November 2019

Spoof Detection for Fingerprint Sensors

Firas Sammoura

Jean-Marie Bussat

Spoof Detection for Fingerprint Sensors

Abstract:

This publication describes methods, techniques, and apparatuses that can achieve spoof detection in fingerprint sensors by confirming that a person is present and authorized to gain access to a mobile device, door entrance, vault, application software, physical locations, and/or or virtual activities that the person wants guarded. To do so, machine-learned models may be used to match at least one of a fingerprint residual on the glass covering the fingerprint sensor to a live fingerprint, a fingerprint coloration due to the hemodynamics of the pad of the finger, or a distortion pattern of the fingerprint due to the rotation of the finger.

Keywords:

Fingerprint sensor, spoof detection, fingerprint matching, fingerprint residual, liveness score, authorized access, fake fingerprint, biometric, replica fingerprint, hemodynamics, finger pressure, coloration pattern, minutia, minutiae, pattern correlation, finger rotation, fingerprint rotation, machine-learned model, ML, artificial intelligence, AI.

Background:

Since antiquity, various civilizations have used fingerprinting to identify individuals because human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual. These characteristics make fingerprints suitable as long-term markers of human identity. In modern times, virtually all countries use fingerprint recognition, in some form or another, to identify some of their citizens. Nevertheless, fingerprint recognition is more than a government or a legal tool for identifying alive or deceased individuals—many user equipment (UE) give a user a choice to use fingerprint identification to gain access to a mobile device, door entrance, vault, application software, physical locations, and/or virtual activities that the user wants guarded.

The UE can use a fingerprint sensor to capture a fingerprint image. Many fingerprint sensors, however, can be fooled, tricked, or spoofed. An unauthorized user can bypass some fingerprint sensors by obtaining a latent fingerprint, manipulating a copy of the latent print, and presenting the copy of to the fingerprint sensor, which can result in unauthorized access to the UE. The unauthorized user may "lift" or otherwise misappropriate a fingerprint in many different ways.

For example, consider the following scene at a bar, as is illustrated in Figure 1.

Figure 1

Figure 1 illustrates a man and a woman sitting at a bar enjoying a glass of wine. After some time, they leave the bar. Oil residue on their fingers leaves fingerprints on the wine glasses. Figure 2 illustrates a close-up view of a fingerprint on a wine glass.

Figure 2

As is illustrated in Figure 2, the man unintentionally leaves clear fingerprints as he lives his day-to-day life. Unbeknownst to him, a nefarious troublemaker can lift a fingerprint off the wine glass when the man and the woman have long left the bar. If the troublemaker cannot altogether take possession of the wine glass, they can use a smartphone equipped with a high-resolution camera to take an image of the fingerprint. Causally, the troublemaker can snap a photograph of the glass illustrated in Figure 2 while pretending to take a selfie or otherwise view content on the smartphone. The troublemaker, then, can process the image of the fingerprint using any number of commercially available or free photo-manipulation applications or software packages. Such photo-manipulation applications may perform sophisticated manipulation techniques to isolate, highlight, and enhance the image of the fingerprint. As a result, the troublemaker can generate a reliable, accurate, and functional copy of the person's fingerprint, which can be used to impersonate the person who left the fingerprint on the wine glass. Also, chances are that the troublemaker can take the wine glass and walk away. With enough time and easy-to-access materials, the troublemaker can use other techniques to create a fake or a replica of

the fingerprint. For example, the troublemaker can use black powder (*e.g.*, ninhydrin) to enhance the patterns and the minutiae of the fingerprint. Then, the troublemaker can create a two-dimensional (2D) image, a three-dimensional (3D) model, and/or a pseudo-3D (2.5D) model of the fingerprint using a variety of materials. The troublemaker can use these fake or replica images and models of the fingerprint to gain access to the person's mobile device, door entrance, vault, application software, physical locations, and/or virtual activities that the person guards using fingerprint authentication.

