Secured Group Photo Uploading on Online Social Networks

Sahla Nazlin A[1], Vishnu K[2]

[1]AP J Abdul Kalam Technological University, M-Tech Student, Department of Computer Science and Engineering, Cochin College of Engineering and Technology, Valanchery, Kerala, India
[2]AP J Abdul Kalam Technological University, Assistant Professor, Department of Computer Science and Engineering, Cochin College of Engineering and Technology, Valanchery, Kerala, India

Abstract: ***Online Social Networks (ONS) have become an important part of our everyday life. Photograph sharing is one of the most significant features of Online Social Networks, unluckily which may be used for purposes we not at all imagine. To check possible confidentiality outflow of a group photo, we design a mechanism in which each human being can take part in the decision making on the photograph posting. To do this we need a professional facial recognition (FR) system that cans recognize everyone in the photo. We are using Open CV face detection and CBIR (content based image retrieval) algorithm to train individual's images and for face recognition. To get enough training sample is actually little difficult task, so FR engine may be unsuccessful to identify the faces of each individual in a group photo. To avoid this we are using an efficient CBIR algorithm. Once the faces are identified from the group photo then acceptance notifications are sending automatically to each identified persons within the close friend circle. The photo will be posted if all the people within the friend circle are accepting the notification; the photo will not be posted if any one of them rejects the notification. We expect that our proposed scheme would be very useful in protecting users' privacy in photo/image sharing over online social networks.***

Keywords: Online Social Network, CBIR, K-Mean Clustering, Face Recognition.

1. Introduction

OSNS have become essential element of our everyday life and has strongly changed the way we interrelate with each other, the needs for social connections, information distribution, appreciation and admiration. At present people are adding more photos without thinking the content of the photo much. However, once something, such as a photo, is posted online, it becomes an everlasting proof, which may be used for purposes we not at all imagine. For example, a posted photo in a party may disclose a relationship of a famous person to a mafiaworld. Because OSN users may be not careful in posting content while the effect is so far-reaching, privacy protection over OSNs becomes a significant issue. The things become more difficult when it is added much functions like photo uploading and tagging. For instance, these days we can contribute to any picture as we like on OSNs, in spite of whether this photograph contains other populace (is a co-photo) or not[1].

At present there is no constraint with sharing of co-photos, on the contrary, social network service providers like Facebook are heartening users to post co-photos and tag their associates in order to get more people involved. However, what if the co-owners of a photograph are not ready to contribute to this photo? Is it a confidentiality violation to distribute this co-photo without authorization of the co-owners? Should the co-owners have some control over the co-photos? .To answer these questions, we need to study the privacy issues over OSNs. The system can solves the subject of posting group photos on a social network by sending a notification to co photo owners regarding their presence. If the entire co-photo owner then the s are accepting the notification, the group photo will be uploaded otherwise the photo will be rejected. We assume that each user u has a privacy policy Pu(i) and an exposure policy Vu(i) for a specific photo i. The privacy policy Pu(i) indicates the set of users who can access photo x and exposure policy Vu(i) indicates the set of users who can access i when user u is involved. If the photo co-owner is not login to the social network he or she is unable to see the notification and the group photo cannot be uploaded for long. To solve this issue it is possible to set a time limit, for example 2 days or 3days.If it is set 3 days time limit after that photo will be uploaded automatically. More over for the photo co-owners safety it is possible to send SMS regarding the photo uploading and time limit, so they can login and either accept or reject the notification, so this time limit setting and SMS notification can be do it as future enhancement . To do all of this we need a good FR system. This system is using CBIR (content based image retrieval) algorithm with K-mean clustering for training images and face recognition. [4].

2. Literature Review

Social-networking users unsuspectingly disclose confident kinds of private information that malicious attackers could takings from to perpetrate important isolation breaches. This paper quantitatively explain how the easy act of tagging pictures on the social networking site of Face book could reveal private customer's privacy that are awfully sensitive. Our outcome put forward that photograph tags can be used to help out predict several, but not all, of the analyzed attributes. We consider our analysis make users to alert importance of their confidentiality and could notify the design of new privacy-preserving method of tagging photograph on social-networking sites.

