

Face Recognition: Control of Photo Sharing on Online Social Networks

Ms. Pathak Anchal¹ Ms. Karina Maiyani² Ms. Sawani Erande³ Ms. Rumana Mulani⁴
Prof. S. S. Gawai⁵

^{1,2,3,4,5}Dr. D. Y. Patil Polytechnic, Akurdi, Pune-411044, India

Abstract— In online social network (OSN) user's resource may contain the privacy of other resources. Most of the social networking sites provides features that allows user to easily upload and post photos on social network. Many privacy violations occur in current online social network which becomes a serious problem. Unfortunately photos that a user is tagged in, have very few privacy control. Nowadays researchers focuses on how to integrate into co-worker's willingness of privacy when setting access rule for resource. In this paper we study the situation when a client shares a photograph containing people other than himself/herself. We proposed a system where photo can be shared in a secure way. Proposed framework can help clients to effortlessly and appropriately design security settings. The existing system has the individual face recognition system installed with each user, which is very time-consuming. Proposed system has a centralized FR engine in charge of recognizing all users over a large OSN. Effectiveness and Flexibility is good of Proposed Solution.

Key words: Wireless Sensor Network, Active Trust, Trustable Routing, Networking

I. INTRODUCTION

Photo sharing is an interesting component of Online Social Networks (OSNs)[6]. Users have no control over data residing outside their spaces. Each user has a different privacy concerns about the photos related to them. Each user can tag/share contents to his/her friends. OSNs only allows us to keep or delete the content. A large proportion of photographs contain face images which are associated with the daily lives of the photographers who captured them. Currently, online social networks (OSNs) such as Facebook, Instagram, Twitter, and Snapchat are prevailing platforms on which people communicate with their social connections such as friends, family members, and colleagues in the real world. Social networks, due to many unfavorable incidents, have been blame for breaching the privacy of their users. Both in academia and in the media, the importance of a user's confidentiality has been rarely discussed. In addition to some proposed technical solutions, there have been a huge number of initiatives to educate users so that they do not provide an excessive amount of personal information. Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam. In the past, there was a buzz regarding the privacy settings of Facebook as it was very complicated but later they have simplified it for better understanding and easy access to common people. Due to lack of knowledge and understanding of privacy features of Facebook, people make many mistakes. Another important thing which should be

controlled is the availability of the personal information which should be prevented from leakage as it may reveal personal information of an individual in the form of videos, images or any data. As the popularity of social networks continues to grow, concerns surrounding sharing information online compound. Users regularly upload personal stories, photos, videos, and lists of friends revealing private details to the public. To protect user data, privacy controls have become a central feature of social networking sites but it remains up to users to adopt these features. Privacy restrictions form a spectrum between public and private data[5]. On the public end, users can allow every Facebook member to view their personal content. On the private end, users can restrict access to a specific set of trusted users. Facebook uses friendship to distinguish between trusted and untrusted parties. Users can allow friends, friends of friends, or everyone to access their profile data, depending on their personal requirements for privacy

II. RELATED WORK

A paper on "Privacy-Preserving Photo Sharing Based on a Secure JPEG" by Lin Yuan, Pavel Korshunov and Touradi Ebrahimi[3] designed a framework which is based on secure JPEG framework that integrates diff. tools to protect photo privacy. There are various tools to ensure the image privacy such as filtering, encryption, scrambling. In this paper general scrambling is used. To secure metadata authors does the encryption of selected JPEG metadata in the exchangeable image file format (Exif) tag. Author has designed server which hosts only secure photos uploaded by users. Also author has developed a multiregion selective JPEG scrambling scheme. This framework prevents unauthorized access to photos, automatic identification recognition and image data mining. A paper on "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collection" by Jae Young Choi, Wesley De Neve, Yong Man Ro[2] proposed a system in which distributed approach(multiple FR engines) is used to perform operations such as subject identification and verification. Most of the existing system have been developed by using centralized approach like video surveillance, national security. In this paper author believes that multiple FR engines-belonging to members with close relationships can improve the accuracy of face annotation. Two key issues are addressed here: first one is the selection of expert FR engines that are able to recognize query face image. And 2nd one is the merging of multiple FR results into a single FR result. Here for the selection of multiple FR engines social graph model(SGM) is constructed. SGM is created by using personal photo collections shared in the collaborative FR framework. Detected images are forwarded to selected FR engines. Then results are merged by using diff face extractors and classifiers. Finally we get the accurate face annotation. Large amount of attention is required for the creation of this framework. A paper on

“Moving Beyond Untagging: Photo Privacy in Tagged World” by Andrew Besmer and Heather Richter Lipford[1] proposed a system in which “Restrict others” tool is used to address photo privacy. It works by allowing tagged users to send a request to the owner asking that a photo be hidden from certain people. The tagged user is able to set the custom permissions at the individual photo level. This tool promotes sharing by reducing the need for the tagged user to untag the photo or restrict all their tagged photos. This tool lets user specify individuals or groups of users they would like to restrict the photo from. A paper on “Autotagging Facebook: Social Network Context Improves Photo Annotation” by Zak Stone, Todd Zickler, Trevor Darrell[4] proposed a framework in which task of automatic face recognition in personal photographs is done. Author combine face recognition scores with social context in a conditional random field (CRF) model and apply this model to label faces in photos from the popular online social network Facebook, which is now the top photo-sharing site on the Web with billions of photos in total.

