December 2019

Identifying fingerprint spoofs using skin properties

Jean-Marie Bussat

Firas Sammoura

Identifying fingerprint spoofs using skin properties

ABSTRACT

Optical fingerprint sensors enable seamless authentication and bezel-less displays by directly integrating a fingerprint sensor under the display screen of a device such as a smartphone. While conventional optical fingerprint sensors provide a convenient authentication technique, such sensors can be insecure due to the ease of generating and using spoofs that pass the authentication test. This disclosure describes techniques that utilize various skin properties to detect spoofs. Non-uniform illumination from the sensor interacts with the 3D structure of the finger and produces brightness variation that can be utilized to detect spoofs. Further, skin properties such as ridge-valley distance, skin deformation under pressure, and macro properties such as the shape of a finger can also be utilized to detect spoofs. Spoof detection can be performed to reject 2D or 3D spoofs prior to performing fingerprint matching.

KEYWORDS

- Fingerprint sensor
- Optical sensor
- Fingerprint spoof
- Spoof rejection
- Biometric authentication
- Device unlock
- Finger pressure
- Skin reflectance
- Skin deformation

BACKGROUND

Optical fingerprint sensors enable seamless authentication and bezel-less displays by directly integrating a fingerprint sensor under the display screen of a device such as a smartphone. The fingerprint sensor is essentially a 2D camera. While conventional optical fingerprint sensors provide a convenient authentication technique, such sensors can be insecure due to the ease of generating and using spoofs that pass the authentication test.

For example, many optical fingerprint sensors can be easily fooled (spoofed) by a simple paper copy of a fingerprint that can be made in cooperative (by somehow managing to take a picture of the user's finger and printing it) or non-cooperative (by lifting and then printing the victim's fingerprint from a surface they touched) fashion. For example, one available surface to lift fingerprints is the back of the phone if it lacks an oleophobic coating, since it is covered with latent fingerprints of the user. Such spoofs are easy to generate and do not require specialized skills.

Two categories of spoofs are common:

- 2D spoofs obtained by printing a picture of the fingerprint (in black and white, grayscale, or color) on a support material, such as paper (which can be white or colored).
- 3D spoofs obtained using a mold of the finger (cooperative spoofing) or generated by post-processing a 2D image to add depth and then printed on a 3D printer.

Authentication techniques that rely on optical fingerprint scanners need to be able to detect and reject both 2D and 3D spoofs.

DESCRIPTION

This disclosure describes multiple techniques to detect and reject spoofs. Various properties associated with physical fingers are utilized in these techniques. For example, the 3D

shape appearance of a finger under different lighting conditions can be utilized, e.g., by observing image parallax, appearance of the edges of a finger, etc. Another property is the deformation of skin that happens under pressure and leads to variation in the average ridge frequency. Yet another property is skin reflectance observed under different illumination colors (at different wavelengths). Still further, dynamic finger behavior, e.g., landing and/or lift-off fingerprint image, can also be utilized. All of these properties can be measured in a fingerprint image processing step to reject spoof images prior to sending the images to a fingerprint matcher that authenticates the user by matching the fingerprint with previously stored information. Some examples of such techniques are illustrated below.

