November 2022

Continuous Use of Biometric Sensor for Multiple Actions

Justin Eltoft

Albert Chen

Continuous Use of Biometric Sensor for Multiple Actions

ABSTRACT

This disclosure describes techniques to continuously sense the presence of an authenticated finger on a fingerprint sensor (or other biometric, such as a verified face in the field of view of a camera) of a device to enable multiple secure device actions. A user's finger and fingerprint are sensed by the device sensor and authentication is performed for the user. The user remains authenticated while the finger maintains contact on the sensor, allowing the user to perform different secure actions without having to re-authenticate for each secure action that is performed while contact between the authenticated finger and the sensor is maintained. This technique can save time, reduce computational load and software complexity, and reduce user toil and annoyance of repeated fingerprint authentication. The described features also provide additional security due to continuous engagement of the fingerprint sensor by the user.

KEYWORDS

- fingerprint sensor
- biometric sensor
- fingerprint recognition
- fingerprint scanner
- fingerprint match
- presence detection
- biometric sensor
- authentication
- secure application
- continuous mode

BACKGROUND

Fingerprint sensors are common on user devices such as smartphones, tablets, laptops, etc. Fingerprint sensors are used to authenticate a user to allow that user to access secure device functions, personal content on the device, secure applications or websites accessed by the device, etc. For example, fingerprint sensors are commonly provided on the front display or on the side or at the back of portable devices such as smartphones. Fingerprint sensors can use any of a variety of technologies such optical, capacitive, and/or ultrasonic, to sense a fingerprint of a finger held to the sensor. Similarly, with user permission, face-based authentication can be performed using one or more cameras of a device. The remainder of this document describes continuous authentication with respect to a fingerprint sensor, but the described techniques are also applicable to face-based or another biometric authentication.

A user can designate a device to require fingerprint sensor authentication to verify the user's identity when, for example, the user wants to unlock and access the device from a screen lock mode, e.g., after the display is turned on from an off state, or other mode. In addition, particular secure applications, websites, or device functions which the user desires to access may require user authentication, which can be performed via the fingerprint sensor. However, if a user desires to perform multiple secure actions for different functions and/or applications that each require authentication, the user must use the fingerprint sensor multiple times, each time receiving a prompt from the device and contacting the sensor with the finger, which is tedious and wastes the user's time. Keeping the user authentication valid even after the user has withdrawn their finger after authenticating (e.g., once at the start of using an application such as a banking app) also weakens security since a different person can grab the authenticated device to perform secure actions till the authentication expires, e.g., until the device screen times out.

DESCRIPTION

This disclosure describes techniques, implemented with user permission, for continuously sensing (detecting the continuous presence of) a user's authenticated finger on a fingerprint sensor (or other biometric, such as a verified face in the field of view of a camera) to enable the user to perform multiple different secure device actions. The described techniques determine whether a user has continuously touched a fingerprint sensor after being authenticated via that sensor, and if so, the user remains authenticated without having to re-authenticate for different device actions such as unlocking the device, actions within secure applications or websites, secure device functions, etc. These features allow a user to perform multiple device actions with a single authentication and without having to repetitively re-authenticate via the fingerprint sensor. The device does not have to display a prompt and authenticate for each different secure device action attempted by the user, speeding up the overall experience and providing additional security by having the sensor state persist while the authorized finger continuously touches the sensor.

The described techniques can be implemented on any suitable device, e.g., desktop or laptop computer, portable user device (e.g., a smartphone, tablet, etc.), security keys (e.g., USB security keys), server device, etc. The user is provided with options to enable or disable described techniques. The user can permit specific data or types of data (e.g., biometric fingerprint data) to be processed and can deny processing of other data or types of data.

Fingerprint detection for multiple secure device actions

According to described features, a user is authenticated, and the user's identity verified by using a fingerprint sensor of a device. In some examples, the user desires to perform a secure device action, such as to unlock the device from a locked state, to log in to a secure service

provided by an application executing on the device, to log in to a secure service provided by a website accessed via a browser application or other application running on the device, access secure and private data, etc. In further examples, secure applications and websites that require user authentication to perform financial and banking tasks (e.g., paying bills, transferring money to/from financial accounts), send messages by the device to private recipients, open sensitive information for display on the device, display passwords on the device, etc. can also utilize the described features.

