Blur Me: Automatic Tagging Framework for Securing Photo Sharing in social Media

HIBA K

Department of Computer Science and Engineering, APJ Abdul Kalam Technological University, kerala, India

---***---

Abstract - *Photo sharing on social media has become one of the most popular social activity in our daily life. Unfortunately, it may become very dangerous when the uploader posts photo online without the permission from other participants within the same photo. As a solution, propose a fine grained access control on social media photos. Every participant will be tagged by the uploader and notified through the internal message to initialise their own access control strategies. The looks of participants will be blurred if they need to preserve their own privacy during a photo. However, these methods highly depend on uploaders reputation of tagging behavior. Mallicious users can easily manipulate unpermitted tagging and photo publishing. To solve this problem, propose developing a participant free tagging system for social media photos. In evaluation carried out a series of experiments to validate system efficiency and effectiveness in protecting user's privacy.*

***Key Words*: Social media, Face tagging, uploader, privacy, security.**

1. INTRODUCTION

With the development of social media users can take photos anytime and anywhere, and share them in social community easily. As more and more people enjoy the benefit of photo sharing, privacy has become a major concern. Most existing photo sharing sites allow registered users to access others photo with limited constraint or no constraints. Your face is in a photo taken by someone else, you cannot control how the photo is shared, and this is most likely decided by the uploader in most social platforms such as Facebook [1]. Such model may raise serious privacy concerns through leakage, in which privacy information of a specific user is revealed by his/ her friends. Therefore, there is a need to preserve user privacy in photo sharing. To preserve privacy in photo sharing, most existing works [2], [3], [4] focused on designing access control based approaches, and little work considers the specific sharing scenario. These existing works [5], [6] requires users to set privacy policy for each photo and hence is not scalable.

When considering the privacy of other participants in photos, people care less about it and current photo sharing mechanisms may cause to critical problems with the very fact that 34% of Facebook users claim they do not always reflect on their photos' content before uploading them [7]. A recent government driven study reported that with 1 in 5 Australians suffered from 'revenge porn', a form of image-based abuse [8]. Those images were mainly distributed across multiple social media platforms like Twitter, Facebook etc. Another example is that inappropriate photos on social networking sites may also result in unemployment situation [9] and those photos may not even be uploaded by those participants. According to the survey carried by Pew Research Centre [10], one of the major arguments from Facebook protesters is that people can post someone's personal information without asking permission. Another survey [11], also claims that averagely 76% users will untag themselves from the photos that are uploaded by their friends or remove those photos from their Facebook timeline in order to preserve their own privacy.

To preserve privacy in photo sharing, This paper propose a participant free tagging system based on the fine-grained access control [12]. This system will initialise every user's individual face identity when they firstly authorize their Facebook accounts through our platform. Their face identities are generated by retrieving their Facebook profile pictures. When a user uploads a photo, the face area will be detected automatically and tagged with the name of the face owner by facilitating face recognition technology. Those tags can neither be removed nor changed by the photo uploader, and the uploader does not have the tagging right as well. As long as the photo is uploaded, those tagged users will be informed through Facebook internal notification. Then they can set their own face access control once they confirm they are the face owners.

2. RELATED WORKS

As a typical instantiation of Privacy Computing [13], privacy preserving Photo sharing has received considerable attention [14], [15]. [1] Addressed the privacy conflicts by quantifying privacy risk and sharing loss based on the tradeoff between privacy preservation and data sharing. Subsequently, [16] addressed the privacy conflicts by changing the granularity of access control from photo level to face level. Researchers have developed many access control mechanisms that specifically prevent leakage of users' privacy from photos posted in social media and some other fields as well [17],[18].

In photo-level access control, sensitive information is protected by applying access control mechanisms onto the photos. Compared to face level access control the mechanism is comparatively rough on the sensitive information protection. A negotiation-based method [19] enabled tagged users to send requests to photo owners who might require the photo to be concealed from certain groups of individuals. Theoretical collective privacy management solution builds upon a well-known game called Clarke Tax [20] . This approach had a strong assumption, where it required users to be able to compute the value of different preferences on sensitive information. Even though multiparty collaboration helps mitigate the conflicts of sharing interests between uploaders and participants, the problem still exists and they did not specify how their mechanisms countered the non-tagging or wrongly tagging behaviours.