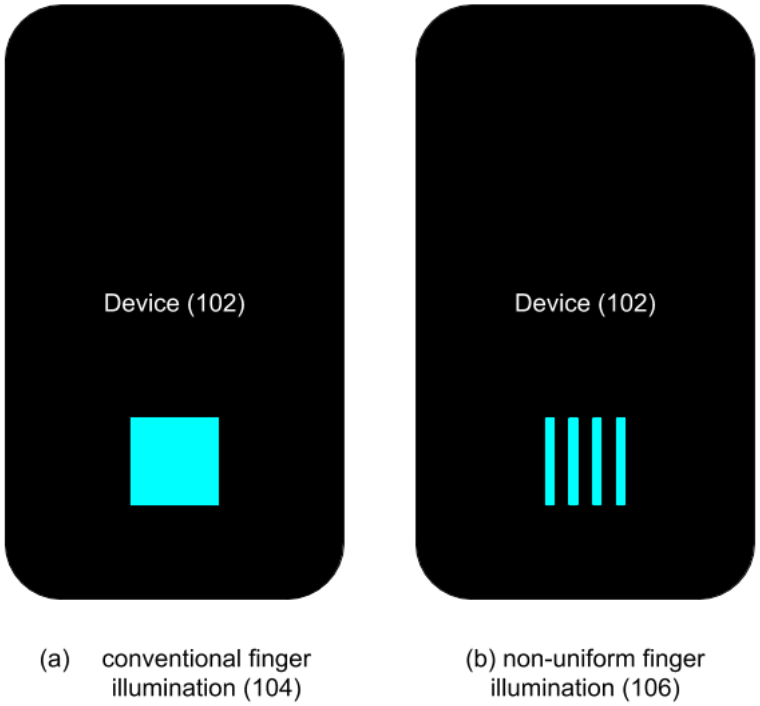

Fig. 1: Non-uniform illumination

Fig. 1 illustrates an example of a device (102) with a conventional optical fingerprint sensor. Current techniques, illustrated in Fig. 1(a) utilize a uniform illumination (104) that is uniform in color and intensity when acquiring a fingerprint image, which is susceptible to

spoofing. Per techniques described herein, illustrated in Fig. 1(b), a non-uniform illumination pattern can be used, e.g., alternating bright/dark lines in horizontal and/or vertical directions, a monochrome gradient, or a color pattern. Such pattern in the light distribution interacts with the 3D structure of the finger when obtaining the fingerprint. Signal processing techniques can then be applied to the resultant signal to detect a spoof, as illustrated in Fig. 2 below.