Therefore, it is desirable to have a technological solution that can detect whether the fingerprint used to gain access to a UE with a fingerprint sensor belongs to a present and authorized person.

Description:

This publication describes methods, techniques, and apparatuses used for spoof detection in fingerprint sensors by confirming that the person is present and authorized to gain access to a mobile device, door entrance, vault, application software, and other physical locations or virtual activities that the person wants to be guarded.

Residual Image Detection

In one aspect, the described methods, techniques, and apparatuses make use of the authorized person's skin oils. Recall the disturbing example illustrated in Figure 2—the reason the person left a fingerprint on the wine glass was that human fingers are covered in skin that contains oils and grease from sweat or greasy foods. The residue of the oils and grease from the finger can be imprinted on surfaces that the person touches, such as the wine glass. Similar to the wine glass, in a fingerprint sensor, glass or some other transparent and smooth composite material

is embedded above the fingerprint sensor. Nevertheless, what was a problem in Figure 2 can be used to combat fraudulent attempts to gain unauthorized access to the UE having a fingerprint sensor, as is illustrated in Figures 3A and 3B.

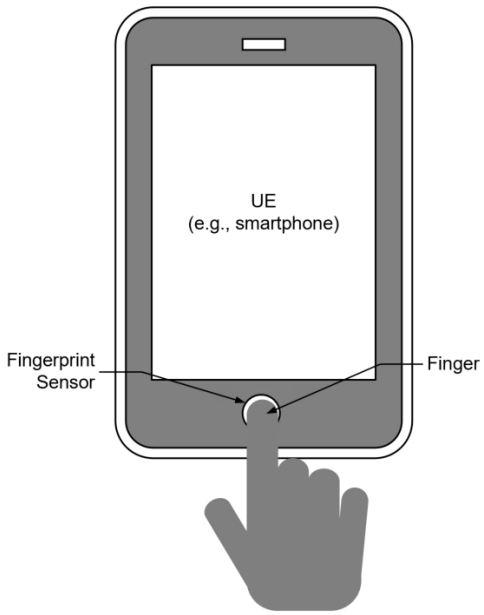

Figure 3A

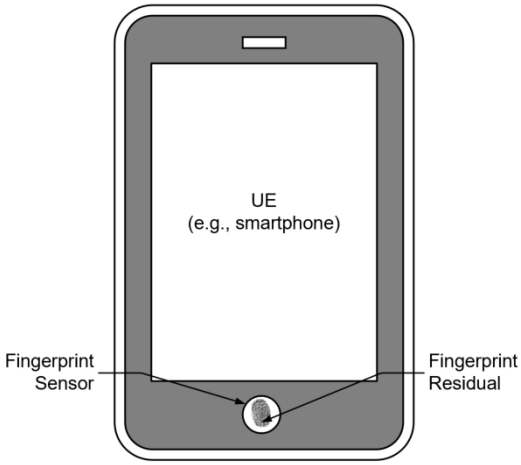

Figure 3B

Figure 3A illustrates a smartphone with a fingerprint sensor and a person placing their index finger on the fingerprint sensor to gain access to the smartphone's functionalities. When the person places the pad of their finger on the glass on top of the fingerprint sensor, the fingerprint sensor captures an image of the fingerprint (live fingerprint) and matches it to a previously saved template of the fingerprint. In Figure 3A, to match the live fingerprint to the template, the UE can utilize various fingerprint-matching algorithms, such as minutiae matching, pattern-correlation matching, or a fusion of minutiae and pattern-correlation matching. The smartphone determines whether the live fingerprint is a match to the template. If the matching is successful, the UE instructs the person to tap their finger on the fingerprint sensor. As the person lifts their finger from the fingerprint sensor, a fingerprint residual is left on the fingerprint sensor, as is illustrated in Figure 3B. The fingerprint sensor proceeds to capture an image of the fingerprint residual and