User authentication can occur at any time when the user is operating the device. For example, the user can authenticate to unlock the device. In another example, the user can authenticate while operating the device and before performing tasks that require authentication. For example, the user can authenticate before launching an application, or accessing other websites or functions that require authentication. In another example, the user can authenticate during execution of an application or when accessing a website, e.g., in response to a prompt that is provided by the application or website.

To be authenticated, the user holds (or taps) a finger against the fingerprint sensor of the device and the sensor reads the finger's fingerprint. The device compares the sensed fingerprint (or a hash thereof) to known user biometric data (or a hash thereof, stored securely and locally on the user device, with appropriate user permissions). The user can set up the device to match fingerprints from any of their fingers for authentication. If the sensed fingerprint and stored data match, the user is authenticated, and continuous authentication mode is entered. This mode is active while the fingerprint sensor continuously detects the presence of the authenticating finger in its sensing area, e.g., contacting the fingerprint sensor. The user need not continually be re-

authenticated in this mode, since the authentication performed when initiating the mode is relied upon for later secure device actions.

While the device is in the continuous authenticated mode, authentication indicators can be output by the device to indicate that the mode is active. In some examples, visual indicators can be displayed on a display screen of the devices, such as an icon in a particular screen location, a border of a particular color displayed on the perimeter or sides of the screen, or other indicator. Some examples can provide an audio indicator of the mode, e.g., a particular sound that is periodically output by the device.

The continuous authenticated mode is exited when the user removes the finger from the fingerprint sensor. Any continuous-mode authentication indicators being output by the device are also removed, e.g., from the display screen. After finger removal, the device falls back to the normal authentication process outside of continuous authentication mode. For example, if no secure device action is being performed when the finger is removed, the user is no longer authenticated. If a secure device action requiring authentication is currently being performed when finger removal occurs, the user may still remain authenticated while that action continues (e.g., while the secure application or website continues to be accessed), as if the user were authenticated one-time when initiating that device action. When the current device action is completed (e.g., the secure application or website is exited or the user logs out), the user is no longer authenticated.

To enter continuous authenticated mode again, the user similarly touches the fingerprint sensor, and the device performs the authentication. The user alternatively has the option to be authenticated via standard authentication methods, e.g., a single authentication for a particular

device action (e.g., for using one secure application) in which the user need not continuously touch the fingerprint sensor.

Exit from the continuous authenticated mode can take place immediately upon any finger removal from the sensor; alternatively, the continuous authenticated mode can be kept active after a removal of the finger if the time period of removal is under a small threshold amount of time, e.g., a fraction of a second, before the finger is positioned again and sensed by the fingerprint sensor.

The fingerprint sensor can be in any location on the device, e.g., rear, side, front display, etc. Some locations may be more convenient for a user to hold a finger against a surface to allow continuous sensing by the sensor, such as the side of the device or the rear of the device. For example, an index finger or middle finger of the user's hand that holds the device can continuously touch the sensor, while the thumb of that hand, or fingers of the user's other hand, can be used to operate a touchscreen display of the device to perform device actions. Voice commands can also be input to the device while continuous authenticated mode is active.

Providing continuous finger sensing can provide additional security for use of secure applications. For example, the user must continually hold a finger on the fingerprint sensor area of the device to remain authenticated for different secure device actions, which prevents the authentication from remaining valid after the user has put down the device or otherwise released their grip on the device, thus enhancing security.

In some cases, the user can optionally be periodically re-authenticated using the fingerprint sensor during the continuous authentication mode. This can add additional security to device use, but in some situations may end up rejecting authentication, e.g., if the sensor incorrectly detects that the user is not the same person. For example, the device can

automatically re-authenticate the user based on the finger that has been continually touching the sensor, and the user need not be informed by the device unless the re-authentication has failed. Re-authentication can also occur in response to a device event, e.g., receiving a message from a different device, losing a network connection to another device, etc. In such cases, a prompt is provided for the user to remove and reapply the finger to the fingerprint sensor for the re-authentication.

Examples

Examples of the above techniques are presented below in Figures 1 and 2.

