April 11, 2018

Disabling facial unlocking using facial expression

Bernadette Alexia Carter

Disabling facial unlocking using facial expression

ABSTRACT

The techniques of this disclosure temporarily disable biometric recognition in a device to prevent unlocking of the device. The user registers one or more specific facial expressions as do-not-unlock expressions. If the facial recognition tool recognizes a registered do-not-unlock facial expression, then unlocking of the device is disabled until preconfigured conditions are met. The user can also register context, e.g., location, time, environmental parameters, etc., that makes the device ineligible for the biometric unlock.

KEYWORDS

- Face recognition
- Biometric locking
- Mobile security
- Face scan
- Biometric authentication

BACKGROUND

Face recognition is increasingly used as an authentication mechanism to grant users access to their mobile phone and other portable computing devices. Along with other biometric authentication schemes, face recognition has gained popularity due to its convenience and relatively good accuracy. Unfortunately, unlocking by face recognition opens up the possibility that a mobile device may forcibly be unlocked by an adversary holding the device owner under duress.

DESCRIPTION

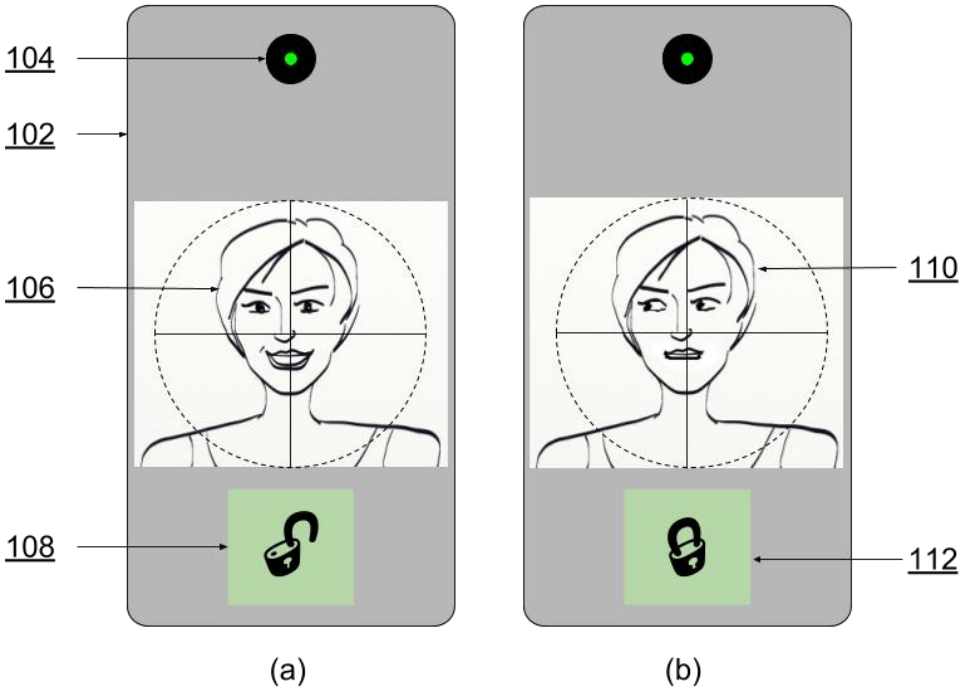

Fig. 1: Disabling facial unlocking using facial expressions

Fig. 1 illustrates disablement of unlocking of a smartphone based on capturing a user's face with a front-facing camera, per techniques of this disclosure. A smartphone (102) equipped with camera (104) obtains an image of the user. The image is compared with prior stored data about the user to determine whether to unlock the smartphone. The prior stored data is obtained with user permission, e.g., when the user signs up to use facial unlocking.

In the example illustrated in Fig. 1, facial expression (106) matches a previously stored expression that the user has registered as an unlock expression. Therefore, when the captured user image matches an unlock facial expression, as in Fig. 1(a), the phone (108) is unlocked. Facial expression (110) is an expression that the user has registered as a do-not-unlock expression. Therefore, when the captured image matches such a do-not-unlock expression, as in Fig. 1(b), the phone remains in the locked state (112).

In this manner, a user can control unlocking of their device based on facial expression. For example, a user that is under duress can prevent the phone from being unlocked by providing an expression that indicates do-not-unlock. Once a do-not-unlock facial expression is determined, unlocking is prohibited until certain preconfigured conditions are met, e.g., a set amount of time having passed since do-not-unlock activation, a certain location passed or reached, etc. The do-not-unlock techniques disclosed herein also apply to other biometric authentication technologies, e.g., fingerprint, speech, etc.

The user can also register context that makes a mobile device ineligible for biometric unlock. For example, a user can register specific locations to disable facial unlocking. Additional restrictions on device unlocking include times, certain events, device environment, e.g., device state mapped to accelerometer states, etc. When a user prevents unlocking, the mobile device remains locked for a period pre-set by user, or until a set of preconditions are met.

Further to the descriptions above, a user 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 (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. 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, or 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.

CONCLUSION

The techniques of this disclosure temporarily disable biometric recognition in a device to prevent unlocking of the device. The user registers one or more specific facial expressions as do-not-unlock expressions. If the facial recognition tool recognizes a registered do-not-unlock facial expression, then unlocking of the device is disabled until preconfigured conditions are met. The user can also register context, e.g., location, time, environmental parameters, etc., that makes the device ineligible for the biometric unlock.