Photo tagging is a well-liked feature of numerous social network sites that allows users to make notes on uploaded photograph with how many are in them, openly connecting the photograph to each individual's profile. In this document,

it is inspected confidentiality concerns and mechanisms regarding this tagged photograph... Using a focal point of group, we explored the requirements and concerns of users, follow-on in a set of design considerations for tagged photograph confidentiality. Now face book added the new security to prevent the privacy leakage issue due to photo tagging, people can set review the tag before appearing the time line option .but still people can share the photo .it is not preventing co-photo owner's privacy. [2]

Algorithm for face recognition can be divided into mainly two functional modules: first is a Face image detector which finds the human faces from a normal photograph against easy or compound background, and second is face recognizer determines identity of the person. Both the face recognizer and face detector follow the same framework; both of them have a feature extractor that can transforms the pixels of the facial image into a valuable representation of vectors, and the function of pattern recognizer is do searches on the database to get the best match with the incoming face image. [3].

Objects shared through Social Media will be affected more than one user's confidentiality .Social Media infrastructures cannot allow users to understand actually these items are actually shared or not. Multiple users' confidentiality preferences are not an easy mission, because confidentiality preferences may disagreement, so methods to resolve conflicts are required. In this paper, it is explained the primary computational mechanism to determine conflicts for multi-party confidentiality organization in Social Media that is able to adapt to disparate situations by modeling the concessions that users make to reach a explanation to the conflicts. Here user can decide how many want to give the access permission to share the group photo. User can set a high and low priority option , who is under high priority those are allow to access and share the group photo but still it is not preserving the co-photo owners privacy[1],[4].

Content Based Image Retrieval (CBIR) is a great tool. Visual cues are used to search images databases and retrieve the required images in CBIR. In CBIR many approaches and techniques are used for this. For indexing and representation of the image contents the visual contents of images, like texture [6]-[8], color [5], shape [6] and region [7], are broadly explored these low level features of an image are directly related to the contents of the image. These image contents can be extracting from image and is used for measuring the comparison amid the queried image and images in the database using different statistical methods. In content-based retrieval systems diverse features of an image query are used to search for analogous images features in the database [8].

3. System Overview

As shown in figure 1: A user can login to the system and can upload a group photo using post photo option. The various steps are given below.

3.1 System Architecture

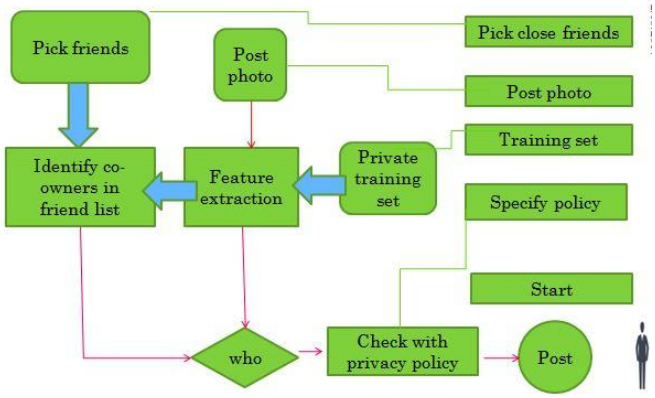

Figure 1: System architecture

3.1.1Start

User can register to Online Social Network by entering the details like name, DOB, gender, Email, mobile number, username, password etc. Once registered successfully user can login to his/her account.

3.1.2 Setting security policy

We assume that each user u has a privacy policy Pu(i) and a exposure policy Vu(i) for a specific photo i. The privacy policy Pu(i) indicates the set of users who can access photo i and exposure policy Vu(i) indicates the set of users who can access x when user u is involved. According to our scheme, this friend list should be intersection of owner's privacy policy and co-photo owners' exposure policies. At present, when the push button "Post Photo" is pressed, co-owners of i are identified, and then notifications along with i are sending to the co-owners to request permissions. If they all agree to post i, i 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 depends the set of users who can access x when user u is involved.

