IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

A Selective Control on Access of Photo Sharing on Online Social Network

Anusha Rao[1], Sonal Fatangare[2]

ME Student, Dept. of Computer Engineering, RMD SSOE, Warje, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, RMD SSOE, Warje, Pune, India[2]

Abstract: Online social networks provides facilities such as sharing, hosting , uploading and photo management which are shared and transferred online on social network. The provision of photo sharing refers to the transfer or posting of a user's digital photos online which facilitates uploading and displaying of images by both websites and applications. It can also be used by the user to manage photo galleries and photo blogs which can make them view the photos but doesn't allow them to download the photo. If a user is permitted to post, comment and tag a photo then it may reveal user's privacy, so to solve this problem various systems has been explained that can recognize everyone in the photo. Photos are shared with a range of people with the help of online photo sharing which provides users various innovative alternatives. Many social networking sites is featured with photo sharing which assists users in posting photo to their families, friends and close ones. It ensures the safe upload of the photo and makes every individual present in the photo be aware of the posting activity and as well make them actively take part in the activity of photo posting. This system considers the needs of the users and focuses on the privacy concerns, as well as user's current behavior and concerns are taken into consideration for the protection of privacy of individuals.

Keywords: Online Social Network, Privacy, Sharing, FR System

I. INTRODUCTION

The massive use of social networking sites and with the vogue of photo sharing on social networking sites users naively tends to share personal information. Social networking users may or may not be aware of getting their personal information to be leaked or will benefit the malevolent hackers or may commit any kind of privacy breaches.

The intense popularization of Internet and the vast germination of web services that facilitates the participatory information sharing, users likely tend to share personal information which may lead to lethal causes. Social media use has become so pervasive communication media that help connect people and stay in touch beyond boundaries. It is becoming progressively more obvious that social networks have become a part of people's lives. To check status updates from the family and friends, tablet and smart phone are used by the young generation. Young people are becoming more socially capable due to social networking sites.

With the adoration of sharing, Facebook has stood out as the most famous SNSs in the world where people expend time for hours. Some people on internet sites carry out dreadful acts and screen themselves behind the secrecy provided by the internet. Young people being unaware of reading the privacy policy of different websites, most of the times unknowingly reveal their personal information. If the young people fail to read the policies then it may cause risk of disclosing individual's personal information which is a cyber crime such as an identity theft.

Facebook has helped a lot to create lots of different source of entertainment and informational media for personal as well as business use around the globe. It is also available in various languages and country thus involving people from all over the globe and connecting people of various dialects together as it provides translation feature. 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 thin which should be controlled is the availability of the personal information which should be prevented d from leakage as it may reveal personal information of an individual in the form of videos, images or any data. So the information should be precise else it may lose control on the information once it is let out on internet.

Facebook has provided an ease of uploading and sharing photos online in an instant. If the individual is not identified by the photo tags, then the face of an individual can be identified through the use of the facial recognition software and publicly available information which identifies the person on the photo. Since the social networking sites provides us the ease and fulfills our needs they have become the integral part of our life who provides social needs such as information sharing, social interaction and communication. Because of such an ease more people are reliable on online social network where they place their images, personal information and videos without giving a second thought. These records placed on social sites can be used for malicious purpose as it becomes a permanent record. For example, any photo posted on the site may lead a connection to some mafia world which may cause threat to someone. Privacy

DOI 10.17148/IJARCCE.2016.56171

protection over OSNs has become an important issue as many users are careless while posting the contents of the photo which may cause far reaching effects.

Facebook has feature of photo tagging which is of prime concern as it makes individual involve other person by tagging individuals and make them involve in the photo posting activity. This is initiated by tagging photos of the individual who are present in the photo and thus inviting them to be active part of it. Users may even post the details or any information of the individual without their involvement and consent. The situation may be brought out due to proper tools and designs alongwith the lack of experience and awareness in users.