III. PROBLEM DEFINITION

To address the issue of photo sharing vulnerabilities and study the situation when a client shares a photograph containing people other than himself/herself (termed cophotograph) and provide privacy protection to photo being shared.

IV. PROPOSED SYSTEM

Photograph sharing is an alluring component which advances Online Social Networks (OSNs). Sadly, it may release client’s security on the off chance that they are permitted to post, remark, and label a photograph openly. In this paper, we endeavor to address this issue and study the situation when a client shares a photograph containing people other than himself/herself (termed co-photograph for short). We are proposing a system where photo can be shared in a secure way.

A. Module Description

1) Set Up

This module will setup basic framework to accept user profiles and their face pictures. It has different tabs on home screen about project description, new user registration, Login and Contact Us page.

B. Face Recognition

According to the Facebook statistics, on average a user has many friends but only few of them are trustworthy. We assume only a small portion of them are close friends. In our application, each user picks up to 30 friends. Notice that all the selected friends are required to use our application and register their profile by uploading their profile photos to carry out the collaborative training. After the classifiers are obtained, feature extraction is done, decision is taken to classify whether picture is a face or nonface. Viola Jones algorithm is used for the checking if the uploaded image is face or not.

1) Privacy Policy & Face Matching

After taking the registrations from user, user can send the friend request to anybody to become friends and other requested person can accept friend request if he wish to become friend. Whenever user wants to upload a group photo then he can upload a group picture using “Update Status” option given in system. Once photo uploading is done, face recognitions are done and checked if anybody in the system has the similar face. Nearest neighbor algorithm is used for finding best match. If the face matching is successful then a request sent to them for seeking a permission for uploading the photo. 4. Control decisions for privacy: Once somebody uploads users X’s photo, he will get the request from the person who is uploading the photo, he can wish to allow or deny him from uploading the photo. Before proceeding to vote for permission he needs to answer the security question provided by him during the profile creation.

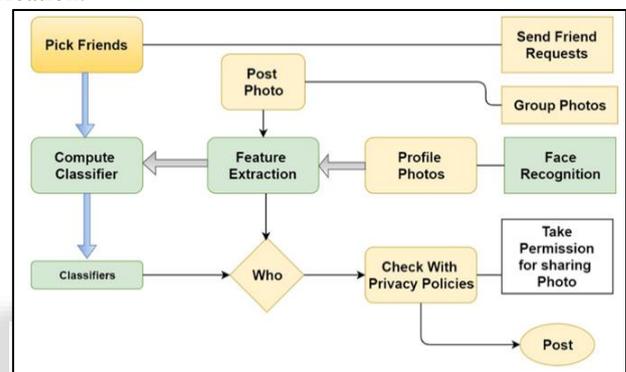


Fig. 1: System Architecture

V. CONCLUSION & FUTURE SCOPE

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations, for example Facebook. Unfortunately, imprudent photograph posting may uncover security of people in a posted photograph. To control the security spillage, we proposed to empower people possibly in a photograph to give the consents before posting a co-photograph. We planned a security safeguarding FR framework to recognize people in a co-photograph. The proposed framework is highlighted with low calculation expense and privacy of the preparation set. We expect that our proposed plan be exceptionally helpful in ensuring clients protection in photograph/ picture sharing over online informal organizations. Approach presented in this procedure will enormously affect client experience of OSNs.

REFERENCES

- [1] A Besmer and H Richter Lipford Moving beyond untagging photo privacy in a tagged world CHI '10 pages 1563 1572 New York NY USA 2010 ACM .
- [2] J Y Choi W De Neve K Plataniotis and Y M Rao, Improved face annotation and Collaborative face recognition Multimedia IEEE Transactions on 13 1 14 28 2011
- [3] Lin Yuan, Pavel Korshunov, and Touradi Ebrahimi Privacy-Preserving Photo Sharing on a Secure JPEG 2013.

- [4] Zak Stone, Todd Zickler, Trevor Darrell Autotagging Facebook: Social Network Context Improves Photo Annotation.
- [5] Altman. Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3):66-84, 1977.
- [6] 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*: 06.

