November 14, 2017

Automatic information protection when device camera is operated by secondary user

Matthew Sharifi

Jakob Foerster

Automatic information protection when device camera is operated by secondary user

ABSTRACT

The techniques of this disclosure ensure user privacy when a user device with a camera is operated by a secondary user. Face detection and recognition are used, with user permission and consent, when a camera application of the device is in use. When it is detected that the device is being operated by a user other than the primary user, e.g., the device's owner, enhanced security and/or privacy features are automatically enabled on the device. Using the techniques disclosed herein, faces within the viewfinder of a camera application are detected. If a face is recognized as that of the device owner while operating a rear camera of the device is in use, enhanced security and/or privacy features are enabled. Such features include filtering incoming system notifications, suppressing or obscuring other device or application alerts, limiting device usage to only the mobile camera application, etc.

KEYWORDS

- Facial recognition
- Restricted access
- Primary user
- Alert suppression
- Rear camera
- Notifications
- Viewfinder

BACKGROUND

The camera application is one of the most heavily used applications on a mobile device. It is used both by a primary user of the device, e.g., the device owner, and others that operate the device to take a photo. For example, while traveling, a primary user might ask a friend or another person nearby ("secondary user") to take a picture using the primary user's mobile device. In such an example scenario, the friend limits their use of the primary user's mobile device to the camera application.

However, notwithstanding limited use, it is still possible for the secondary user to see potentially private information intended for the primary user, e.g. in a system notification that appears while the secondary user is operating the device to take a photo. Such notifications may reveal private information of the device owner, such as content, images, or other information from email, instant messages, SMS communications, etc. It is difficult to hide these notifications from the secondary user, because prior to handing over the mobile device to a secondary user, the owner typically unlocks the mobile device. Therefore, the operating system of the mobile device does not receive any indication that a secondary user is operating the device.

DESCRIPTION

The techniques of this disclosure detect when a mobile device is operated by a user other than the primary user of the mobile device, e.g., when the primary user hands the device to that user to use the camera application. Based on such detection, enhanced security features are enabled to prevent display of private information on the mobile device while it is being operated by the secondary user. Examples of mobile devices include smartphones, tablets, wearables, head mounted displays, etc.

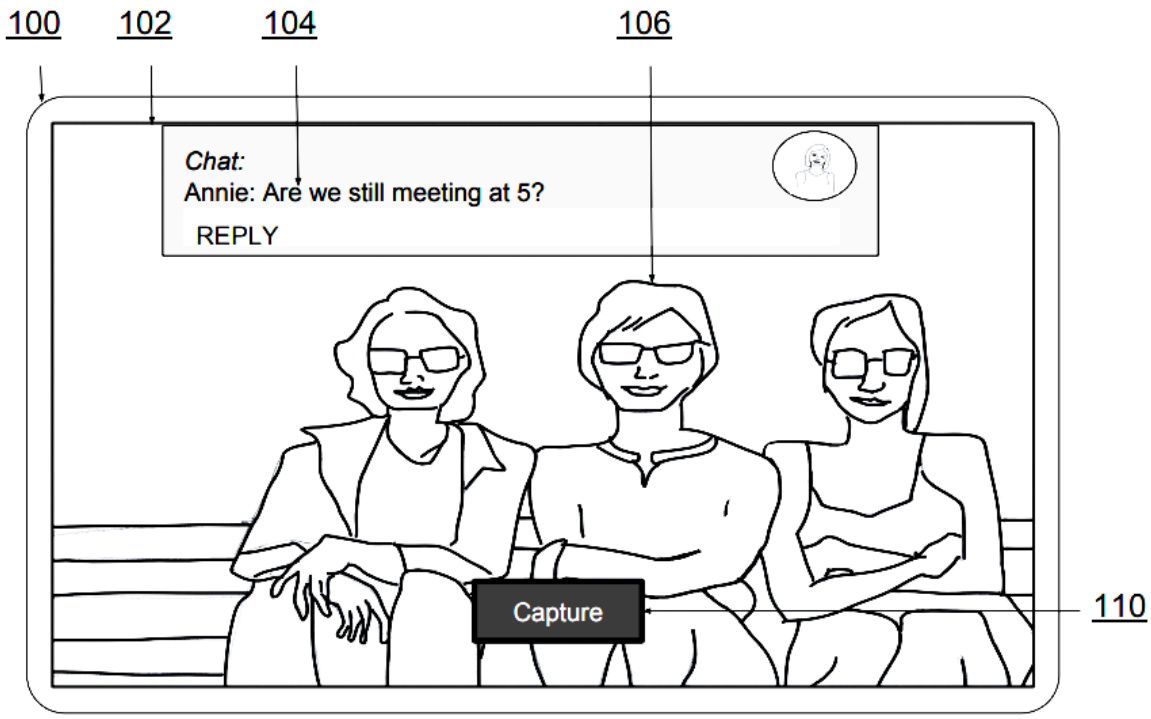

Fig. 1A <u>Problem:</u> Notifications not suppressed when device is operated by a secondary user

Fig, 1A illustrates a problem scenario where notifications are not suppressed when the camera application is operated by a secondary user. In the example, a secondary user is operating the camera application (102) on a mobile device, e.g., smartphone (100) using the rear facing camera. The camera application includes a “Capture” option (110) to capture the picture shown in the viewfinder. While the secondary user is using the camera application to take a picture that includes the device owner (106), a notification of a chat message (104) pops up that includes the name and picture of the chat friend as well as the content of the chat message. This private information intended for the primary user is visible to the secondary user who is temporarily using the device.

