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

Ms. Khandagale Dipali P.
Computer Science and Engineering
SVERI's COE, Pandharpur, Solapur University
Solapur, Maharashtra
dips.khandagale@gmail.com

Prof. Khandagale Satyawan P
MCA Department
Zeal College, Narhe, Pune
Pune, Maharashtra
satyavan.khandagale@zealeducation.com

Prof. Mrs. Satarkar Prajakta A.
Computer Science and Engineering
SVERI's COE, Pandharpur, Solapur University
Solapur, Maharashtra
pasatarkar@coe.sveri.ac.in

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.

Keywords: *Privacy, FR engine, online Social networks, Flexibility.*

*****

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.

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.

A. Motivation

Despite the spectrum of available privacy settings, users have no control over information appearing outside their immediate profile page. When a user posts a comment to a friend's wall, he cannot restrict who sees the message. Similarly, if a user posts a photo and indicates the name of a friend in the photo,

the friend cannot specify which users can view the photo. For both of these cases, Facebook currently lacks a mechanism to satisfy privacy constraints when more than one user is involved. This leads to privacy conflicts, where asymmetric privacy requirements result in one user's privacy being violated. Privacy conflicts publicly expose personal information, slowly eroding a user's 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 co-photograph) 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.

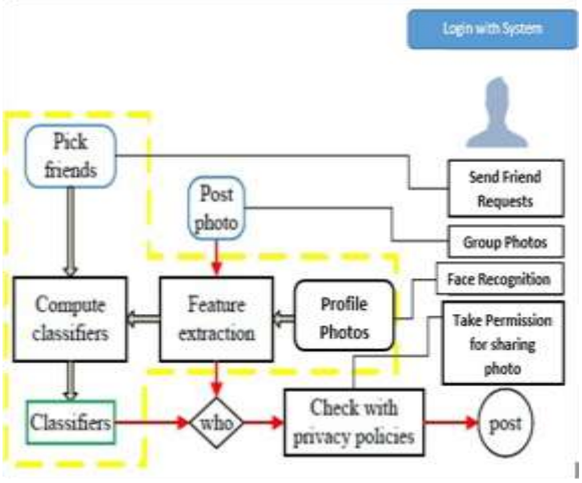


Figure1. Proposed System

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.

2. 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 non-face. Viola Jones algorithm is used for the checking if the uploaded image is face or not.

3. Privacy Policy and 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. This is just to add the more security for the system. Secure key can be shared between two people which can be used while taking permission for uploading the photo. Once user allows to upload the photo by clicking on ”Allow” photo will be shared and if he clicks on ”Deny” photo will not be posted.

5. Other Security policies : When a photo is shared online, another users will not be able to manipulate it. Users are not allowed to save it , which adds more security to the system and the privacy of posted photos is preserved.

B. Flowchart of proposed system

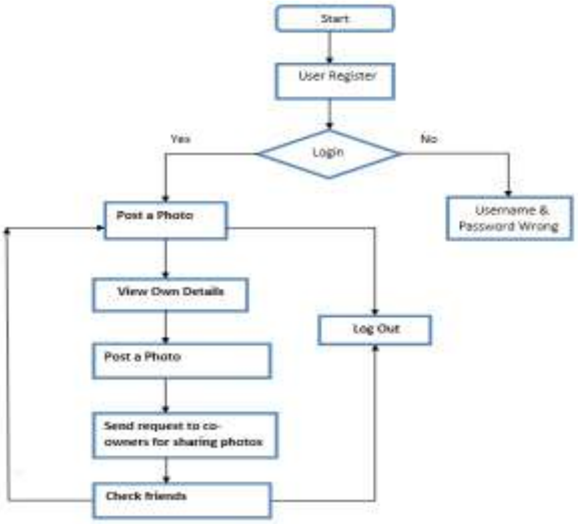


Figure2. Flowchart of proposed system

V.IMPLEMENTATION DETAILS

A. ALGORITHM

1.Viola Jones Algorithm

```
1. for number of scales in image uploaded do
2. downsample image by one scale
3. compute integral image for current scale
4. for each shift step of the sliding detection window do
5. for each stage in the cascade classifier do
6. for each filter in the stage do
7. filter the detection window
8. end
9. accumulate filter outputs within this stage
10. if accumulation fails to pass per-stage threshold do
11. break the for loop and reject this window as a face
12. end
13. end
14. if this detection window passes all per-stage thresholds do
15. accept this window as a face
16. else
17. reject this window as a face
18. end
19. end
```

20. end

2 Nearest Neighbor Algorithm

1. Scan all elements of X, looking for an element x whose nearest prototype from U
has a different label than x.
2. Remove x from X and add it to U
3. Repeat the scan until no more prototypes are added to U.
4. Use U instead of X for classification

B. MATHEMATICAL MODEL

1. Input: Input group photos , which contains a photo of friends who also using
same online social network
I= {I1, I2, ..., In},
Where I is set of input photos to the system.
1. Output: Candidate list with matching faces .
O= {O1, O2, ..., On},
where O is a similar matching profile pictures to input query of group photo.
2. Process:

- For each photo there have n pixels for any given co-ordinates { i,j} Pixels may be arranged in the form of column vector,

  X={ x1,x2 , …….xn }
- If size of image is M*N , there will be total MN such n-dimensional vectors. The mean vector, mx of vector population can be approximated by sample average.