The face-level access control mechanisms are to deal with the privacy problem with every participant in photos. Researchers [12],[21] proposed similar fine-grained access control mechanisms on social media photos. In these works, each face owner in the photo could determine if their faces are often viewed by others. The face would be blurred into an uninterpretable area if the permission wasn't given by the owner. The conflicts of sharing interests are solved in these works [12],[21].

3. SYSTEM DESIGN

In designing, integrate the photo sharing web-based system by leveraging the well-developed functions embedded in Facebook (i.e. Facebook App) which is provided with face-level access control mechanism but with an enhanced automatic participant-free face tagging process integrated. The system framework is shown in fig.1, which is composed of four stages. 1) Face identity initialization, 2) automatic face tagging process, 3) privacy setting mechanism, 4) photo rendering process.

Face identity initialization: Facebook users tend to upload photos that contain their own faces as the profile pictures. To facilitate the face recognition process, we first collect users' photos on Facebook, which contain their own faces as the face recognition training data. Then group the faces according to similarity by employing face recognition and the face set with largest number of faces considered to the users. The system will train the face set and face identity generated.

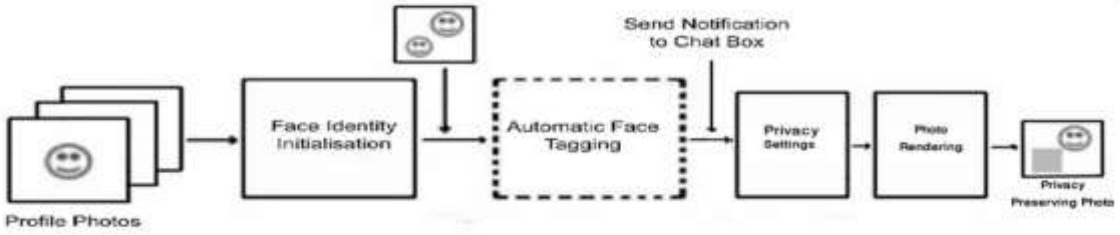


Fig -1: System framework

Automatic face tagging: For each detected face on the uploaded photo, system will perform face recognition once a social media user chooses a photo to upload. If there is minimum of one face being identified, the automated tagging process is activated. Two different approaches according to two scenarios of performing automatic tagging processes: (a) Face owner can be directly identified through our system by applying internal searching. (b) One or several faces cannot be found through internal searching. However, there is at least one face being successfully identified on uploaded photo.

Privacy setting: As long as the photo is uploaded, those tagged participants will be informed through Facebook internal notification. Then they can set their own face access control once they confirm they are the face owners. If the participant disallows the access to the photo the face will be blurred out.

Photo rendering: It is the process of masking/unmasking the faces in the uploaded photo. If a participant disallows the access to the photo containing his/her face in social media, his/her face will be blurred out by applying covers (e.g. mosaic). His/Her online friends who are not granted with access permissions will not see his/her appearance in the photo.

3.1 Exception Handling Mechanism

No Face is identified- During this situation, we allow the uploader to tag depicted users. Those tagged users are ready to view other people's faces during this photo, however, this photo can't be shared by anyone or appear in the other places but only uploader's homepage and therefore the users tagged by uploader cannot set their own access control also.

Face is wrongly identified- The computer can wrongly identify a face or the face can be mistakenly tagged by authorized users. Since our system will send notifications to all tagged users, only when the face owner is confirmed to be true, each tagged user's access control is then activated. In this case, the user can decline if it is not his or her face in the photo, and the face still remains blurred if no one claims the face. Even though the face may be tagged with different users in cooperative tagging process, it will go through the same confirmation process. Those faces are manually tagged by honest users (recognized by the computer), therefore, we assume that those users being tagged through cooperative tagging process will not lie and falsely claim the faces which are not supposed to be their own. In this case, the privacy is guaranteed.

3.2 SUPPORTING TECHNOLOGIES

Supporting technologies are includes the approaches about how the participants customize face-level access permissions to the photo containing their faces. There are two sets of APIs can be used for system design. These APIs are directly called by sending 'Ajax requests' to API providers' server.

