June 2022

# Automatically Setting Photo Visibility Based on Identifying Users Jointly Viewing Photos

D Shin

# Automatically Setting Photo Visibility Based on Identifying Users Jointly Viewing Photos

## ABSTRACT

When physically together, users can view photos jointly on a device such as a smartphone, tablet, smart TV, etc. During such a session, inadvertent disclosure of photos not shared jointly with all viewers can happen. This disclosure describes techniques to automatically set photo visibility on a device being viewed by multiple users. With user permission, the front-facing camera of the device is used to capture an image of all viewers. The viewers are mapped to user identifiers and access control techniques are implemented to select photos that are viewable by all viewers. All other photos are set to protected mode and can only be viewed with specific action by the device owner. The techniques improve the user experience of joint photo viewing while preventing inadvertent exposure of private photos.

## KEYWORDS

- Joint photo viewing
- Photo album
- Shared photos
- Photo visibility
- Access control
- Face recognition
- Face matching

## BACKGROUND

Users often view their photos in the company of others such as friends, family, etc. Such joint photo viewing on a smartphone, tablet, or other device is an important social activity during which people flip through the photos on their devices while exchanging related stories and reliving corresponding memories. When using a device to view photos with others, a user needs to be careful to avoid inadvertently showing photos that the user does not wish to share with the other parties.

Current photo sharing mechanisms involve transfer of photo files between devices and/or updating access settings for photos stored at a server. Photos shared via such mechanisms can then be viewed by each authorized viewer. However, such a viewing experience is based on the photos being accessed separately via individual devices owned by each of the viewers. The inherent social and community dynamics involved in the user experience of jointly viewing photos on a single device are lost when the joint viewing takes place via multiple distinct devices.

## DESCRIPTION

This disclosure describes techniques to support joint viewing of photos by multiple users via a single device owned by one of the users while ensuring that photos not shared among the users are protected. In such situations, the visibility of photos viewable via the device is set based on the photos shared among the users who are detected to be present within the field of view of the device camera. The operation can create the digital equivalent of the social experience of flipping through a physical photo album jointly with other people while avoiding the risk of accidental disclosure of private photos.

With user permission, individuals that are viewing the device are detected via the user-facing camera of the device by recognizing familiar faces based on pre-calibration. Only those photos or albums that are shared among those who are detected to be in the field of view of the device camera are made visible for joint viewing. Optionally, the device owner can take explicit action to be able to open other photos and albums that are not visible for joint viewing.

The identification of users, performed with user permission, is based on one-time calibration that can be performed via one of more suitable mechanisms such as a survey that prompts users to match faces with specific individuals using existing photos. At runtime, when viewing photos, the user-facing device camera captures a photo of the user and proximal surroundings. A suitably trained model can be employed to detect the faces in the captured photo and check for matches with those in the library of pre-calibrated faces compiled as described above. Only those photos and albums that are viewable by all of those detected to be viewing jointly are made visible within the user interface to fit the joint viewing context and to avoid inadvertent disclosure of photos not shared among the viewing users.