  $mx=1/k * \sum_k^{k=1}$ with K=MN.
- Similarly, co-variance matrix, n*n,

  $Cx= 1/k * \sum_k^{k=1} (xk-xx)(xk-mx)^T$
- After obtaining the co-variance matrix,the eigen values λk and eigen vectors Xk are calculated from the co-variance matrix,
- Eigen values can be calculated as |C -λI| =0 where C is co-variance matrix and λ is a eigen value and,

X={ x1,x2,………xn } is an eigen vector.
- To determine face, if P and Q are two pixels with co-ordinates (x1,y1) and (x2, y2) the distance

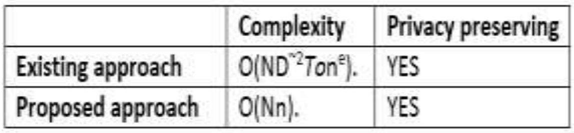
  $DE= \{x1 - x2+y1 - y2 \}^{1/2}$
- A face is classified as belonging to class k with minimum DE. Otherwise face is classified as unknown.
- Output O={Required item}

VI. RESULTS AND DISCUSSION

In this subsection, we describe the expected computational complexity of 2 approaches: existing approach and the proposed approach. The notations involved are: N is the number of nodes/users and D is the average degree of the friendship graph, n and p are parameters of training data X, denotes number of training records and the length of each record respectively.

Existing approach: If we consider the complete sub-graph in the friendship graph, then expected cost should be O(N D^2Tone). It deals with training set of p x n size. Hence computational cost is O(To(n^e + n^2p))= O(nToe). There are local training problems to find D classifiers for one neighborhood. So total cost of N neighborhoods O(ND ^{2} Tone).

Proposed approach: Has a centralized FR engine in charge of recognizing all users over a large OSN. Hence the total cost is O(Nn). Where N is number of users in friends list in system and n is number of co-owners detected in the photo being uploaded.



	Complexity	Privacy preserving
Existing approach	O(ND^{-2}*Ton*^{e}).	YES
Proposed approach	O(Nn).	YES

Figure3. Complexity analysis

A. Scalability Analysis

To make the proposed system design scalable, we need to consider the following cases, We need to boost the facial recognition algorithm by eliminating the irrelevant haar features. We need to make sure we are giving some provision to increase the facial recognition performance by the use of initiating multiple threads instead of matching the faces sequentially, as this approach is time-consuming and user experience will not be good. If the users social circle is going to be changed then FR should also be modified accordingly.

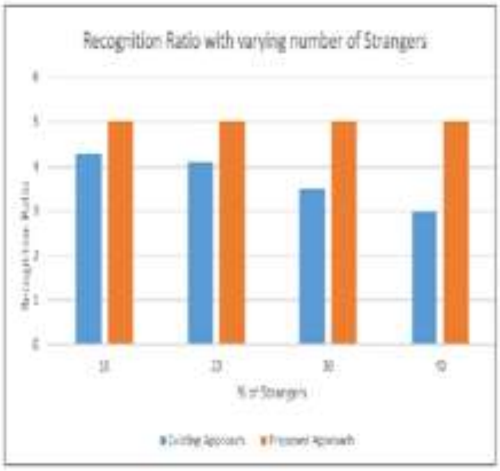


Figure4. Recognition Ratio

B. Stranger Analysis

In our system, if the people are not friends of each other and if they want to share the photo of each-other, it would not be possible. It is added as one of the privacy constraint. As if you do not know the person, you are not allowed to post his photo online. So there are no chances of having the photos of strangers in the shared photos. In the existing system, they have given the provision of the stranger classification which brings trivial extra storage cost and the consumption cost. Here when a stranger is detected in the picture it is kept aside without processing it further.

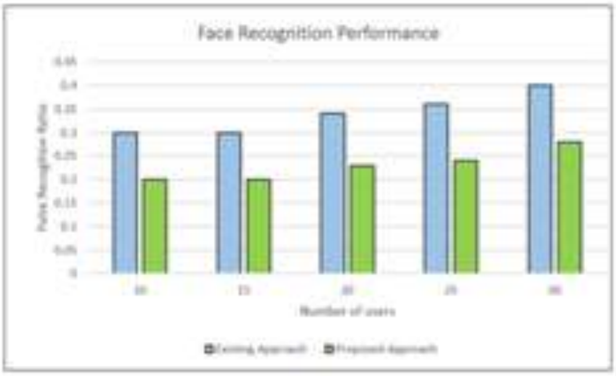


Figure5. Face Recognition Performance

C.Face Recognition performance

We study the recognition ratio against the number of friends and the number of strangers. Standard face recognition is used for face detection and the eigenface detection method is used. Another criteria to measure the performance is the false positive rate. A false positive recognition will reveal the test image to the wrong person. Thus, low false positive rate is desirable. We observe that false positive rate is lower in our scheme than the existing scheme.

VII. CONCLUSION

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.

ACKNOWLEDGMENT

I would like to take this opportunity to express my gratitude to my guide Prof. Prajakta A.Satarkar for providing all resources and great platform to accomplish my target. I also express my special thanks to my friends for supporting me in my research work.

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] I. 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: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734-1744. Springer Berlin Heidelberg, 2006.