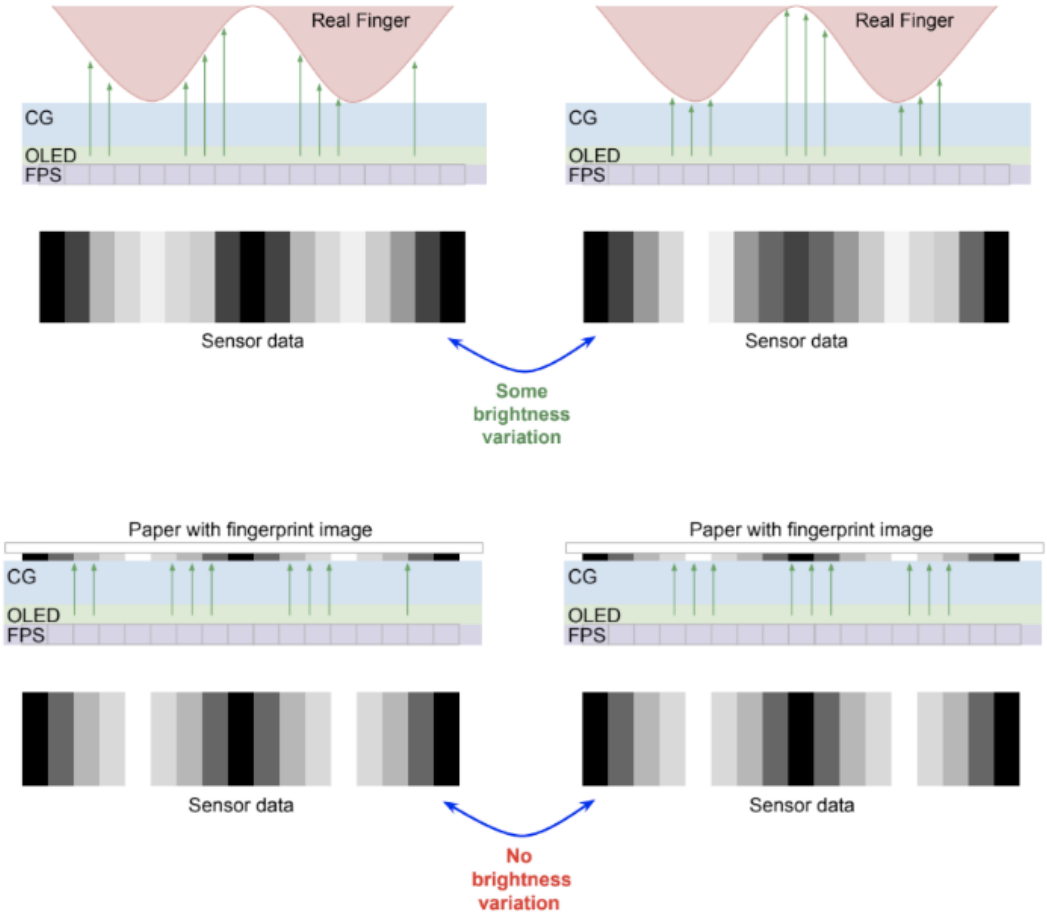

Fig. 2: Spoof detection via parallax/brightness variation

In the example illustrated in Fig. 2, a fingerprint sensor (FPS) is placed under an organic light-emitting diode (OLED) display (OLED) of a device which itself is housed under a cover glass. Signal processing techniques can be used to determine that a finger is real when brightness variation is observed under different lighting conditions, as seen in Fig. 2(A) and can determine

that a spoof (e.g., a paper with fingerprint image) is being presented when no brightness variation is seen under different illumination conditions.

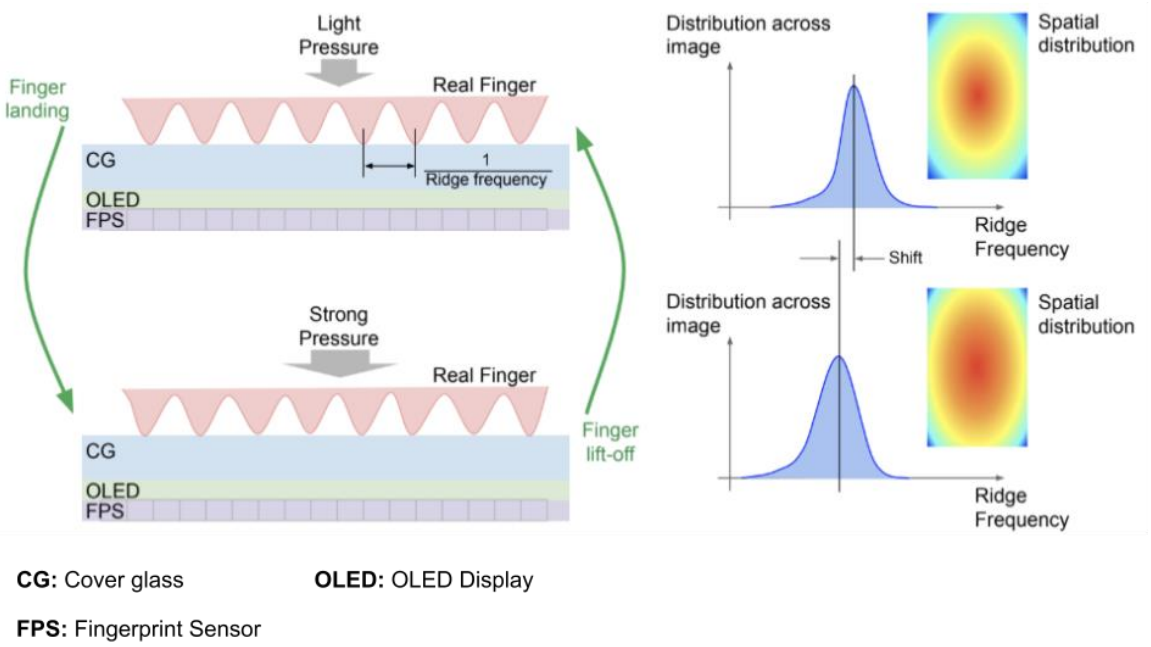

Fig. 3: Spoof detection via skin property monitoring

The plastic properties of skin, e.g., skin deformation under various conditions can be observed and used to detect spoofs. Human skin deforms when it comes in contact with the cover glass of the device. A spoof may not deform (e.g., when a fingerprint mold is constructed from a rigid material) or may deform differently (e.g., since the material properties differ from those of human skin) and reject access to the device.

