Photo-TaPE: User Privacy Preferences in Photo Tagging

Vincent Toubiana Vincent Verdot

Benoit Christophe Matthieu Boussard

Alcatel-Lucent Bell Labs France
Route de Villejust, 91620 Nozay, France
[firstname.lastname]@alcatel-lucent.com

ABSTRACT

Although they are used to expose pictures on the Web, users may not want to have a link between their identity and pictures without being able to modify them or control who accesses them. Photo tagging — and more broadly face-recognition algorithms — often escapes to the users' control and creates links between private situations and their public profile. To address this issue, we designed a geo-location aided system to let users declare their tagging preferences directly when the picture is taken. We present Photo-Tagging Preference Enforcement (Photo-TaPE) a system enforcing users tagging preferences without revealing their identity. By improving face-recognition efficiency, Photo-TaPE can guarantee the user tagging preferences in 67% of the cases and significantly reduces the processing time of face-recognition algorithms.

Categories and Subject Descriptors

K.4 [**Computers and Society**]: Privacy

Keywords

Privacy, Photo tagging, Face Recognition

1. INTRODUCTION

Over the last few years, the amount of pictures and videos recorded has seen an exponential growth. As example, Facebook holds the larger photo collection over the Web with more than 100 billions pictures, at a rate of 250 million new uploads per day [2]. Many photo-sharing services are now provided to organize and share pictures on the Web. In order to simplify the management and classification of images, many services provide a tagging function that allows users to indicate who is portrayed on the pictures and so easing management and further sharing. This manual operation is usually also assisted by face-recognition mechanisms to automate the face tagging process. While this feature appeared as very useful to share a picture with the pictured persons, it also raises serious privacy concerns: since users can be tagged anytime anywhere on photos they are not necessarily aware of, their identity might be associated to pictures they do not want to share. Service providers attempted to address these concerns but raised more privacy issues than they solved [3] as — in some cases — users may not remove tags linking to their profiles. To address the privacy concerns that photo-tagging raises with a minimal impact on existing picture-based services, we suggest to enforce pictured users' tagging preferences and introduce a tagging profile allowing them to declare this preference. A simple solution to enable such a system would be to use face-recognition algorithms — based on a centralized database of faces — to retrieve a user tagging profile and then apply his preference but it would actually damage users' privacy. First, tagging profile should be retrieved with a degree of confidence that can not be guaranteed by current face-recognition algorithms. Second, such system could be misused to identify persons with a single picture [1].

In this paper we present Photo-Tagging Preference Enforcement (Photo-TaPE) that is designed to be run on users' cameras and leverage localization information to automatically apply the tagging preferences of people pictured in photos.

WWW 2012 Companion, April 16–20, 2012, Lyon, France.
ACM 978-1-4503-1230-1/12/04.

2. USER TAGGING PREFERENCE

In the current picture publication process, the control is often not shared with the pictured persons but is only owned by the photographer: people have no control on how photos they appear on will be posted and shared. We foresee a need for a solution that would offer to the pictured person some control over his image without damaging every picture they may appear on.

We introduce the concept of *"Tagging Profile"* that will convey the tagging preferences that users want to see associated to their (pictured) faces. Each *TP* is composed of a *"Tagging Preference"* description reflecting the user preference (either "tag", "send by e-mail" or "obfuscate") and a *"Profile Picture"* used to associate a face to its owner profile via face-recognition. To improve the effectiveness of face-recognition algorithms, we use location information to reduce the set of face candidates.

Leveraging location sharing services. Photo-TaPE aims to provide to photographers *an effective and accurate solution to retrieve pictured users' tagging profile in order to respect their privacy preferences.* In order to maximize accuracy, we leverage localization information to only consider the *TP* of people who actually are in the pictured area. Each user should carries a pointer to his *TP*, this pointer can be carried physically (*e.g.* through a QR-Code) or virtually (hosted on his smartphone or his Location Sharing service

profile). In this paper we adopt a Web-based approach and assume that the *TP* is hosted by a location sharing service. This system has several limitations regarding user location privacy. We assume that users trust a location service to inform Photo-TaPE of their presence and agree to disclose their location to other users in the same area. Notice that this does not disclose user location to users that are not in proximity and therefore does not entail our objective to protect users privacy with regards to their social networks.

Through its *TP*, each pictured person now controls how his face can be annotated when published or shared. By leveraging external sources of information, our solution improves the overall accuracy of face-recognition algorithms.

