International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

AN AUTOMATIC TAGGING FRAMEWORK AGAINST UNPERMITTED PHOTO SHARING IN SOCIAL MEDIA

Vijitha A[1], Jitha K[2]

[1]*Dept. of Computer Science and Engineering, MEA Engineering College, Kerala, India*
[2]*Assistant Professor, Dept. of Computer Science and Engineering, MEA Engineering College, Kerala, India*

Abstract—On social platforms like Facebook, it is popular and pleasurable to share photos among friends, but it also puts other participants in the same picture in jeopardy when the photos are released online without permission from them. To solve this problem, recently, the researchers have designed some fine-grained access control mechanisms for photos shared on the social platform. The uploader will tag each participant the photo then they will receive internal messages and configure their own privacy control strategies. These methods protect their privacy in photos by blurring out the faces of participants. Malicious users can easily manipulate unauthorized tagging processes and then publish the photos, which the participants want them to be confidential in social media. To address this critical problem, we propose a participant-free tagging system for photos on social platforms. This system excludes potential adversaries through automatic tagging processes over two cascading stages: 1) an initialization stage will be applied to every new user to collect his/her own portrait samples for future internal searching and tagging, and; 2) the remaining unidentified participants will be tagged in cooperative tagging stage by the users who have been identified in the first stage. For the system evaluation of efficiency and effectiveness, we conducted a series of experiments. The results demonstrated the tagging efficiency (96)

Key Words: Social media, face tagging, privacy protection, system security.

1. INTRODUCTION

Social media playing a big role in all over world. There are lot of social media platform where you can join with anyone. Social media is growing tremendously from last 10-12 years.as technology are growing then lots of peoples get benefits of it. Apart from this we can see there are some advantages and disadvantages of social media. Social platforms like Facebook, it is popular and pleasurable to share photos among friends, but it also puts other participants in the same picture in jeopardy when the photos are released online without the permission from them. Social media have gradually changed people's default privacy settings by forming a "sharing culture" among online users. They start to tolerate, get used of, or even accept the exposure of their personal private information in social media platforms. For example, it was reported that 91 percentage teenagers uploaded their own photos on Facebook (i.e. a famous social media platform), and 92percentage used to post their real name onto Facebook profile. There are also online exhibitionism and narcissism (i.e. behaviour's that are more open at sharing photos in social media), which have been regarded as actions of personal brand-building. Along with the growing willingness to share, people are also reported to be less conscious of the content of photos they are going to upload. For example, there are 34 percentage of Facebook users claimed that they did not think about the possible harm (e.g. leak of personal privacy) to their friends before they uploaded the photos. In a survey recently run by Pew Research Centre (PRC), they issued a questionnaire about why some users dislike using Facebook, and identified one of the most possible reasons as "people can post some- one's personal information (e.g. photos) without asking for permissions". In another survey posted by CNET, over 90 percentage of photos that tagged users who were drunk or at other embarrassed moments will be untagged or even removed soon from their Facebook timeline, since the tagged users usually wanted them to be unseen from others. These negative impacts are depressed but still under control, however sometimes, the harm is even worse and could be hard to estimate. For example, an in appropriate photo posted in social media may result in unemployment situation in some cases. It was reported that over 57 percentages of small business employers are using social media to screen job candidates. Among those employers, 45 percentages of them have experiences of not hiring a candidate due to their provocative or inappropriate photographs collected from social networking sites. It is somewhat unfair to the unemployed candidates because these 'harmful' photos may not even be uploaded by the candidates themselves. We propose a participant-free tagging system for photos on social platforms. To address this critical problem, we propose a participant-free tagging system for photos on social platforms. This system excludes potential adversaries through automatic tagging processes over two cascading stages: 1) An initialization stage will be applied to every new user to collect his/her own portrait samples for future internal searching and tagging. 2) The remaining unidentified participants will be tagged in cooperative tagging stage by the users who have been identified in the first stage. For the system evaluation of efficiency and effectiveness, we conducted a series of experiments.