The observation of deformations can be performed statically, e.g., when a finger is resting on the screen by analyzing a single image to determine fingerprint properties such as ridge-valley distance and the variation in these properties across the image. The differences in the distribution of such properties of a real finger and a spoof can be used to detect spoofs. The observation can also be performed dynamically, e.g., when the finger is landing or lifting off

from the sensor. In the dynamic analysis, fingerprint properties such as ridge-valley distance can be analyzed across a sequence of images, e.g., from landing to lift off. Fig. 3 illustrates an example of spoof detection via skin property monitoring.

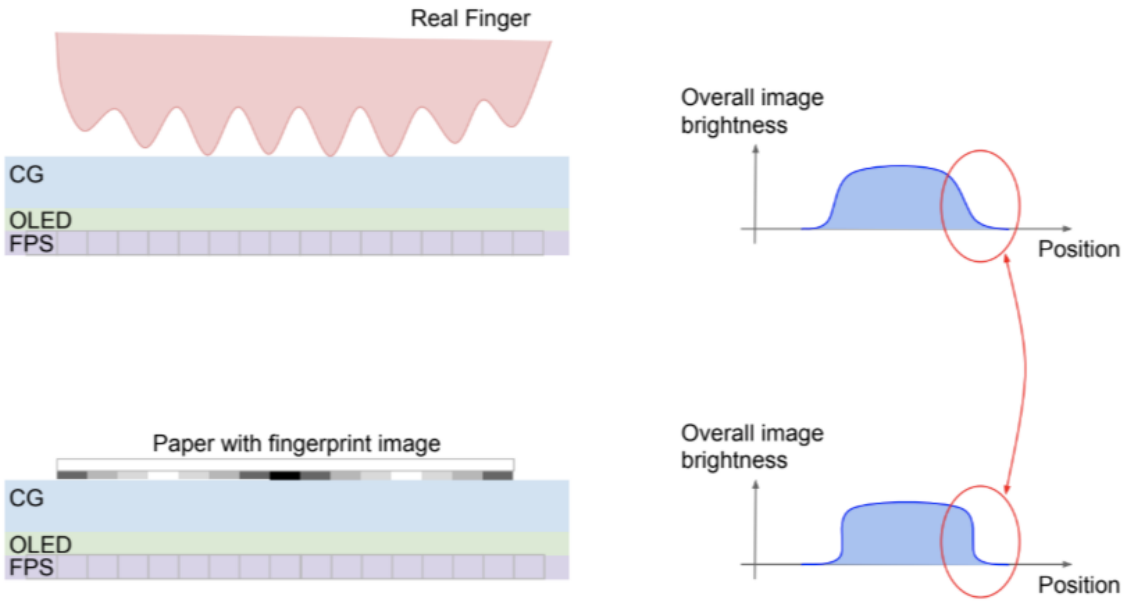

Fig. 4: Spoof detection via edge properties

Fig. 4 illustrates another technique where distinct macro three-dimensional features of a finger, such as shape, are used to detect spoofs, e.g., paper with an image of the fingerprint printed on it. The overall image brightness corresponding to different positions can be analyzed to detect differences in edge properties. For example, the change in brightness at the edge of a finger may be slower than that at the edge of a spoof, as seen in Fig. 4. Such a technique is suitable, e.g., when the sensor is large enough to capture the macro features.

CONCLUSION

This disclosure describes techniques that utilize various skin properties to detect spoofs. Non-uniform illumination from the sensor interacts with the 3D structure of the finger and produces brightness variation that can be utilized to detect spoofs. Further, skin properties such

as skin reflectance observed under different illumination colors, ridge-valley distance, skin deformation under pressure, and macro properties such as the shape of a finger can also be utilized to detect spoofs. Spoof detection can be performed to reject 2D or 3D spoofs prior to performing fingerprint matching.