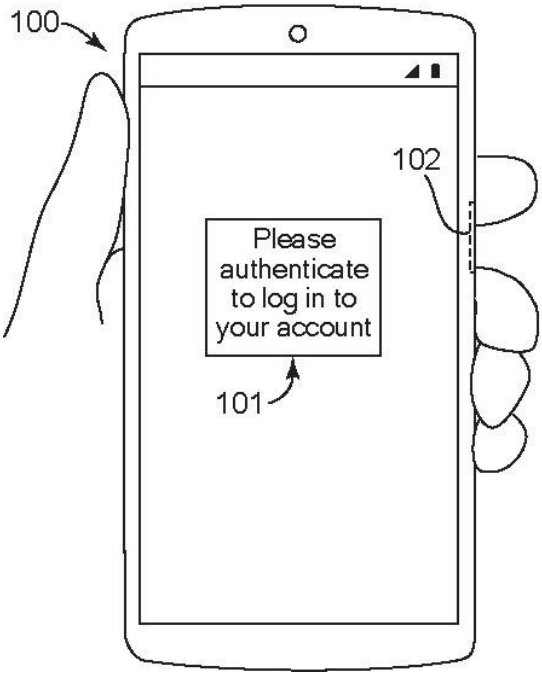

Fig. 1

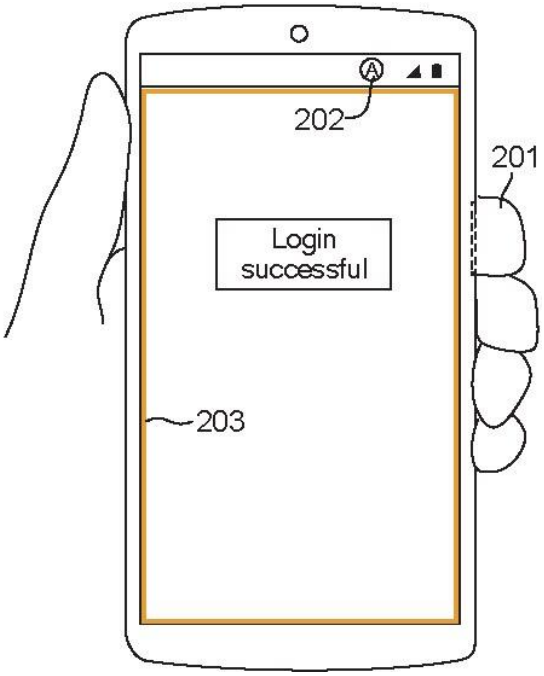

Fig. 2

Example of continuous authentication mode

Fig. 1 shows a device (100), e.g., a smartphone, on which a user has initiated a financial application. The application has requested via a prompt (101) that the user authenticate via the

fingerprint sensor. In this example, the fingerprint sensor (102) is located on the side of the phone 100.

Fig. 2 shows the device after the user has touched a finger (201) to the fingerprint sensor on the device for authentication. The device has sensed the user's fingerprint and determined it to be authentic based on a match with stored data. This causes the device to enter continuous authentication mode while the user maintains the finger on the fingerprint sensor. Some examples of visual indicators indicating that the continuous authentication mode is active include an icon (202) displayed in the status bar, and/or a border (203) that is displayed around the perimeter of the display screen. The indicator(s) remain displayed while continuous authentication mode is active and are removed from the screen when the mode is exited.

Users are provided with options to grant permissions to and/or to disable described features entirely. The various features of the system are implemented only with user permission to access user information that serves as input to the system (e.g., user fingerprints, user context information, user's preferences, etc.). Users 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, and if the user is sent content or communications from a server. Certain techniques are not implemented if users deny permission. 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. 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.

CONCLUSION

This disclosure describes techniques to continuously sense the presence of a finger on a fingerprint sensor of a device to enable multiple secure device actions. A user's finger and fingerprint are sensed by the device sensor and authentication is performed for the user. The user remains authenticated while the finger maintains contact on the sensor, allowing the user to perform different secure actions without having to re-authenticate for each secure action that is performed in a continuous time period, thus saving time, reducing computational load and software complexity, and reducing user toil and annoyance of repeated fingerprint authentication. The described features also provide additional security due to continuous engagement of the fingerprint sensor by the user.