2. LITERATURE REVIEW

The pervasive use of digital cameras and the increase of content sharing websites like Flickr and Picasa, people can now easily publish their photos or videos online and share

them with family, friends, co-workers, etc. While extremely convenient, this new level of pervasiveness introduces acute privacy issues. The persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. Most content sharing websites allow users to enter their privacy preferences. For example, Flickr provides five privacy levels: "private", "family only", "friends-only", "friends-and-family" and "public", for users to choose for each of their own photos. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main rea-sons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure settings. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images due to the following important considerations.[1]

An Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. In particular, we examine the role of image content and metadata as possible indicators of users' privacy preferences. We propose a two-level image classification framework to obtain image categories which may be associated with similar policies. Then, we develop a policy pre- diction algorithm to automatically generate a policy for each newly uploaded image. Most importantly, the generated policy will follow the trend of the user's privacy concerns evolved with time. We have conducted an extensive user study and the results demonstrate effectiveness of our system with the prediction accuracy around 90The goal of the A3P system is to enhance users' experience in content sharing sites, by suggesting customized set- tings when uploading images.

. Sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed cophoto for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus- based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform. Generally speaking, the consensus result could be achieve by iteratively refining the local training result: firstly, each user performs local supervised learning only with its own training set, then the local results are exchanged among collaborators to form a global knowledge. In the next round, the global knowledge is used to regularize the local training until convergence. In this section, firstly, we use a toy system with two users to demonstrate the principle of our design. Then, we discuss how to build a general personal FR with more than two users.[2]

The potential harm to users' privacy caused by the photo sharing. In order to address the concerns on both sides, previous methods mainly adopted access control mechanisms onto social media photos from either photo-level or face- level protection. In the photo-level category, only selective social media users were allowed to view the photos. However, a user who had the permission to view a photo could assess to all the information in the photo. Therefore, photo- level access control mechanisms were relatively coarse and they could hardly provide diverse privacy preserving protections if participants in a photo did have different requirements of sharing. Distinguished from photo-level protection, the face-level protection provided a fine-grained solution by managing the access to each participant's face in the photo. Typically, each participant will be informed when the photo containing their faces are uploaded, and the participant will decide the access permission to his/her own face. For example, 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. This category of face- level access control mechanisms enabled personally privacy settings for each participants in photos and successfully handled the cases of interests conflicts of photo sharing in social media.[3]

3. SYSTEM DESIGN

We designed a web-based photo sharing application (i.e. Facebook App) that provided face-level privacy protection (i.e. participants' faces). The application was implemented and integrated into Facebook by leveraging platform's APIs. Distinguished from previous work, the new design has realized the automatic participant- free face tagging mechanism. In our system design, we reckon that only tagged users could set their own face access control (i.e. to decide who could view their own faces on a specific photo shared on Facebook). Only those who have been correctly tagged by our system could go for the cooperative tagging process.

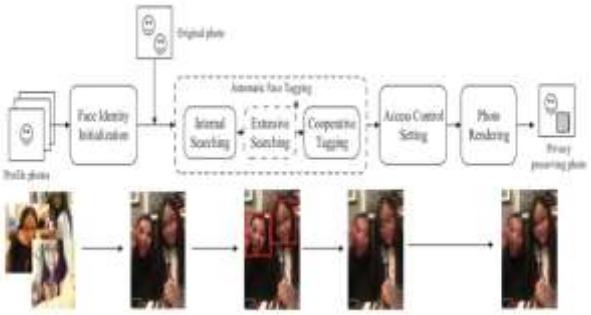

Fig1: System Framework

The system framework is shown in Figure.5, which is composed of several stages.

1) The face identity initialization

2) Automatic face tagging process

3) Access control setting mechanism

4) Photo rendering phase.

Compared to previous works, our contributions are the face identity initialization and automatic face tagging process which are designed to mitigate the malicious tagging behaviours. In the above framework, we employed Facebook's APIs to retrieve users' face information so that the system can generate individual's face identity for later use. During the automatic face tagging process, we adopted face recognition technology developed by Microsoft for internal searching and cooperative tagging processes

3.1 API SUPPORT

There are two sets of APIs that can be used for our 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. Give an arbitrary user ion Facebook, we summarize the detailed tasks from the first set of APIs as follows: Once user has authorized his/her Facebook account through our App, the system will retrieve user i's Facebook ID and a list of photos uploaded (lip∈Li,p ∈N, p = 1,2,3...,n) by user iin Facebook. The second set of APIs is provided by Microsoft Face as part of our auto-tagging process. Though Facebook has its own auto-tagging technique for face recognition, the performance highly relies on users' behaviours. Facebook users can either choose to untag or falsely tag faces. These behaviours 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. Therefore, we redesigned the automatic tagging processes and utilized Microsoft Face to provide face recognition functions. This improved the performance of automatic tagging processes.