Step by step description. When a user takes a picture, the following process is followed by Photo-TaPE:

Tagging Preference and Face fetching. When a picture is taken, the camera gets the *TP* of every person present in the area and fetches their profile pictures and preferences. These faces will be added to the local Gallery of faces that can be recognized by Photo-TaPE.

Retrieving the preferences to apply. To process a new picture, Photo-TaPE first extracts every face on the picture (Figure 1- steps 2,3). The key step is to recognize each of these faces by finding a closest match in the local Gallery (Figure 1- step 4). If a face is recognized, Photo-TaPE retrieves the tagging preference of the pictured person (Figure 1- step 5).

Applying users tagging preferences. Then, for each matched face, Photo-TaPE applies a filter matching its owner's preference ("blur", "tag", "send by e-mail") as presented in Figure 1-6,7. Finally, the picture that Photo-TaPE delivers to the end users is a photo respecting the preferences of every pictured person.

Implementation. We prototyped Photo-TaPE as an Android application that makes extensive use of the FaceDetect Android APIs to detect and extract faces appearing on a picture. We also use the FOURSQUARE location sharing service to get the list of people who are in the same area than the photographer. The profile a user sets on its FOURSQUARE account serves as *TP*. Indeed, this profile contains a picture from which a face pattern can be derived, and several fields that the user could use to indicate his tagging preferences. To improve the accuracy of the trained algorithm, we also collect other available pictures on linked accounts (*e.g.* Facebook and Twitter). As the face recognition process is resource consuming, we offload it to the Web service Face.com.

Table 1: Face recognition results

Photo-TaPE		Large Database	
Succ: 67%	Time(Avg) 4.56s	Succ: 9%	Time(Avg) 12.1s

3. EVALUATION

We carried out an experiment to evaluate the validity of our solution and to see whether or not it would correctly convey the preferences of photographed persons. We asked users to check-in at a specific venue to express the fact that they wanted to be tagged and then pictured them to verify that their faces would not be blurred by our application. To compare our approach to a baseline, we used two face databases.

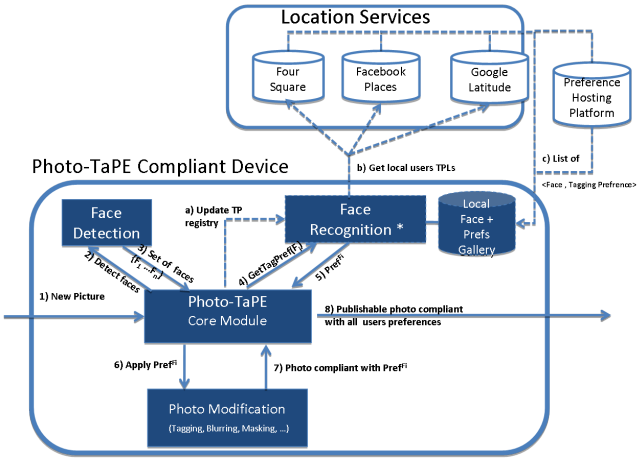

Figure 1: Typical process of Photo-TaPE prototype

The first database was solely composed of faces of person who recently checked-in at the venue. For each person, we fetched between one and three pictures. The second database contained in addition pictures of 700 other faces that were stored in public FACE.COM databases.

For each person who checked-in, we took a picture and tried to recognize him at first using only the local Gallery and then with the full database and we observed the number of misclassifications (people who were not correctly recognized).

From the 12 experiments we realized, the full database configuration was able to retrieve the find the right user only once. Our algorithm performs better with a success ratio of 8 users recognized out of 12 tested. On the four unrecognized users, only one caused an erroneous username to be returned thus emphasizing the benefits of using a shorten collection that leads to significantly fewer errors.

4. CONCLUSION

In this paper we present a novel scheme to enforce the privacy of pictured users and provide them with a tool to control their image on the Web. We argue that such scheme can not be supported by a sole centralized system and that auxiliary location information would help to improve the accuracy and efficiency of face recognition, both properties being critical to support user tagging preferences retrieval.

5. REFERENCES

[1] R. G. Alessandro Acquisti and F. Stutzman. Faces of facebook: Privacy in the age of augmented reality. In *BlackHat*, 2011.

[2] P. Blog. Facebook photo trends, February 2011. http://blog.pixable.com//2011/02/14/facebook-photo-trends-infographic.

[3] D. Tynan. Facebook's new privacy controls: Still broken. `http://www.itworld.com/it-managementstrategy/198069/facebooks-new-privacy-controls-still-broken`.