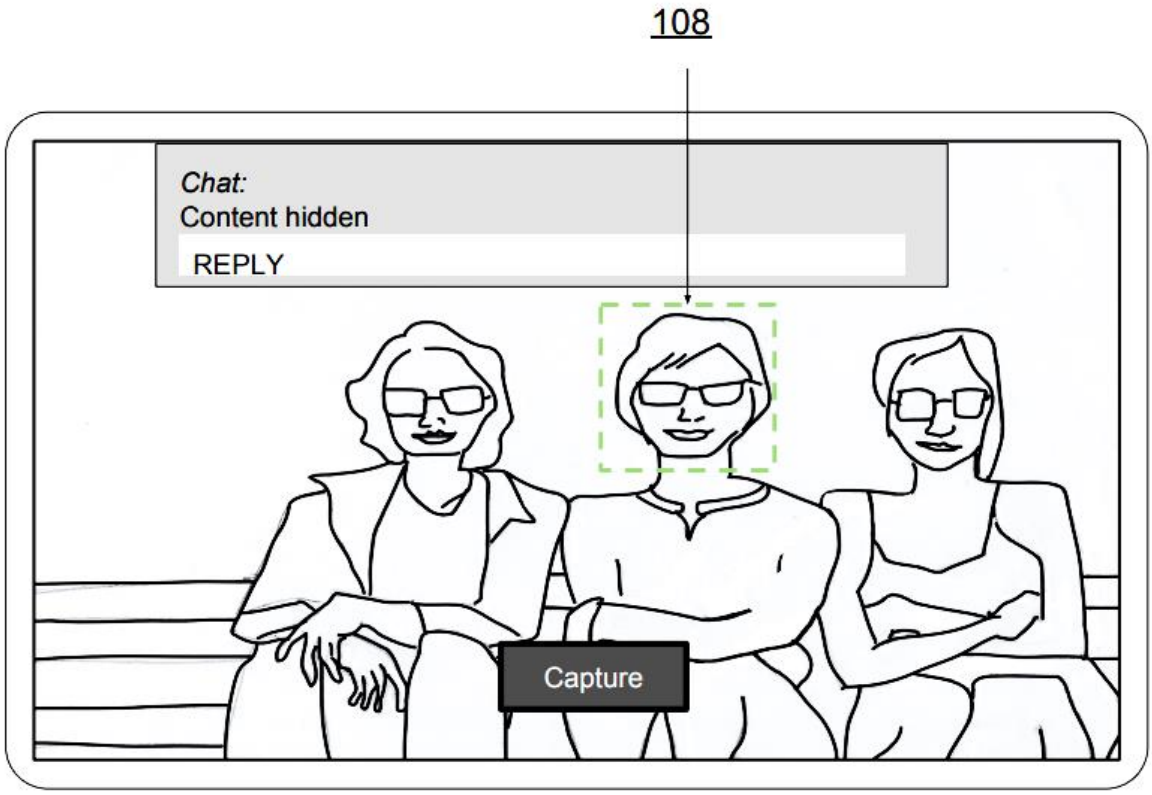

Fig. 1B <u>This disclosure:</u> Notifications suppressed when device is operated by a secondary user

Fig, 1B illustrates how the techniques described herein automatically enable enhanced security and privacy features by suppressing or hiding notifications when a secondary user is using the camera application on the device. To determine when to hide notifications, facial recognition and detection are applied as the secondary user operates the device, with express user permission and consent, to detect faces. As illustrated in Fig. 1B, if a face (108) is recognized as that of the device owner, it is determined that the device is being used by a secondary user for taking a picture. Based on this determination, enhanced security and/or privacy features are enabled including, e.g., filtering any incoming system notifications, obscuring device alerts,

hiding content in application notifications, limiting device usage to only the mobile camera app, etc.

To recognize the owner's face, the techniques of this disclosure, may perform facial recognition and detection on the device, e.g., the smartphone, with express user consent. In one scenario, facial detection and recognition are performed using a set of reference images that are matched against the faces detected in the camera viewfinder and frames captured by the device. Facial detection and recognition may be performed on sample frames or on all frames. Standard techniques of machine learning and deep neural and convolutional neural networks are implemented on the device for the purposes of facial detection and recognition.

The reference images used for matching are obtained and used with express user consent of the device owner, e.g., from 'selfie' images that are captured using a front-facing camera of the device. Developing and training using reference images may also be used in other device security or privacy features, e.g., to unlock a mobile device when the device owner's face is detected by the front facing camera. The face detection and recognition aspects of the techniques in this disclosure are performed on-device in real-time. Tracking of a given face of a particular user can be applied to avoid recomputing all features for a full frame each time.

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

Portable electronic devices, e.g., smartphone, tablets, wearables, head mounted displays, etc., display system notifications, application alerts, incoming messages or portion of a message even when the device is currently running an application, e.g., a camera application in full screen mode. In some situations, e.g., the device is temporarily being used by a secondary user, e.g., friend, passer-by, etc. to take a photo using the camera application of the device, displaying these notifications is undesirable since such notifications are intended for the primary user. As the secondary user takes a photograph using the camera application, upon user permission, the techniques of this disclosure recognize the owner's face as present within a viewfinder of the camera. Enhanced security and/or privacy features such as hiding notifications are automatically enabled in response to such recognition.