

A Survey Paper on Photo Sharing and Privacy Control Decisions

Divyalaxmi R. Nampalli
MEStudent
Department of Computer Engineering
RMDSOE, Warje
Pune, India
divya.nampalli@gmail.com

Prof. Trupti Dange.
Assistant Professor
Department of Computer Engineering
RMDSOE, Warje
Pune, India
trupti.dange@gmail.com

Abstract: Photo sharing is an alluring component which enhances Online Social Networks. Sadly, it may release clients' security on the off chance that they are permitted to post, remark, and label a photograph openly. We study the situation when a client shares a photograph containing people other than her (termed co-photograph for short). We need to minimize the security breaches that happen because posting the photos of people without the awareness of people involved in photo. For this reason, we require a proficient facial acknowledgment (FR) framework that can perceive everybody in the photograph. Notwithstanding, all the more requesting security setting may restrain the photographs' quantity freely accessible to prepare the FR framework. To manage this issue, our instrument endeavors to use clients' private photographs to plan a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their protection. We additionally add to a disseminated records based system to diminish the computational many-sided quality and ensure the private preparing set. We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and effectiveness. Our instrument is executed as a proof of idea Android application on Facebook's stage. OSNs will not contaminate to true users and polluted by unauthorized users and their posting the photos in insecure way. Hence OSNs will be secure and safest.

Keywords: Photo Privacy, Social networks, secure multi-party computation, collaborative learning.

I. INTRODUCTION

Social sites have become important part of our daily life. Online social networks (OSNs) such as Facebook, Google and Sound of Birds are inherently designed to make able people to part personal and public information and make social connections with friends, coworkers, persons having like-position, family, and even with strangers. To keep safe (out of danger) user facts, way in control has become a chief thing point of OSNs. However it becomes everlasting record once some photo/image is posted/uploaded. Late consequences can be dangerous, people may use it for different unexpected purposes. For example a posted may reveal the mafia relationship of any celebrity.

A user profile usually includes information with respect to the users work history birthday, sex, residence, interests, education, and, travel information and be in touch information. Moreover, users upload the picture and tag other people even though they are willing or not willing to be part of uploaded image/content.

When other people are tagged the situation becomes more complicated. The user uploading the image is totally unaware of the consequences that arise for the person which is involved in tagging or image. Currently nobody can stop such unavoidable situation. We need to have a control

over such actions to minimize the risks of photos being tagged or uploaded. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things more.

Most of the times user is unwilling to get tagged or being exposed without his permission. Is it violation if we share picture without taking a permission from all the people involved in picture? To answer this we need to explain the privacy and security issues over the social sites.

Whenever a photograph is shared it includes everybody's security, which can be put on risk if the proper permissions are not sought. We need to enforce maximum level of privacy and security of the content being uploaded on social sites. So while using the online social networks one can feel desired level of confidence and security. He/she can confidently make use of social sites without worrying or photos being shared in insecure and unauthorized way. Desired level of privacy and security is a first important thing for a user using online social sites.

With respect to current architecture and implementations of social sites, either user will alone because highly imposed security constraints else will be impacted by several security threats because of low security mechanisms. Few authors studied about the security

challenges because of lack of joint or collaborative control over the images being shared across the online social sites.

To minimize this or to completely avoid this they have suggested social sites like Facebook, Instagram to make use of multi-party privacy model to increase privacy. There should be mutual acceptable policy to grant access for a photo when multiple user are involved. For security user might need to create a group where they can grant access for their uploaded images. Exposure policy can be defined as the group of users where an image can be accessed when particular user is involved and the privacy policy can be stated as the group of users/friends who can have a direct access of the uploaded images. These two policies are used to define the overall audience or group of users/friends who can be given access to uploaded image. But before establishing this there should be a proper process of defining these groups. For this the facial recognitions are used. Most of the times the people found in the co-photo are close friends. So face recognitions engines are trained for identifying the friends in social circle. FR engines with more accuracy rates require large number of test data/samples specific to a person but most of the times it is not possible.

Users who care about the privacy and security mostly restrict themselves from uploading the photos but if these people are provided with proper privacy preserving techniques then they can post photos without any reluctance.

We are designing a privacy enhancing system of photo sharing which makes use of collaborative training system. We are enabling the users of social site to have own personal FR engine based on social relations which will make use of images stored in their personal system. It will help to build a social relationship tree, which can be used for policies for sharing of data. We make use of cryptographic techniques are well to build such training data.

We need to propose a secure approach to gain efficiency and privacy both. The user is trained first from his local training set, means set of photos in her gallery. Exposure policies are defined to have access on photo. And then by global knowledge of relationships the photo sharing can be initiated. Finally data will be distributed to the right people who have access.

Efficiency and privacy can be achieved by simultaneously comparing the current and previous experiments.

1. The users in a shared photo are automatically detected without being tagged by somebody.
2. We propose a secure sharing of private photos by making use of social context to have personal FR Engines.
3. We can achieve privacy, security and efficiency.