This paper proposes a system based on new consent, which approaches to achieve privacy and efficiency at the same time. The local train data is formed by setting individuals private photo set so as to train the data and make individual learn the local training results. Once this result is achieved then global knowledge can be formed by exchanging the data among the users thus expanding the knowledge of the users. Later, the knowledge can be expanded and can be used as reference by the users. At last the information can be shared among various users and thus consensus can be reached through it.

A. Motivation

OSN has been widely used to share information, appreciation and respect. In a media where people upload or share photos, videos or any data without giving it much thought regarding its privacy. The users are careless while posting any information over OSN that may have effect which we never expect as currently there is no restriction on sharing information or photos. Instead network service providers like Facebook initiate people to share more information or photos by providing tags and make others also get involved in it.

II. LITERATURE SURVEY

There are several systems proposed for privacy preserving of photos on online social network. These systems preserve the privacy of the photo.

In 2008, Z. Stone, T. Zickler, and T. Darrell [2], described that the sensitive and private user attributes can be revealed by the act of tagging pictures on the social-networking site of Facebook. Through Facebook lots of data is being shared which may even be private and very sensitive so a prime concern is given to user privacy. Even it is been revealed that even the date and place of birth of a profile can be used to predict the Social Security Number (SSN) of a Facebook user and additional to that much more can be revealed through users friends list.

People may be identified on the photo through sensitive information which may be embedded in the photo as metadata by accompanying much more information that could be exploited like comments, captions marked regions and photo tags. Even if through the photo tags [2], if the individual is not identified, it is possible to infer someone’s identity through the combination of face recognition software and publicly available data. So it is preferred that the users should be able to hide their tags rather than deleting it and thus keep a high degree of interaction by keeping track of the photos they have online with the album owner but the photos shouldn’t be linked directly to their profiles.

In 2008, A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang [3] , developed privacy settings based on the concept of social circles which protects personal information through a web based solution. The friend’s lists are automatically generated through Social Circles Finder that identifies the intensities of the relation by analyzing the social circle of the person which in turn helps in categorizing of friends for privacy policy setting. The social circle of the subject will be identified by the application but won’t be revealed to the subject. The subject’s interest of sharing the information will be considered by interrogating the subject and based on that the piece of personal information will be shared in the form of visual graphs.

In 2009, J. Bonneau, J. Anderson, and L. Church explains privacy suites [4] which allows users to easily choose “suites" of privacy settings that can be created by an expert using privacy programming or can be created through exporting them to the abstract format or through existing configuration UIs. A Privacy suite can be verified by a good practice, a high level language and motivated users which then can be then distributed to the members of the social sites through existing distribution channels.

In 2009, JaeYoung Choi’, Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis [5], made use of available multiple and distributed database and also FR engine on OSN to improve accuracy of face annotation. This system utilized the real-world personal photos which were available on web and the standard MPEG-7VCE-3 data set to form a collaborative FR method [5] which improved the accuracy of face annotation by considering the annotation results obtained from individual FR engines. Social relationship among community members and social context in personal photographs are used to form FR databases and engines to annotate faces in a collaborative way rather than considering individual FR on which fusion techniques are applied to combine results from multiple FR engine and give a single result. The collaborative system thus used the face annotation method to improve the accuracy of the system which was done through the set of database.

In 2011, Alessandra Mazzia Kristen LeFevre and Eytan Adar [10], explains how users apply privacy policies to their networks. It [10] is an interface and system that allows the user to recognize its profile based on different factors such as natural sub-groupings of friends that is build up at different stages of granularity. The automatically constructed group can be automatically recognized and distinguished with the help of group labels. This tool is better than other tools like Facebook's Audience View and Custom Settings page.

