Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 2, Issue 5, August 2018
Proceedings of National Conference on Knowledge Discovery in Information Technology and Communication Engineering (KITE 18), May 2018

My Privacy My Decision: Control of Photo Sharing on Online Social Network

Shilpa S, Sravani P, Subinu Salam, Yathish N S
Department of Computer Science and Engineering, Brindavan College Of Engineering, Bengaluru, India,
shilpa7297@gmail.com

Abstract: Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak user's privacy if they are allowed to post, comment, and tag a photo freely. In project, we attempt to address this issue and when a user shares a photo containing individuals other than himself/herself (termed co-photo 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.

Keywords: Social network; photo privacy; secure multi-party computation; support vector machine; collaborative learning

I. INTRODUCTION

Online Social Networks have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos, over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue.

Comparing with previous works, our contributions are as follows.

1) In this project, the potential owners of shared items(photos) can be automatically identified with/without user-generated tags.
2) We propose to use private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user.
3) Orthogonal to the traditional cryptographic solution, we propose a consensus-based method to achieve privacy and efficiency.

II. RELATED WORK

In [6], Choi et al. discuss the difference between the traditional FR system and the FR system that is designed specifically for OSNs. They point out that a customized FR system for each user is expected to be much more accurate in his/her own photo collections. A similar work is done in [5], in which Choi et al. propose to use multiple personal FR engines to work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suitable FR engines that contain the identity of the queried face image with high probability. In [2], Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in [2] to study the effectiveness of the existing countermeasure of untagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when untagging.

III. EXISTING SYSTEM

In Online Social Networks have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. Posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people.

A. Disadvantages of existing system

- Very Less Security for Posted Images on Social Network
- Lack of Privacy for Private users.

- Less Security for the photos in online social networks.
- Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved.

IV. PROPOSED SYSTEM

Photo sharing is one of the most popular features in online social networks such as Face book. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in a co-photo. The proposed system is featured with low computation cost and confidentiality of the training set. We expect that our proposed scheme be very useful in protecting users' privacy in photo/image sharing over online social networks.

A. Advantages of proposed system

- Restriction on the sharing photos without permission.
- Providing high security for private data in Social networks.
- Efficiency is more.

V. SYSTEM ARCHITECTURE

Our prototype application is implemented on Google Nexus 7 tablets with Android 4.2 Jelly Bean (API level 17) and Facebook SDK. We use OpenCV Library 2.4.6 to carry out the face detection and Eigen face method to carry out the FR. Fig. shows the graphical user interface (GUI). A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works During the training process, a socket is established exchange local training results. After the classifiers are obtained, decision tree is constructed and the program switches from the setup mode to the sleeping mode. Facebook allows us to create a list of friends such as "close friends" or "Acquaintances". We can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner's privacy policy and co-owners' exposure policies. However, in Facebook API, friend lists are read-only items, they cannot be created or updated through the current API. That means we cannot customize a friend list to share a co-photo. Currently, when the button "Post Photo" is pressed, co-owners of x are identified, then notifications along with x are send to the co-owners to request permissions. If they all agree to post x, x will be shared on the owner's page like a normal photo. In this sense, users could specify their privacy policy but their exposure policies are either everybody on earth or nobody depending on their attitude toward x. The data flow for a photo posting activity is illustrated by the solid red arrows. After the requests are sent out, the program will go back to the sleeping mode.