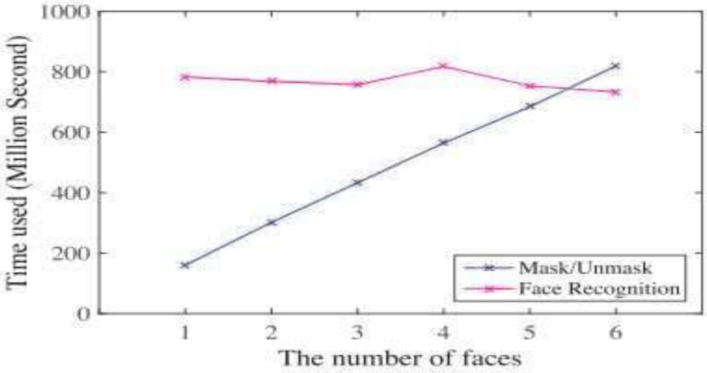
The first set is provisioned by Facebook for the usage of users' information retrieval. Once user has authorized his/her Facebook account through our App, the system will retrieve user's Facebook ID and a list of photos uploaded by user in Facebook.

The second set of APIs is provided by Microsoft Face as part of auto-tagging process. Though Facebook has its own auto-tagging technique for face recognition, the performance highly relies on users' behaviors. Facebook users can either choose to untag or falsely tag faces. These behaviors potentially reduce the chance and accuracy of being automatically tagged in Facebook. Moreover, Facebook's internal face recognition does not support the usage of external Apps. So, we designed the auto tagging processes and utilized Microsoft Face to provide face recognition functions. This improved the performance of automatic tagging processes.

4. System Evaluation

4.1 Efficiency Evaluation

In this section we evaluate the time used for our auto-tagging mechanism and photo masking. The results are shown in chart-1



.

Chart-1: Efficiency evaluation

Tagging efficiency mainly relays on the performance and accuracy of the face recognition technology, training data of face set and therefore the behavior of tagged users during cooperative tagging process. The time required for the tagging process equals to the time consumed for face recognition process. In this experiment, the photos having the same number of faces are gathered into the same group. Because the face recognition is conducted by Microsoft Face, the processing speed totally depends on the internet connection.

When evaluate the time required in masking or unmasking process, conclude that as the number of faces is growing, the time required for rendering a masked or unmasked photo increase as well.

4.2 Privacy evaluation

This section evaluate the privacy preserving performance of system by evaluating the size of blur area's impact on privacy preserving. for every group photo and individual photo, we apply two different sizes of blur area: (1) face area (face rectangle directly obtained from API result) (2) head area (includes face and hair area). The feedback from participants includes the content on the guessing of every masked user's name and the clues leading to their inference once they provide the right answer. The results show in chart-2.

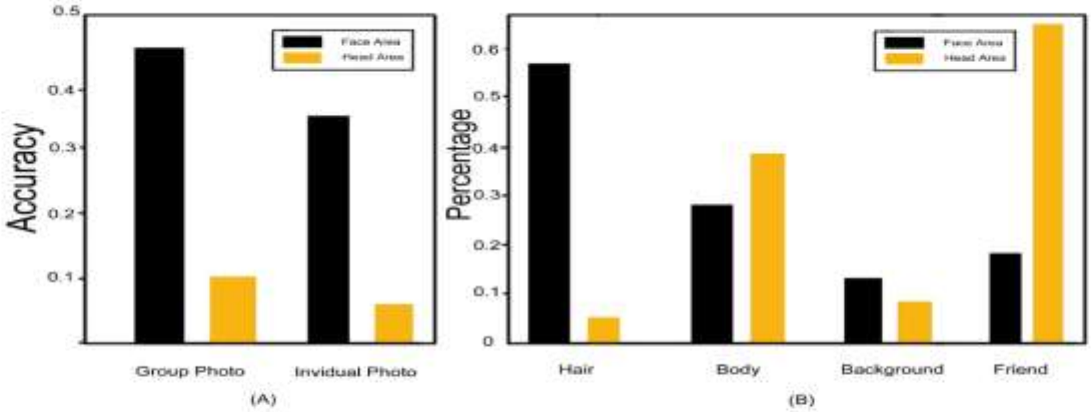


Chart-2: Privacy preserving result

Results show that the covering face area only is not enough for privacy preserving. 36.3% and 48.7% faces are correctly identified in individual photos and group photos respectively. The most reason why people can infer the proper answer is due to the hair, other clues are user's body features (for example figure, tattoo)photo background and therefore the other friends who are in the same photo. As we enlarge the blur area with the multiple 1.85 from the original face rectangle, making sure all the user's face and hair area are covered and the other people in the same photo are less likely being influenced by the enlarged blur area. We find that over 90% of users' identities are preserved both in group photos and individual photos. The main clue for inferring masked users becomes the other friends in the same photo.