matches the fingerprint residual to the previously captured image of the live fingerprint. To match the image of the fingerprint residual (Figure 3B) to the image of the live fingerprint (Figure 3A), the smartphone may use the same fingerprint-matching algorithm (*e.g.*, a fusion of minutiae and pattern-correlation matching) or a different fingerprint-matching algorithm (*e.g.*, pattern-correlation matching). The smartphone may use a first matching score (*e.g.*, 99.5% certainty) between the live fingerprint and the template and a second matching score (*e.g.*, 95% certainty) between the fingerprint residual and the live fingerprint. It is acceptable for the second matching score to be a little lower because the fingerprint residual (Figure 3B) can have a lower image quality than the live fingerprint (Figure 3A). The described methods, techniques, and apparatuses require two back-to-back fingerprint matches:

- The live fingerprint (Figure 3A) needs to match the saved template (not illustrated); and
- The fingerprint residual (Figure 3B) needs to match the live fingerprint (Figure 3A).

For the troublemaker to gain access to the smartphone illustrated in Figure 3, they need to obtain a high quality 2D image of the fingerprint, create a high quality 2.5D or 3D model of the fingerprint, cover the 2.5D or 3D model of the fingerprint with oil(s), and attempt to gain access to the smartphone illustrated in Figure 3. Regardless of the quality of the fake or replica fingerprint 2.5D or 3D model, the model creates a different fingerprint residual than a live fingerprint.

To analyze whether the fingerprint residual belongs to the authorized person and that the person is present, the smartphone may use a machine-learned (ML) model. The ML model may be a standard neural network-based model with corresponding layers required for processing input features, such as fixed side vectors, image energies, variable-length sequences, and so forth. In addition, the ML model may be a support vector machine, a recurrent neural network (RNN), a

convolutional neural network (CNN), a dense neural network (DNN), heuristics, or a combination thereof. The ML model is trained to match a fingerprint residual to a live fingerprint instead of a 2.5D or 3D model of the fingerprint made using artificial material.

Also, the smartphone may also instruct the person to tap more than once on the fingerprint sensor when the person tries to access sensitive information, such as banking application software. Each time the person places their finger on the fingerprint sensor, the smartphone matches the latest live fingerprint to the template, and the latest fingerprint residual to the latest live fingerprint, further decreasing the chances for the troublemaker to spoof the fingerprint sensor.

Coloration Pattern due to Pressure

In one aspect, the described methods, techniques, and apparatuses make use of the person's blood flow and tissue under the pad of the finger. Studies on the effect of pressure on hemodynamics (the study of blood flow) on the pad of a finger can be utilized to determine whether the fingerprint is from a live and authorized person. The application of force produces blood perfusion coloration patterns in the fingerprint as the pad of the finger is pressed against the transparent surface (*e.g.*, glass) covering the fingerprint sensor—the fingerprint changes color when the person presses the pad of the finger against the glass. As the pressure on the pad of the finger increases, the fingerprint has a lighter reddish hue because blood flows away to a lower pressure point.

When the live and authorized person places their finger on the glass above the fingerprint sensor, the fingerprint sensor captures an image of the live fingerprint and compares it to the previously saved template of the fingerprint, as is illustrated in Figure 3A. The smartphone determines whether the live fingerprint is a match to the template. If matching is successful, the smartphone instructs the person to press their finger. The fingerprint sensor captures a second

image of the fingerprint when the smartphone senses a force above a specified threshold force. As the person gradually presses their finger exerting more force on the fingerprint sensor and more pressure on the pad of the fingerprint, the fingerprint sensor captures a third, a fourth, and so forth, fingerprint image at different forces. Qualitatively, as pressure on the pad of the finger increases, the fingerprint sensor senses a lighter reddish hue of the fingerprint. The change in color of the fingerprint is used to create a "liveness" score. The described methods, techniques, and apparatuses require multiple fingerprint matches:

- The live fingerprint (Figure 3A) needs to match the saved template (not illustrated); and
- The second, the third, and so forth, fingerprint images with different colorations need to correlate to the force sensed by the smartphone.