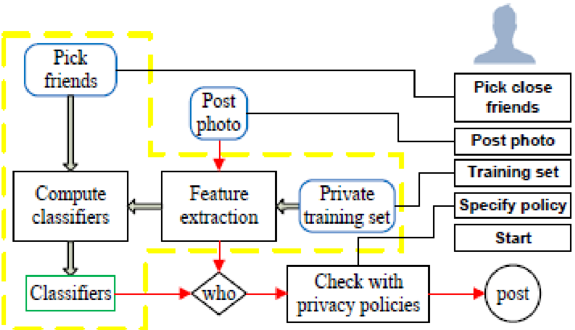

Fig 1. System architecture of our application

VI. FLOW CHART

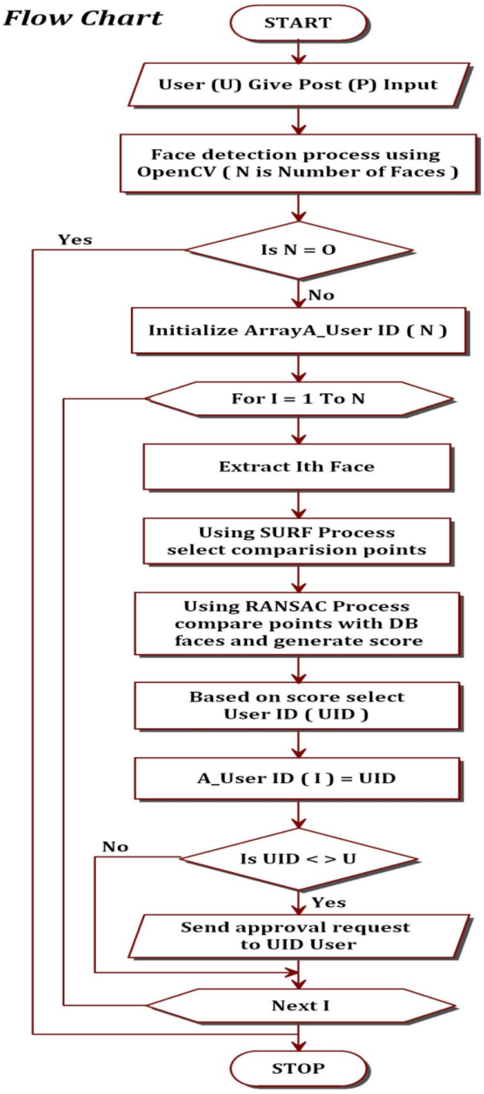
Flow Chart
START
User (U) Give Post (P) Input
Face detection process using OpenCV (N is Number of Faces)
Yes
Is N = O
No
Initialize ArrayA_User ID (N)
For I = 1 To N
Extract Ith Face
Using SURF Process select comparision points
Using RANSAC Process compare points with DB faces and generate score
Based on score select User ID (UID)
A_User ID (I) = UID
No
Is UID < > U
Yes
Send approval request to UID User
Next I
STOP

Fig 2. Flowchart

VII. CONCLUSION

Photo sharing is one of the most popular features in online social networks such as Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in a co-photo. The proposed system is featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme. Photo sharing is one of the most popular features in online social networks such as Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in a co-photo. The proposed system is featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme. We expect that our proposed scheme be very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. For example, in our current Android application, the co-photo could only be post with permission of all the co-owners. Latency introduced in this process will greatly impact user experience of OSNs. Moreover, local FR training will drain battery quickly. Our future work could be how to move the proposed training schemes to personal clouds like Dropbox and/or icloud. The heading of acknowledgment and references should not be numbered as section.

REFERENCES

[1] I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.

[2] A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[3] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan. 2011.

[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.

[5] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.

[6] K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition frameworkonasocialnetworkplatform. InAutomaticFaceGesture Recognition, 2008. FG '08. 8th IEEE International Conference on, pages 1–6, 2008.

[7] K. Xu, Y. Fang, X. Li are with the Department of Electrical and Computer Engineering, Gainesville, FL 32611, USA. E-mail: xukaihe@ufl.edu, ffang, andylig@ece.ufl.edu.

[8] L. Guo is with Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA. E-mail: lguo@binghamton.edu.

[9] Y. Guo is with School of Electrical and Computer Engineering, Oklahoma, State University, Stillwater, OK 74078, USA. E-mail: richard.guo@okstate.edu