3.1.3 Training

A log in/out button could be used for log in/out with our social network site. After login in, the profile picture will be shown. , we need an efficient content based image retrieval facial recognition (FR) system that can used to train users images. We are using Open CV face detection and CBIR algorithm to train individual's images and for face recognition. FR engine could be trained to recognize social friends (people in social circle) but to get enough training sample is a difficult task. FR engine with advanced recognition ratio demands more training samples

3.1.4 Pick friend

User can search through this social networking site to get friends ,there is an invite friend option is there to find friends, user needs to set "close friends" among their Social Network friends either by sending friend request or accepting others friend request. When a person try to upload a group photo,

FR system identify all co-photo owners from this close friends group.

3.1.5 Photo Uploading

Once a user is logging in to his/her account, he/she can use the photo posting feature of OSN. When posting a group photos on online social network an automatic acceptance notification is sending to the co photo owners informing their presence in that group photo, so each co-photo owners are getting the chance to view the photo where they are in before the up loader post the photo and any one of them press reject button nobody can upload that photo, if all are pressing acceptance button, then only the photo will be posted. It is to prevent possible privacy leakage of a photo, this mechanism is enabled each person in a photograph be aware of the posting the photograph and actively participate in the decision making on the photograph posting.

3.1.6 Algorithm

Input: Query image.
Output: Most similar image to the input image.
Procedure:

{

Step 1: The input image.
Step 2: Extract the feature vector for the input image by calculating image features.
Step 3: Calculate the weighted features vectors for the input Image.
Step 4: Calculate the distance between the input image and the centroid of each K-mean cluster and find the smallest distance.
Step 5: Calculate the distance between the input image and the images in the cluster that has the smallest distance with the input image.
Step6: .Retrieve the image that is more similar to the input Image.

}

4. Conclusion

Photo giving out is one of the most well-liked features in online social networks such as Facebook. Lamentably, imprudent photograph posting may uncover security of people in a posted photograph. To control the security spillage, we anticipated 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. Hypothetical examination and trials were directed to show adequacy and effectiveness of the proposed plan. We expect that our proposed plan be exceptionally helpful in ensuring clients' protection in photograph/picture sharing over online informal organizations. For instance, in our application, the co-photograph must be post with consent of all the co-proprietors. Idleness presented in this procedure will enormously affect client experience of OSNs. Moreover, neighborhood FR preparing will deplete battery rapidly. Our future work could be the way to move the proposed preparing plans to individual mists like Drop box and/or icloud.

References

[1] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang,-and Xiaolin Li" My Privacy M Decision: Control of Photo Sharing on Online Social Networks". IEEE Transactions on Dependable and Secure Computing Volume: PP, Year: 2015.
[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, pages1563–1572, New York,NY USA, 2010. ACM..
[3] 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.
[4] S. D. P.W. Huang, "Image retrieval by texture similarity," Pattern Recognition, vol. 36, p. 665- 679, 2003.
[5] Y. C. C.H. Lin, R.T. Chen, "A smart content-based image retrieval system based on color and texture feature," Image Vis. Comput., vol.27 (6), p. 658-665., 2009.
[6] A.-W. R.C. Gonzalez, R.E. Woods, Digital Image Processing. Reading, MA, 1992.
[7] K.-K. M. Ju Han, "Rotation-invariant and scale-invariant gabor features for texture image retrieval," Image and Vision Computing, vol. 25, p.14741481, 2007.
[8] B. C. M. Kokare, P.K. Biswas, "Texture image retrieval using rotated wavelet filters," Pattern Recognition Letters, vol. 28, p. 1240-1249, 2007. [9] A. J. K. Iqbal,M O. Odetayo, "Content-based image retrieval approach for biometric security using colour, texture and shape features controlled by fuzzy heuristics," Journal of computer and System Sciences, vol. 78,p.12581277, 2012

Author Profile

Sahla Nazlin A received B-Tech degree in Computer Science Engineering from Government Engineering College Palakkad, Kerala, in 2008. Now doing M-Tech in Computer Science Engineering from Cochin College of Engineering and Technology Valanchery, Malappuram, Kerala, India