3.1.1 Access Control

Supporting technologies also include approaches about how the participants customize face-level access permissions to the photo containing their faces. Basically, online friends of a photo participant (e.g. user i) can only view the authorized area in the shared photo such as user i's face area after been authorized. If online friends' visit to the photo are not authorized by user i, the specific face area will be blurred out. In our work, the access control processes will be similar to the works. In our system framework, we will reuse this part to implement the face-level protection. The access control module is located in the server side.

3.2 FACE IDENTITY INITIALIZATION

We decide to collect users' profile picture photos on Face-book to facilitate face recognition processes. The profile picture photos usually contain users' own faces. In the face identity initialization step, we define Lito be the photo set of an arbitrary user in Facebook. All the photos in user i's profile album will be collected and stored in Li. Only when user registers his/her Facebook account through our app for the first time, his/her photos will be collected and uploaded to set Li. According to our empirical survey, the face set containing the largest number of faces is most likely to be user i's face set. Therefore, we first extract all the faces appearing in the photo set Li, and then group them according to face similarity. The group that has the largest number of faces will be recognized as user i's face set Fi. The face areas in the set Fiare used as the primary training data of Facebook user for the face recognition process. After training, we store user i's trained model (ti) on the server side which will be used in auto- tagging process. In our face identity generation, we designed 3 stages based on the survey results.

Fig2: Generate Face Identity

3.3. AUTOMATIC FACE TAGGING

The system will conduct face recognition on every face area once a photo is uploaded by Facebook users. If at least one face is recognized, the automatic tagging process will be activated. We proposed two different methods according to three consecutive sub-stages of performing automatic tagging processes:

1) Internal Searching: Face owner can be identified directly by our system,

2) Extensive Searching: Remaining untagged users could be identified by external public searching engine (e.g. Google)

3) Cooperative Tagging: This sub-stage will be activated when there are still some participants who cannot be recognized by both internal and extensive searching sub-stages.

3.3.1 Internal Searching

Algorithm 1 Tagging Mechanism

Input: Detected faces (u_{vk}) in uploaded photo (v)
Output: Candidates of each depicted face in uploaded photo

```
for k ← 1 to n do
    for q ← 1 to m do
        confidence ← compareFaces(u_vk, I_q);
        if confidence ≥ ε then
            sendNotification(u_vk, I_q);
        end
    end
    if candidates.length() == 0 then
        cooperativeTaggingList ←
        putInCooperativeTaggingList(u_vk);
    end
end
```

Fig3: Tagging mechanism algorithm

In the above internal face searching sub-stage, if the system receives more than one confirmations from candidates related to only one face area, there must be some candidate/candidates who have made mistake/mistakes. This happens usually when different people look similarly to each other so that their confidence scores are higher than ε. According to our investigation, this mistake may be caused by malicious spoofing. Spoofing means that attackers adds portraits of others into the attackers' own profile photo album to deceive the face identification process. In some other scenarios, the mistake may be caused by the face areas from Twins. That is why, in our design, the internal searching will provide more than one candidates and our system will send face confirmation request to all the remaining candidates to avoid the false identification. If more than one candidate claim the ownership of a face area, our system will conduct the cooperative tagging process in which the real face owner are determined by the people who have been correctly tagged by the system.

3.3.2 Cooperative Tagging

If there are still some remaining participants that our internal searching is unable to identify, the cooperative tagging pro- cess will be activated to help find the face owner. Note that cooperative tagging will only run when at least one face in the photo have been correctly tagged in the previous sub-stages. Since the users who have been tagged are identified by our automatic tagging system, they are believe to be honest in cooperative tagging process. It is unlikely for them to falsely recognize the remaining participants in the photo because they apparently know who they were taking the photo with. Based on this intuition, our system allows these users who have been tagged are identified to tag the rest participants in a cooperative way. The cooperative tagging process will not be activated if only one person involves in this process, and the current tagging result will be regarded as the final result. If two or more participants involves in cooperative tagging process, our system will adopt the voting principle in this process to identify the face owner, which means that the candidate with the highest number of votes will be considered as the face owner.