In 2012, Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova developed a technique [11] which enables privacy-oriented image search for automatically detecting private images. The security policies are

DOI 10.17148/IJARCCE.2016.56171

provided by combination of textual metadata images with variety of visual features. In this the selected image features (edges, faces, color histograms) which can help distinguish between natural and man-made objects/scenes can be done through image features like edges, faces or color histogram through which the presence or absence of object can be determined. The classification models which are trained on large scale dataset are utilized in which social annotation game is used to obtain privacy assignments.

In 2012, Sergej Zerr developed a technique [12] which enables privacy-oriented image search for automatically detecting private images. The security policies are provided by combination of textual metadata images with variety of visual features. In this the selected image features (edges, faces, color histograms) which can help the distinguish between natural and man-made objects/scenes can be done through image features like edges, faces or color histogram through which the presence or absence of object can be determined. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

In 2015, Anna Cinzia Squicciarini represented A3P system [14] which automatically generates personalized policies as it is a free privacy settings system. Based on the images content, person's personal characteristics and metadata, the user uploaded image can be handled by A3P system. It consists of two components: A3P Core and A3P Social. The A3P core receives the image uploaded by the user, which it classifies and decides whether there is a need to call upon the A3P-social. If the metadata is unavailable or if it is created manually then it may cause inaccurate classification, violation policy and even may cause inaccurate privacy policy generation.

III. PROPOSED SYSTEM

A. Problem Statement

To propose a facial recognition system for preserving privacy of photo sharing that can recognize everyone in the photo which enables each person in a photo be alert of the posting action and participate in the decision making while posting the photo.

B. System Architecture

A mechanism has been designed to make users aware of the posting activity and make them actively take part in the photo posting and decision making paradigm for which a facial recognition (FR) system is recommended which can recognize everyone present in the photo. If more privacy setting is done then it may limit the number of photos which will be utilized as the training set for FR system. In order to overcome this problem and for training set for FR system we would utilize the private photos of users which would differentiate the photo co-owners without affecting their privacy. A distributed consensus based method is developed which would protect the private training set and even reduce the computational complexity.

Our contributions to this work when compared with previous work are mentioned below:

- We can find the potential owners of shared photos automatically even when the use of generated tags is kept as an option in our paper.
- Private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user is proposed in our paper.
- We propose a consensus-based method to achieve privacy and efficiency.

The figure below shows the system structure of the FR system.

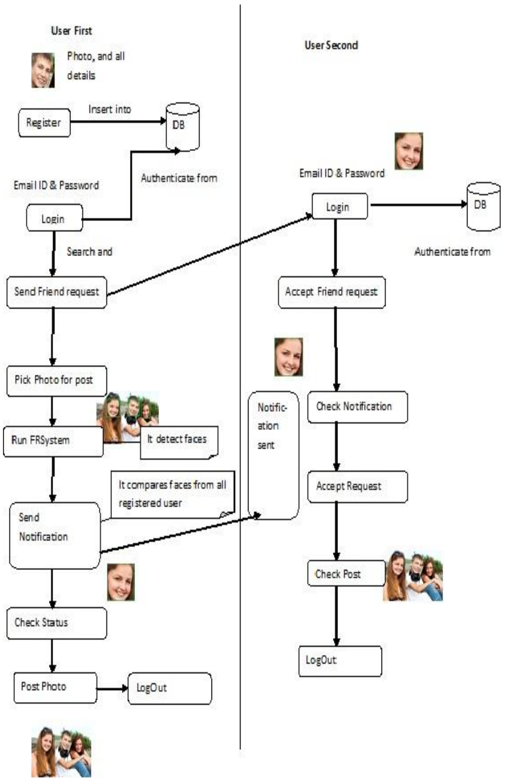

Fig 1: System architecture of FR system

IV. FACIAL RECOGNITION SYSTEM

A privacy-preserving FR system is used to identify individuals in a co-photo. The owners present in the shared photos can be automatically recognized and identified with or without user-generated tags. The FR engine is derived from the private photos and social contexts. The privacy is protected by providing users facility to restrict others from seeing their photos. Each user is able to define his/her policy which are privacy policy and exposure policy. Computation cost is very low. FR system provides privacy by notifying the subject about the posting activity and thus leading the other subjects to take active part in it.