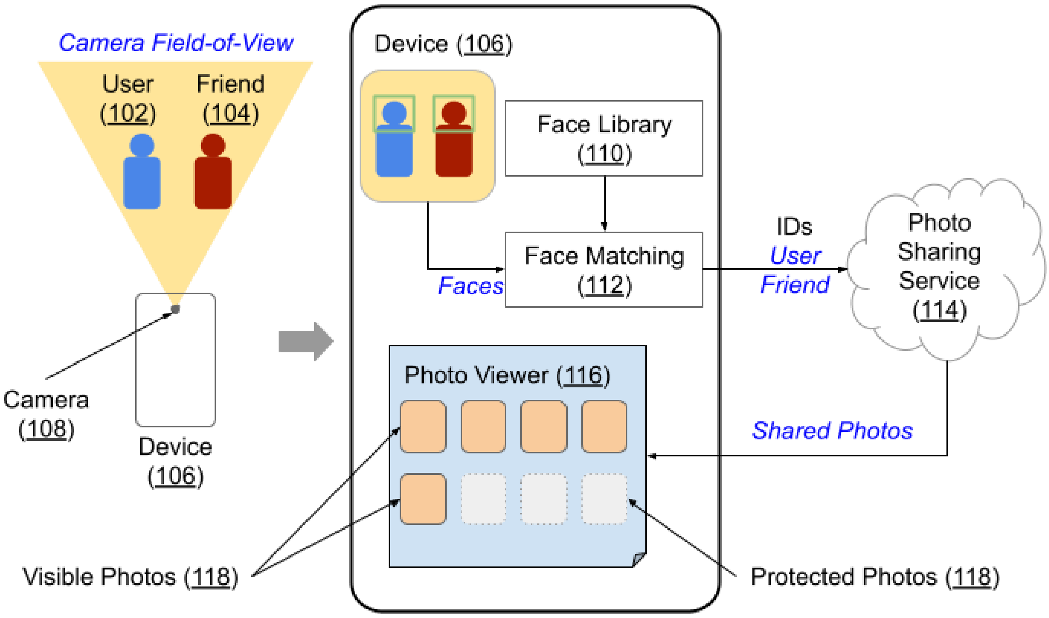

**Fig. 1: Automatically setting photo visibility for joint photo viewing by multiple users**

Fig. 1 shows an example of operational implementation of the techniques described in this disclosure. A user (102) and a friend (104) initiate a session to view photos on the user's device (106) while physically together. The user-facing camera (108) on the device is used to capture an image of the device context visible within the field of view of the camera. Faces of the two individuals (i.e., the user and the friend) detected within the captured image are matched (112) against an existing library of known faces (110). With user permission, the matched faces are mapped to user IDs for a photo sharing service (114) to determine the photos that they are both permitted to view. These commonly shared photos are then made visible (118) for joint viewing via the photo viewer (116) on the user's device. The rest of the photos that are viewable by the user but not the friend are marked as protected (118) such that they can be viewed only upon explicit action by the user.

With user permission, the operation described above can support joint viewing by any number of users as long as the users are present within the field of view of the device camera and their faces can be mapped to user identifiers that define access control for the photos being viewed. Photos shared among the set of users detected to be jointly viewing photos can be identified using any appropriate technique that can search photo collections and can be sorted and rendered within the photo viewer based on the photo content, album identifiers, date, or other criteria. Gaze estimation for the detected faces can additionally be incorporated to determine which of the users are attentively viewing the device display and to adjust photo visibility accordingly to display the photos that are shared among attentive viewers.

The techniques described in this disclosure can be incorporated to enable selective photo viewing from any device that has a front-facing camera (or other mechanism for detecting viewers). A manual mode can also be provided where the user identifies the users that are viewing the photos together. The techniques can support any application or service with photo viewing and sharing capabilities. The application or service as well as the photos being viewed can be local to the device and/or provided remotely via the cloud.

The capture of the device context for detecting users who wish to view photos jointly can occur when the photo viewer is invoked. With permission, periodic snapshots can optionally be taken during the viewing session to adapt dynamically to changes in viewership. The interval for taking such periodic snapshots can be set by the developers and/or determined dynamically at runtime. Implementation of the techniques described in this disclosure can enhance the user experience of joint photo viewing on a single user device while preventing inadvertent exposure of private photos.

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 photos, a user's context including other users nearby, social network, social actions or activities, 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

This disclosure describes techniques to automatically set photo visibility on a device being viewed by multiple users. With user permission, the front-facing camera of the device is used to capture an image of all viewers. The viewers are mapped to user identifiers and access control techniques are implemented to select photos that are viewable by all viewers. All other photos are set to protected mode and can only be viewed with specific action by the device owner. The techniques improve the user experience of joint photo viewing while preventing inadvertent exposure of private photos.