3.4. EXCEPTION HANDLING

3.4.1 No face has been identified

The first exception is about 'no face has been identified'.ie, no participant can be identified through all the previous sub-stages including internal searching, extensive searching, and cooperative tagging. The photo cannot be shared by any- one or appear in any other places but only uploader's home-page. The participants tagged by the uploader also cannot set their own access control.

3.4.2 Face is wrongly identified

The system may wrongly identify a face or those authorized users may falsely tag a depicted participant in the cooperative tagging process . Once received the notifications from the system, each tagged participant will set their own access control after they have confirmed the face ownership. In the case, if the face sent to the tagged user is not his/hers, the user can response a negative confirmation to the notification, and the face will be blurred out if there is no user to claim the ownership of the face. Even though there may be some cases in which the tagging results of one depicted face are not consistent in cooperative tagging process, each face will go through the same confirmation process. Those faces are manually tagged by honest participants (i.e. The ones who have been certified by the system). We assume that the participants who are recognized by cooperative tagging process are honest and will not wrongly claim the faces which do not belong to them. Therefore, the privacy can be protected.

4. SYSTEM VALIDATION

All the experiments below are conducted on an Amazon Web Server EC2 with 100MB/s down/up-link speed. On the server side, we adopted MySQL as our system database and the PHP version was 5.6.30. On the client side, we used MacBook Pro that has macOS Sierra system (version 10.12.6) installed. The test computer had memory of 16GB and the processor was 2.7 GHz IntelCore i7

4.1 EFFICIENCY EVALUATION

We evaluate the efficiency of the auto- tagging mechanism and the photo masking process in terms of time consuming

4.1.1 Tagging Efficiency

Tagging efficiency highly depends on the accuracy and performance of the face recognition technology, the training data of face set, and the behavior of tagged users during the cooperative tagging process. The tagging efficiency is actually affected by three factors:

1) Face recognition,

2) Training data

3) Tagging behaviours.

The third factor is highly related to personal characters, which cannot be easily examined through experiments. In fact, even though there may be some mistakes in the cooperativetagging process due to the unpredictable behaviour of the tagged users, as long as they take part in this process, the tagging efficiency will be improved due to their honest confirmations. We can see that the number of faces that appeared in a photo had little impact on the time consumed in the face recognition processes. We systematically investigated the reason for this phenomenon. We found that since our system use the face recognition service provided by Microsoft Face, the Internet condition has significant impact on the time used for this process. Therefore, when there was a good networking condition, the time consuming was steady. In our experiments, the average time for auto- tagging was around 0.77s per photo.

4.1.2 Time Consuming

The time required for the tagging processes can be assessed by evaluating the time used for the face recognition processes. In the experiments, we organized six groups. Every group contains ten photos and the photos in same group have the same number of faces inside each photo. For example, every photo in group one only has one face inside, and every photo in group two will have two different faces inside. The same also happens in group three to group six.

4.1.3 Tagging Successful Rate

All the volunteers have uploaded more than five photos that containing their por- traits to the album. Each volunteer provides ten test photos containing their own faces (200 photos in total). We found out that our system achieved a high tagging successful rate is around 96 percentage by using the Facebook profile pictures as the training data to generate the face identities. Tagging successful rate from 30 volunteers who have already generated their face identities in our server. The results showed that the tagging rate was around 96percentage.. This proved that it was a solid solution to extract the face information from users' Facebook profile picture album to generate their face identities.

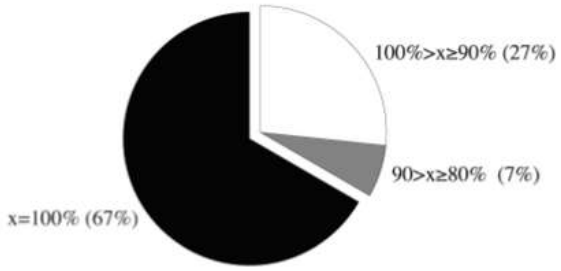

Fig4: Tagging successful rate that generated their face identities in our server.