5. CONCLUSIONS

In this paper designed and evaluated a privacy-preserving photo sharing framework, called Blur Me, which could help associated friends preserve their privacy once they share images with others in Facebook. The system can solve the matter caused by tagging behaviours from adversarial users. The evaluation results demonstrate the performance of the system.

REFERENCES

[1] Hu, H., Ahn, G.J., Jorgensen, J.: Multiparty access control for online social networks: model and mechanisms. IEEE Transactions on Knowledge and Data Engineering 25(7), 1614–1627 (2013).

[2] Such, J.M., Porter, J., Preibusch, S., Joinson, A.: Photo privacy conflicts in social media: A large-scale empirical study. In: Proc. of ACM CHI 2017.

[3] Zhang, L., Jung, T., Liu, K., Li, X.Y., Ding, X., Gu, J., Liu, Y.: Pic: Enable large-scale privacy preserving content-based image search on cloud. IEEE Transactions on Parallel and Distributed Systems 28(11), 3258–3271 (2017).

[4] Such, J.M., Criado, N.: Resolving multi-party privacy conflicts in social media. IEEE Transactions on Knowledge and Data Engineering 28(7), 1851–1863 (2016).

[5] Ilia,P.,Polakis,I.,Athanasopoulos,E.,Maggi,F.,Ioannidis,S.:Face/off: Preventing privacy leakage from photos in social networks. In: Proc. of ACM CCS 2015.

[6] Vishwamitra.N., Li,Y., Wang,K.,Hu,H.,Caine,K.,Ahn,G.J.:Towards pii-based multiparty access control for photo sharing in online social networks. In: Proc. of ACM SACMAT 2017.

[7] Kathrin, K., Baran, K.S.: Facets of Facebook: Use and Users. Walter de Gruyter & Co., Hawthorne, NJ, USA (2016).

[8] Kaszubska, G.: Not just revenge porn image-based abuse hits 1 in 5 Australians. RMIT, October 2017.

[9] Jansons, P.: Businesses use social media to screen job candidates. CareerBuilder, April 2016

[10] Smith, A.: 6 new facts about Facebook. Pew Research Center, February 2014.

[11] Trenholm, R.: Most Facebook photos are taken while we're drunk, survey says. CNET, December 2011.

[12] Liridona, G., Kathrin, K.: Chapter 1. Unfriending and becoming unfriended on Facebook, January 2016.

[13] Li, F., Li, H., Jia, Y., Yu, N., Weng, J.: Privacy computing: concept, connotation and its research trend. Journal on Communications 37(4), 1–11 (2016).

[14] Such, J.M., Criado, N.: Resolving multi-party privacy conflicts in social media. IEEE Transactions on Knowledge and Data Engineering 28(7), 1851–1863 (2016).

[15] Xu, Y., Price, T., Frahm, J.M., Monrose, F.: Virtual u: Defeating face liveness detection by building virtual models from your public photos. In: Proc. of USENIX Security 2016.

[16] Zhang, L., Liu, K., Li, X.Y., Liu, C., Ding, X., Liu, Y.: Privacy-friendly photo capturing and sharing system. In: Proc. of ACM UbiComp 2016.

[17] Wang, H., Cao, J., Zhang, Y.: A flexible payment scheme and its role-based access control. IEEE Trans. Knowl. Data Eng. 17(3), 425–436 (2005).

[18] Enamul Kabir, M., Wang, H., Bertino, E.: A conditional purpose-based access control model with dynamic roles. Expert Syst. Appl. 38(3), 1482–1489 (2011).

[19] Besmer, A., Richter Lipford, H.: Moving beyond untagging: photo privacy in a tagged world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2010, pp. 1563–1572. ACM, New York (2010).

[20] Squicciarini, A.C., Shehab, M., Paci, F.: Collective privacy management in social networks. In: Proceedings of the 18th International Conference on World Wide Web, WWW 2009, pp. 521–530. ACM (2009).

[21] Cutillo, L.A., Molva, R., Onen, M.: Privacy preserving picture sharing: enforcing usage control in distributed on-line social networks. In: Proceedings of the Fifth Workshop on Social Network Systems, SNS 2012, pp. 6:1–6:6. ACM (2012).