II. BACKGROUND AND RELATED WORK

1) A Paper on "On the Move to Meaningful Internet Systems"

AUTHORS: M B. Carminati, E. Ferrari, and A. Perego.

The degree of edibility of workflow management systems heavily influences the way business processes are executed. Constraint-based representations are deliberated to be more flexible than traditional models because of their semantics: everything that does not violate constraints is permissible. Though constraint-based representations are elastic, changes to process descriptions might be desired to comply with evolving business domains and exceptional situations. Elasticity can be enlarged by run-time support for dynamic changes. Transferring instances to a new model and ad-hoc changes. Changing the process definition for one instance. Proposed a general framework for a constraint-based process modeling language and its implementation. Approach supports both ad-hoc as well as dynamic changes.

2) A Paper on "Face recognition for improved face annotation in personal photo collections shared on online social networks".

AUTHORS: M. Bellare, C. Namprempe, and G. Neven

Using face annotation for effective management of personal photos online, Proposed a novel collaborative face recognition framework enlightening the correctness of face annotation by effectively making use of many Recognition engines available in an OSN. In particular collaborative FR framework consists of two major parts, select FR engines and merge multiple FR results. The selection of FR engines aims at determining a set of customized FR engine which are suitable for knowing query for facial images belonging to a particular user. For this purpose they exploit both social network group context in social sites and social context in phone galleries. Additionally to take advantage of the availability of multiple FR results retrieved from the selected FR engines they devise two effective solutions for integration Face Recognition results adopting old fashioned techniques for merging many classifier results Experiments were conducted using around 547 thousand personal photos collected from an existing social site networks. Results prove this method gives more accuracy matched to conventional Face Recognition approaches that only make use of a single FR engine. Further demonstrated that their collaborative FR framework has a low computational cost and comes with a decentralized design.

3) A Paper on "The FERET database and evaluation procedure for face-recognition algorithms".

AUTHORS: K. Choi, H. Byun, and K.-A. Toh.

This database is a large database of facial images, divided into expansion and reprocessed parts. The development part is made available to researchers, and the reprocessed portion is for testing face recognition algorithms. The FERET assessment process was designed to: (1) allow a comparison between different algorithms, (2) identify the most important procedures, (3) examine the state of the art in recognition, (4) identify future guidelines of research, and (5) improvement of state of the art in FR.

4) A Paper on “Proceedings of the 6th international conference on Multiple Classifier Systems”

AUTHORS: K.-B. Duan and S. S. Keerthi.

Cooperative multi agent systems MAS are ones in which several agents attempt through their interaction to jointly solve tasks. Because of communications among the agents multi agent problem complexity can rise with increase agents or their behavioral superiority. Provided a broad survey of the cooperative multi agent learning literature. Past surveys of this area have largely concentrated on issues to particular subareas e.g. robotics. In this survey they attempt to draw from multi agent learning work in a spectrum of areas including RL, evolving computation, game theory, agent modeling and robotics. They found it leads to a division of the work into two categories. Applying a single learner to discover joint solutions to multi agent problems which is called as team learning or using multiple parallel learners one per agent concurrent learning. They conclude with a presentation of multi agent learning problem domains and resources.

5) A Paper on “Moving Beyond Untagging: Photo Privacy in Tagged World”

AUTHORS: Andrew Besmer & Heather Richter Lipford.
 Department of Software and Information Systems.

Photo tagging is a popular feature of many social networks. Examined privacy concerns and mechanisms for tagged images. Using a focus group, explored the needs and concerns of users, resulting in a design considerations collections for tagged photo privacy and security. Designed a privacy enhancing mechanism based on their findings, and tested it using a mixed methods approach. Results identify the social tensions that tagging generates, and the needs of privacy tools to address photo privacy management issues.

III. EXISTINGSYSTEM

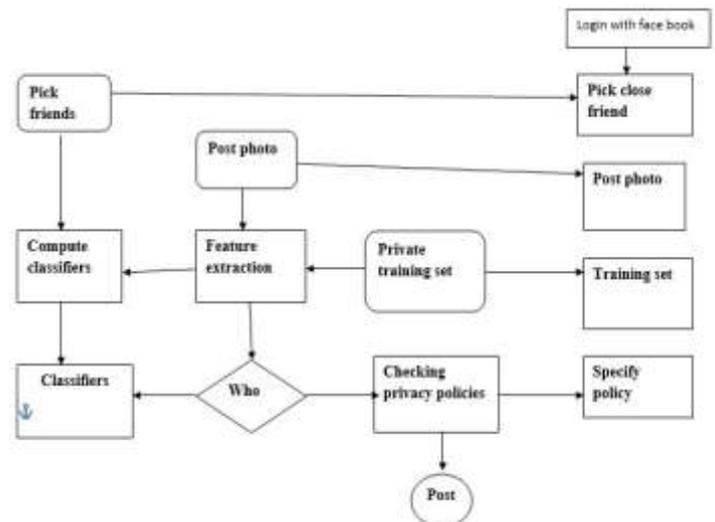


Fig.1 Existing System Architecture

Existing system consists of following three important components:

- a. Privacy Policy and Exposure Policy
- b. FR System
- c. FR with social contexts

Privacy and Exposure policy can be defined as follows. Set of users who can access the photos is called Privacy Policy. And set of users who can have access to a photo when particular user I is involved. Algorithm of Secure set intersection is used to find access policy S, means all the uses who can have access to a shared photo. After policy establishment photo can be shared with identified list of users.

