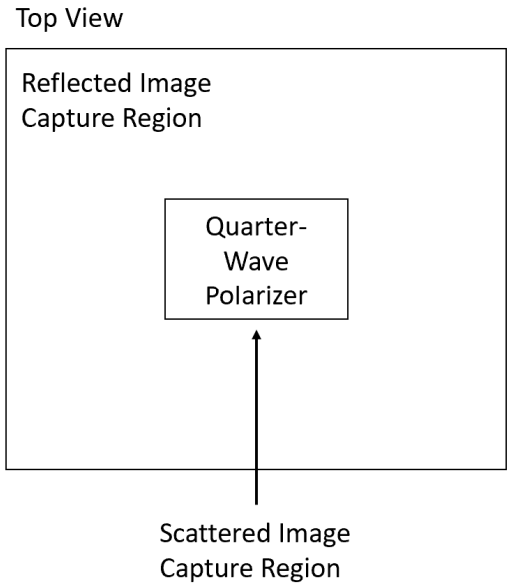

Figure 3A

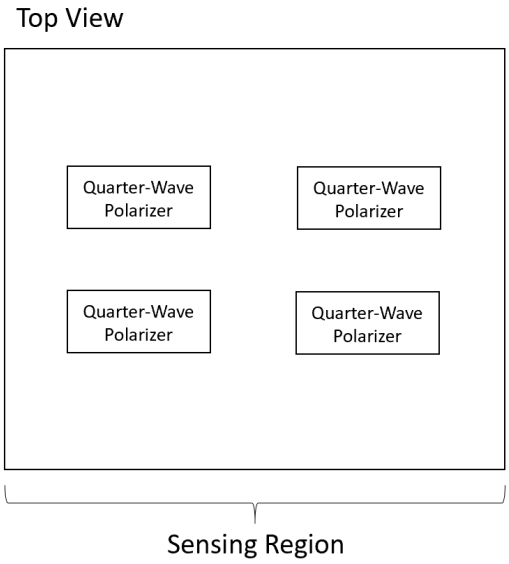

Figure 3B

As illustrated, Figure 3A depicts only one quarter-wave polarizer above an optical fingerprint sensor. Figure 3B, on the other hand, depicts four quarter-wave polarizers patterned in a two-by-two grid and all located in the same vertical layer above an optical fingerprint sensor.

In any configuration, no quarter-wave polarizer extends the full length of the sensing region. As a result, the optical fingerprint sensor detects reflected light where a quarter-wave polarizer is absent (reflected image capture region) and detects scattered light where a quarter-wave polarizer is present (scatter image capture region).

Figure 4 illustrates both an authentic fingerprint and a spoof fingerprint captured by an optical fingerprint sensor utilizing the configuration as depicted in Figure 3A.

Figure 4

In the examples illustrated in Figure 4, an optical fingerprint sensor captured two fingerprints with identical biometric identifiers. The optical fingerprint sensor utilized the same quarter-wave polarizer configuration as depicted in Figure 3A.

For both the authentic and the spoof fingerprint, the optical fingerprint sensor detected reflected light where the quarter-wave polarizer was absent, and as a result, reconstructed portions of the fingerprint using the reflected light (reflected image). In addition, the optical fingerprint sensor detected scattered light where the quarter-wave polarizer was present, and as a result, reconstructed portions of the fingerprint using the scattered light (scattered image). Using both images, the optical fingerprint sensor reconstructed a full fingerprint image for both the authentic and the spoof fingerprint.

As illustrated in the examples of Figure 4, both fingerprint images are identical insofar as the reflected image is concerned. The scattered image, however, is noticeably dissimilar between

the two fingerprints. For example, the scattered image for a spoof fingerprint may appear clear, focused, and/or vivid. In contrast, the scattered image for an authentic fingerprint may appear blurry, unfocused, and/or fuzzy. The differences in the scattered images are due to the inherent properties of a presented finger. For example, two-dimensional, printed spoof fingerprints exhibit uniform light scattering, while authentic fingerprints exhibit non-uniform light scattering. Since three-dimensional fingers with ridges and valleys generate authentic fingerprints, the scattered light appears non-uniform.

In addition to the above descriptions, portions of the collimator underneath a quarter-wave polarizer can be removed to permit greater scattered light detection. By so doing, characteristics of authentic and spoof fingerprints in the scattered image can be magnified further. Moreover, the reflected image capture region and the scattered image capture region can contain sensing circuitry of varying gains to amplify the scattered image. As a result, discrepancies between the scattered image of an authentic fingerprint and a spoof fingerprint can be magnified.

Finally, through the utilization of an on-device, machine-learned algorithm (anti-spoof detection algorithm), spoof fingerprints can be identified and rejected. In more detail, the anti-spoof detection algorithm may be a standard neural-network-based model with corresponding layers required for processing input features (*e.g.*, fixed-side vectors, text embeddings, variable-length sequences). The anti-spoof detection algorithm may be implemented as one or more of a support vector machine (SVM), a recurrent neural network (RNN), a convolutional neural network (CNN), a dense neural network (DNN), one or more heuristics, other machine-learning techniques, a combination thereof, and so forth.

The anti-spoof detection algorithm may be trained off-device using a triplet loss machine-learned approach. For example, the anti-spoof detection algorithm may be trained by comparing

anchor images (*e.g.*, scattered images extracted from enrolled fingerprint images) to positive images (*e.g.*, scattered images extracted from authentic fingerprint images) and negative images (*e.g.*, scattered images extracted from spoof fingerprint images). By minimizing the distance (*e.g.*, Euclidean distance) between the anchor images and the positive images, and simultaneously maximizing the distance between the anchor images and the negative images, the anti-spoof detection algorithm can learn to distinguish spoof fingerprints from authentic fingerprints. After sufficient training, the anti-spoof detection algorithm can be deployed to the computer-readable media of a computing device.

Operating on-device during fingerprint authentication, the anti-spoof detection algorithm can: 1) extract a feature vector for the scattered images of enrolled fingerprints and verify fingerprints (*e.g.*, fingerprints captured during authentication); and 2) compute a matching score between the enrolled and verify scattered images. Provided the matching score exceeds an established threshold certainty, the computing device can authenticate the user; otherwise, a spoof fingerprint can be identified and rejected.

Further to the above descriptions, color filters may be added above the optical fingerprint sensor such that the sensor can identify skin properties (*e.g.*, skin color). The anti-spoof detection algorithm can be additionally trained to compare skin properties of an enrolled finger image and a verify finger image. In so doing, an additional level of security can be implemented in fingerprint authentication services.

In summary, the addition of a quarter-wave polarizer above an optical fingerprint sensor, along with the utilization of an anti-spoof detection algorithm, can enable a computing device to distinguish a spoof fingerprint from an authentic fingerprint, and thereby increase the security and privacy of computing devices.

References:

[1] Patent Publication: US 20190034690 A1. Display for recognizing fingerprint and electronic device. Priority Date: July 31, 2017.

[2] Patent Publication: WO 2008111994 A1. Spectral biometrics sensor. Priority Date: July 19, 2006.

[3] Patent Publication: US 20150310251 A1. Display-integrated user-classification, security and fingerprint system. Priority Date: April 28, 2014.

[4] Patent Publication: EP 0359554 A2. Biological object detecting system and fingerprint collating system employing same. Priority Date: September 16, 1988.

[5] Patent Publication: US 20170017824 A1. Low profile illumination in an optical fingerprint sensor. Priority Date: February 2, 2015.