To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual present in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, an efficient facial recognition (FR) system is needed which recognizes everyone in the photo. However, if more privacy settings is done then it may bound the number of photos necessary to train the FR system. So in order to solve this problem, private photos of users is utilized to train the FR system and thus prevent the leakage of the privacy of the individuals.

V. IMPLEMENTATION STRATEGY

Technique and algorithm used for implementation of the proposed system are given. It consists of following modules.

- Friend request
- Picking close friends
- Sharing photo
- Face Detection and Feature extraction
- Check policy status
- Post or block

User must enter the user-id and password to Log In to the website. After successful login user will pick friends. Individual human identification will take place that is it will compute classifications of photos and store the data over cloud. Then it will check the privacy policy for which it is required to specify policy. Once the privacy policy is set then it performs the process of photo matching. If photo owner grants the permission then the photo will be posted and if not then the photo will be blocked.

Friend Request:
A log in/out button could be used for log in/out with the social website. After logging in, a greeting message and the profile picture will be shown. This prototype works in three modes: a setup mode, a sleeping mode and a working mode. After receiving the friend request user can accept anyone of them. A list will be available out of which we can choose anyone whom we want to send the friend request. The request will be available to the receiver and he can either accept the friend request or deny it as per the user's interest. The search tab is provided to search a new friend from the list of people available and then request can be sent that particular person.

Picking Close Friends:
A user needs to manually specify the set of "close friends" from their friend list on social website and form the neighborhood by clicking the button "Pick friends". In this application, each user picks up to 10 "close friends". The individuals from the friend list should have application installed in their system to carry out the collaborative training. The setup mode could be activated by pressing the button "Start".

Sharing Photo:
User 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. Currently, when the button "Post Photo" is pressed, co-owners of x are identified, and then notifications along with x are sent 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.

Generate OTP:
When new user is registered and then login to his\her account then random OTP is generated to verify the user, secure the privacy of individuals and prevent it from unauthorized user accessing the account. Similarly OTP is generated when the owner uploads a photo to make sure that the concerned authorized person is posting the photo.

Face Detection and Face Recognition:
Face detection is based upon the training of a classifier using number of positive images that represent the object to be recognized and even large number of negative images that represent objects or feature not to be detected. The photo x is provided in which I faces are detected. This technique can be adapted to accurately detect facial features. The area of the image is regionalized containing the highest probability of the feature so as to analyze the facial feature. By doing this, the speed of the detection is increased as it eliminates the false positive which reduces the area to be examined.

Local Binary Patterns is used for person-independent face recognition. The face area is first divided into small regions from which Local Binary Patterns (LBP), histograms are extracted and concatenated into a single feature vector. This feature vector forms an efficient representation of the face and is used to measure similarities between images. It is used to summarize the local structure in an image by comparing each pixel with its neighborhood. Take a pixel as center and threshold its neighbors against. If the intensity of the center pixel is greater-equal its neighbor, then denote it with 1 and 0 if not. Better facial feature extraction method can be applied to our system to obtain a better recognition ratio.
Local Binary Pattern algorithm:
Input: Training Image set.

Output: Feature extracted from face image and compared with centre pixel and recognition with unknown face image.

```
1. Initialize temp = 0
2. FOR each image I in the training image set
3. Initialize the pattern histogram, H = 0
4. FOR each center pixel tc ϵ I
5. Compute the pattern label of tc
6. Increase the corresponding bin by 1.
7. END FOR
8. Find the highest LBP feature for each face image and combined into single vector.
9. Compare with test face image.
10. If it matches it most similar face in database then successfully recognized
```

Check Policy Status:
The privacy policy status is set for individual users. The policy should satisfy both the privacy policy and the exposure policy of the individuals.