FR with Social Context explained as following. Fig 1. Existing System Architecture. In Mavridis et al study the insights of photograph sharing on informal communities. He proposed domains as below:

Domain Name	Entities	Relationships
Social domain	Characters	Connection
Visual domain	Tangible Faces	Co-events in photos
Physical Domain	Bodies	Closeness

They have explained about how the different domains are interrelated. There exist a close relationship and impact between all these domains. Data given for one domain, can be used to get decent estimations in other domain.

FR System, Every user has a photo gallery in his phone, which can be used as a training data. FR system detects the faces and features of all images stored in the gallery and stores as feature vector which is private training set. With this each user will have personal own FR engine to detect

his one-hop neighbors. The personal FR can be constructed as a **multi-class classification system**, where each class is corresponding to one user. It can be built by **binary classifiers merging**.

Disadvantages of Existing System

- 1 Lots of manual work
- 2 Affected by noise

IV. PROBLEM STATEMENT

To enable sharing of pictures or images in secure manner so that privacy is maintained and there will less possibility of loss of information.

V. PROPOSED SYSTEM AND IMPLEMENTATION

We will propose to empower people conceivably in a photograph to give notifications before any photo is posted online. It will distinguish or detect the faces to people getting affected by other person who is posting the photo online. The proposed framework is highlighted with low calculation expense and classification of the preparation set. Hypothetical investigation and analyses were directed to show adequacy and proficiency. This method of photo sharing is more trustworthy and effective in maintaining the security and privacy over online social networks.

Application that is implemented was on Nexus 7 tablets, used Android Jelly Bean API, and FB SDK. They have used OpenCV library for FR. They have designed a GUI framework for this application. They have provided start stop buttons in GUI. Once user logs in greetings along with profile picture will be displayed. In the Set up the system will generate decision tree. For this purpose private training set of user is used means his photo gallery. Whenever this process of detecting the faces is going on user needs to select the close friends. From the FB survey it is identified every users has average of 150 friends and among 35 are close friends. Each of user needs to have this Application installed. In the set up mode classifiers are selected and process for creation of group where we can share the photo starts, based on privacy and exposure policy. Currently in online social applications we can't customize friends list. But here we can implement that. When a photo is posted as clicking on "Post" a notification and image will be sent to all the users who are co-owners of that photo. Co-owners have the right to accept or reject that invitation. Once that is done owner of photo can share photo, if he get the rejection he can't post the photo.

We will be using JSP and servlets for designing a social site like framework. And would be using MySQL to store images and other profile information. Image processing algorithms will be used to identify/detect the faces. We will

be using the profile images as reference. We will be following technologies to develop the application:

1. Operating system : Windows XP/7
2. Coding Language: Java
3. IDE: Eclipse
4. Database: MYSQL

Advantages of Proposed System

1. Sharing of photo efficient
2. Security of sharing photo is increased
3. Less possibility of loss of information

VI. CONCLUSION

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations for example Facebook. Lamentably imprudent photograph posting may uncover security of people. To control the security spillage we proposed to authorize people possibly in a photograph to provide alerts before anybody is posting a photo where user is involved. We planned a security safeguarding FR framework to identify people in a photograph. The proposed framework is highlighted with low calculation expense. We designed a plan be exceptionally helpful in ensuring clients' protection in photograph/picture over online sites. Moreover neighborhood Facebook Recognition preparing will deplete battery rapidly. Proposed Future work is Automatic Tagging- Whenever we are posting a photo we will get a notification of automatically tagging friends, we can opt to tag the photo or reject it.

ACKNOWLEDGMENT

I would like to acknowledge my vigorous thanks to Prof. Trupti Dange for giving her valuable suggestions. I also express my special thanks to my friends for supporting me in my research work.

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. *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] 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.

-
- [5] B Carminati E Ferrari and A Perego, Rule based access control for social networks, OTM 2006 Workshops, Science pages 1734 1744 Springer Berlin Heidelberg 2006
- [6] Kaihe Xu, Student Member, IEEE, YuanxiongGuo, Member, IEEE, LinkeGuo, Member, IEEE, Yuguang Fang, Fellow, IEEE, Xiaolin Li, Member, IEEE, My Privacy My Decision: Control of Photo Sharing on Online Social Networks. 10.1109/TDSC.2015.2443795, IEEE Transactions on Dependable and Secure Computing.