To analyze the correlation of fingerprint coloration to the force sensed by the smartphone, the smartphone may use an ML model, such as the ML model mentioned with respect to analyzing a live fingerprint above.

Distortion Pattern due to Rotation

In one aspect, the described methods, techniques, and apparatuses make use of distortion patterns of the fingerprint as the person presses their finger on the glass above the fingerprint sensor and rotates the finger (*e.g.*, clockwise, counterclockwise). Studies on the effect that finger rotations have on fingerprint distortion can be utilized to determine whether the fingerprint is from a live and authorized person.

When the live and authorized person places their finger on the glass above the fingerprint sensor, the fingerprint sensor captures an image of the live fingerprint and compares it to the previously saved template of the fingerprint, as is illustrated in Figure 3A. The smartphone

determines whether the live fingerprint is a match to the template. If matching is successful, the smartphone instructs the person to rotate their finger. The fingerprint sensor captures a second, a third, and so forth, image and compares the fingerprint images taken during finger rotations to the template. Each fingerprint image that is captured during the rotation of the finger may be differently distorted compared to the template, such as three pixels, seven pixels, ten pixels, and so forth, depending on the rotation angle of the finger. To calculate the relative rotation between the captured fingerprint images, the smartphone may utilize a fusion of minutiae and pattern-correlation matching algorithm. The fusion of minutiae and pattern-correlation matching algorithm calculates a delta (absolute percentage) of rotation and translation vector (delta vector) between each of the matched image blocks across all fingerprint images. The smartphone, then, compares the delta vectors to the rotational angles of the fingerprint images.

To analyze the distortion patterns of the fingerprint, the smartphone may use an ML model, such as the ML model mentioned with respect to analyzing a live fingerprint above.

Further to the above descriptions, a user may be provided with controls allowing the user to make an election as to both if and when systems, applications, and/or features described herein may enable collection of user information (*e.g.*, biometric information, social actions, social activities, a user's preferences, a user's current location), and if the user is sent content and/or communications from a server. In addition, certain data may be treated in one or more ways before it is stored and/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. In another example, 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 fingerprint scanner to unlock the device or gain access to application software. Instead, the user may choose another security feature, such as a username and a password to protect the device or the application software.

In conclusion, the described methods, techniques, and apparatuses can be used for spoof detection in fingerprint sensors by confirming that the person is present and authorized to gain access to a mobile device, door entrance, vault, application software, physical locations, and/or virtual activities that the person wants guarded. To do so, machine-learned models may be used to match a fingerprint residual on the glass covering the fingerprint sensor to a live fingerprint, a fingerprint coloration due to the hemodynamics of the pad of the finger, and/or a distortion pattern of the fingerprint due to the rotation of the finger.

References:

[1] Patent Publication: US20050238212A1. System for fingerprint image reconstruction based on motion estimate across a narrow fingerprint sensor. Priority Date: April 23, 2004.

[2] Patent Publication: WO2005109320A1. Fingerprint image reconstruction based on motion estimate across a narrow fingerprint sensor. Priority Date: April 23, 2004.

[3] Patent Publication: WO2005109321A1. System for fingerprint image reconstruction based on motion estimate across a narrow fingerprint sensor. Priority Date: April 23, 2004.

[4] Patent Publication: WO2017143571A1. Fingerprint identification method, device, and terminal. Priority Date: February 25, 2016.

[5] Thakkar, Danny. "Fingerprint Reader Technology Comparison: Optical Fingerprint Scanner; Capacitive-Based Fingerprint Reader and Multispectral Imaging Sensor." Bayometric, n.d. https://www.bayometric.com/fingerprint-reader-technology-comparison/.

[6] Yau, Wei-Yun, Hoang-Thanh Tran, Eam-Khwang Teoh, and Jian-Gang Wang. "Fake Finger Detection by Finger Color Change Analysis." International Conference on Biometrics. vol. 4642 (2007): 888–96. https://doi.org/10.1007/978-3-540-74549-5_93.