4.2 MASKING/UNMASKING EFFICIENCY

We also evaluated the time used for masking or unmasking process. Intuitively, the time used in both grows with the increase of the number of faces in a photo, since blurring out the face areas takes the most time in these process. We can see that with the number of faces areas in a photo growing, the time used for processing a masked or unmasked photo increased linearly. The increment was around 0.13s per face on average

4.3 PRIVACY EVALUATION

We will first evaluate the effect of the blur area's sizes on privacy protecting. Based on the result, we can then evaluate the effectiveness of our approach in preserving the privacy of depicted users

4.3.1 Impact of blur area's size on privacy preserving

The results of our survey show that it is not enough to protect privacy if we only cover face area. 46.7 faces in group photos are correctly recognised while it is 37.3 in individual photos. The dominating clue for inferring the masked users correctly is the hair, and there are other helpful clues for correct inference, including user's body feature (e.g. figure, tattoo), photo background and the other friends appeared in one photo. Figure 9 : Privacy Evaluation Case. This figure shows the possible clues which could possibly lead to the right inferences. There are three reasons that we concluded from our experiments, they are hair, body features (A), background (B) and the friend in the same frame (C).

The example images show in Fig. 9 As we enlarge the blur area with the multiplication of 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 reason why people can infer the right answer becomes the other friends in the same photo.

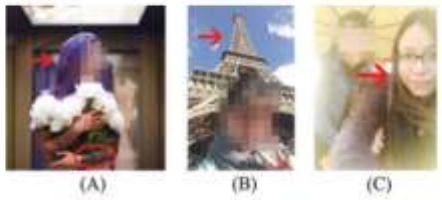

Fig5: Privacy Evaluation Case

4.3.2 Malicious Tagging Attack Mock-up

In order to evaluate the robustness of privacy preserving of our system, we mock up several attacks by faking face identities and pretending to be other people. we register new facebook accounts and upload a's portrait pictures in profile picture album of this newly registered account. a's portrait pictures are obtained from a's facebook photo and a is also a member using our system. after we have uploaded a group photo containing a's face, our spoofing account did receive the confirmation notification. even though we confirm the ownership of the faces through our spoofing account, we are still unable to apply our access control to a's face. Therefore, our system is immunized to the malicious tagging attack.

6. CONCLUSION

An automatic tagging framework to preserve users' privacy for photo sharing in social media. The new framework could tackle the problem of malicious tagging from adversaries To validate the newly developed framework, we carried out a number of supporting research works as well as experiments in the context of Facebook. In fact, the proposed framework can be easily integrated into other social media platforms like Twitter, WeChat and other microblog services. The experiment results indicated that our framework achieved the efficiency with 96% tagging rate.

REFERENCES

[1] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, ''A3P: Adaptive policy prediction for shared images over popular content sharing sites,'' in Proc. 22Nd ACM Conf. Hypertext Hypermedia, New York, NY, USA, 2011, pp. 261–270.

[2] B. A. Bouna, R. Chbeir, A. Gabillon, and P. Capolsini, ''A flexible image-based access control model for social networks,'' in Security and Privacy Preserving in Social Networks. Vienna, Austria: Springer, 2013, pp. 337–364.

[3] K.Xu,Y.Guo,L.Guo,Y.Fang,andX.Li,'' My privacy My decision: Control of photo sharing on online social networks,'' IEEE Trans. Dependable Secure Comput., vol. 14, no. 2, pp. 199–210, Apr. 2017.

[4] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, ''iPrivacy: Image privacy pro- tection by identifying sensitive objects via deep multi-task learning,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1005–1016, May 2017.

[5] H.Hu,G.-J.Ahn,andJ.Jorgensen,''Enablingcollaborativedatasharing in Google+,'' in Proc. IEEE Global Commun. Conf. (ACSAC), Dec. 2012, pp. 103–112. [19] A. C. Squicciarini, M. Shehab, and F. Paci, ''Collective privacy management in social networks,'' in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 521–530