DOI 10.17148/IJARCCE.2016.56171

Post or Block:
If the policy is satisfied then the notification is sent to the co-owner. The photo is posted once the owner gives permission to upload it else it is not uploaded. Each time the photo is uploaded OTP is generated and notification is sent to every co-owner, with whose acceptance later photo is posted on their page.

VI. DISCUSSION

The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. Preserving user privacy and making them actively participate in the photo posting activity is a very prime concern in OSNs. The co-photo can be posted only with the permission of the co-owner and if the privacy and exposure policy gets satisfies.

To make the system more secured the notification is sent to the co-owner and only with his/her acceptance the photo is posted. In addition random OTP is generated while uploading photo to verify the user who is posting it as someone may access his\her account to upload photos which are in actual not to be posted by the concerned account holder.

VII. CONCLUSION

Photo sharing is the process of publishing or transfer of a user's digital photos online. Individuals in a co-photo are identified by the proposed FR system. The system reveals the detailed description of our system. Generally speaking, the consensus result could be achieved by iteratively refining the local training result. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately). These functions provided by websites and applications facilitate the upload and display of images.

The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. The system that is built has proven that how to build a general personal FR with more than two users. The system can reduce the privacy leakage by using this design as it provides intimation to the co-owners and even to the owners through random OTP generation.

ACKNOWLEDGMENT

I take this opportunity to express my heartfelt gratitude to my guide **Prof. Jyoti Raghatwan** and head of department **Prof. Vina M. Lomte**, Department of Computer Engineering, RMD SSOE, Savitribai Phule Pune University, for their kind co-operation and capable guidance during the entire work. I would also like to thank our Principal and Management for providing lab and other facilities.

REFERENCES

[1] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, Xiaolin Li, ”My Privacy My Decision: Control of Photo Sharing on Online Social Networks”, IEEE Transaction on Dependable and Secure Computing, Volume: PP , Issue: 99, pp-1-1, 2015
[2] Z. Stone, T. Zickler, and T. Darrell, “Autotagging facebook: Social network context improves photo annotation”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-8, 2008.
[3] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, “Social circles: Tackling privacy in social networks”, in Proc. Sympsable Privacy Security, 2008.
[4] J. Bonneau, J. Anderson, and L. Church, “Privacy suites: Shared privacy for social networks”, in Proc. Symp. Usable Privacy Security, 2009.
[5] JaeYoung Choi', Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis, ”Face Annotation for Personal Photos Using Collaborative Face Recognition in Online Social Networks”, 16th International Conference on Digital Signal processing, pp.1-8, 2009.
[6] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, “Providing access control to online photo albums based on tags and linked data”, pp. 9–14, 2009.
[7] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, “Providing access control to online photo albums based on tags and linked data”, pp. 9–14, 2009.
[8] 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, pp. 1563–1572, 2010.
[9] Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham, ”Semantic web-based social network access control”, pp. 108-115, 2011.
[10] Alessandra Mazzia Kristen LeFevre and Eytan Adar, “The PViz Comprehension Tool for Social Network Privacy Settings”, Tech. rep., University of Michigan, 2011.
[11] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , “I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search “, Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.
[12] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , “I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search “, Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.
[13] Kambiz Ghazinour, Stan Matwin and Marina Sokolova, “Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.
[14] Anna Cinzia Squicciarini, “Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites”, IEEE Transactions on Knowledge And Data Engineering, Vol. 27, no. 1, January 2015.

BIOGRAPHIES

Anusha P. Rao is a Master of Engineering student in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received Bachelor of Engineering degree in 2012 from DPCOE, Wagholi, Pune. Her research interests are Image Processing, Data Mining, Network security etc.

Sonal Fatangare is an Assistant Professor in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received Master of Engineering degree in 2014 from JSPM, BSIOTR, Wagholi, Pune. Her research interests are Data Mining and Network security.

DOI 10.17148/IJARCCE.2016.56171