IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Preventing Privacy Leakage of Photo Sharing on Online Social Networks

Rekha[1*], Venkatesh Prasad[2]

[1,2]Department of Computer Science and Engineering, REVA University, Bangalore, India

Corresponding Author: rrsuryawanshi24@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.202205 | Available online at: www.ijcseonline.org

***Abstract*—** Photograph sharing is a tempting feature which popularizes online social networks. It might liberate user's secrecy if users are agreed to post, tag, comment, mention a photo publicly. In this paper we address this problem and learn the case when a user posts a photo having individuals excluding her/him. To stop the security dropout of a photo we plot a system that permit everyone in a photograph be alert about the photo uploading action and join in the judgment of photo uploading activity. To achieve this motive FR system needed which identifies individuals in the photograph. However requesting extra security can restrain the quantity of photos freely accessible to prepare the Face recognition technique. To control such problem proposed system endeavors to utilize user's personal photos for outline a individualized Face recognition system specifically made for distinct probable photo co-possessor with covering their secrecy. We evolve a distributed consensus system to minimize the computational miscellaneous and defend the personal instructing data.

Keywords—online Social networks, photo secrecy, FR system, support vector machine, collaborative learning

I. INTRODUCTION

Social networking sites have become an essential part of our lives. The nature of the social networking sites allow users to add more content like post a co-photo, tag their friends, comment to the photo etc. Once the photo is posted on social networking sites it becomes permanent record which may leak user's privacy. For example when posted a photo of a party may leak a link of a superstar to a mafia world. Nowadays people can post any photo as they like on social media without thinking this photo contain other people or not. However, imagine what if the co-proprietors of photo are not ready to post the image? Is it a protection breach when posting the co-photo with no permission of the co-proprietors? Should the co-proprietors of the photo have control on their co-photos?

To answer all these questions we should be careful about privacy issues over online social networks. Generally privacy is considered as a situation of social withdrawal as stated by Altman's privacy regulation hypothesis [4], privacy is a dialectic and dynamic circumscription regulation process in which privacy is not stable but it is "a selective control of retrieve to the oneself or to ones group". In this "dialectic" means openness and closeness oneself to others and "dynamic" means required secrecy level changes with time according to circumstances.

Our contributions when compared with previous work are as follows:

1. We can discover the potential owners of posted photos automatically with or without user- generated tags.

2. Personal photos in a privacy-preserving manner and social contexts is used to achieve a personal FR motor for any specific user.

3. We develop a consensus-based system to attain secrecy and efficiency.

II. RELATED WORK

A paper on "Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collection" by J. Y. Choi, Wesley De Neve, K. Plataniotis, Yong Man Ro.[2]. They suggest a framework in which dispersed methodology(various FR engines) is utilized to perform activities for example, subject recognizable and verification. In this paper Two problems are discoursed which are: initial one is determination of expert FR engines that can perceive inquiry face picture. And the second is the converging of various face recognition outcomes to a solitary Face recognition outcome. They uses various private Face recognition systems to work collectively to enhance the identification ratio. To choose the appropriate Face recognition motor which contain queried face picture identity with high possibility they utilizes the social contex.

"Moving Beyond Untagging : Photo Privacy in Tagged World" a paper by A. Besmer and Heather Richter Lipford[1]. They designed a framework where "confine others" apparatus is utilized for photograph security. It

services by permitting labelled clients to transmit an appeal to the proprietor inquiring that a photograph be invisible from some individuals. The labelled client is capable to place the custom authorizations at the people photograph quantity. So this apparatus advances distributing by decreasing the requirement for labelled client to limit all their labelled photographs or to untag the photo. The apparatus gives client a chance to determine people or gatherings of clients they might want to limit the photograph from.

"Buddies with faces" a paper by N. Mavridis, W. Kazmi, and P. Toulis[3]. They studied how online Social networks enrich image identification conversely. They addressed three realms model: " first, a social realm, where identities are entities, and friendship a relation; Second, a visible sensory realm, of which faces are entities, and co-appearance in pictures a relation; and third, a physical realm, in which bodies Belong, with physical proximity being a relation." They shown that the connection in physical realms and social realm are hugely correlated With visual sensory realm. So, the result is identify the people in co-photograph and face recognition system focuses on "close" buddies.

"Autotagging Facebook: Social Network Setting Improves Photo Annotation" a paper by Z. Stone, Todd Zickler, T. Darrell[7]. They proposed conditional random field system in which they used present photos of users as training data and then they merged face recognition results and co-appearance statistics to enhance the exactness of face annotation.

"Collective Privacy Management in Social Networks" a paper by A. C. Squicciarini, M. Shehab[5]. They developed a game theoretic method where the security regulation can combine to impose over the distributed data. And also individual users can specify his/her security regulation and exposure regulation.

III. SYSTEM ARCHITECTURE

Our proposed system is very helpful for securing the users secrecy when photograph posting on online social networks like Facebook because this scheme has been designed to make users or clients be aware about the photograph uploading or posting activity by sending the notification before posting on online social networks.

There are three posting policies which are public, friends and get approval. In public policy public can allow to post the photo of users, in friends policy friends of user can post the photo and in get approval policy photo is posted after getting the permission from user.

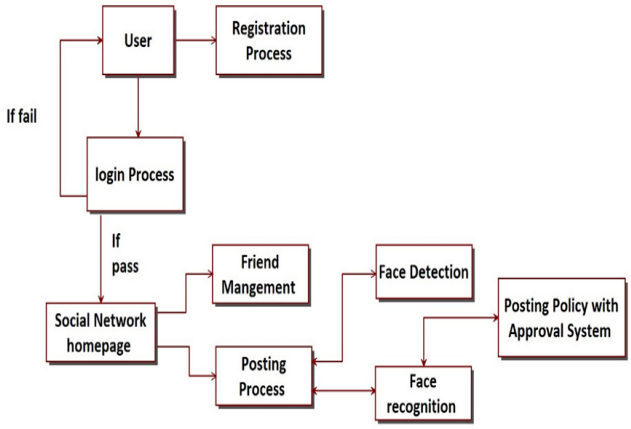

Fig. 1: System Architecture

A. Modules Description

1. User Registration process
   In the user registration process new user can register them self with personal information like name, userID, password, date of birth, gender, place and mobile number. After registration user needs to login to the social network homepage.
2. Friends(Group Management)
   In the friend management process user can send friend request to another user. If he/she accepts the friend request from the user then we are adding him/her in the friend list and they can also create the friend group.
3. Posting process
   In the posting process user can post photo of another user using this technique. If user agree to posting appeal positive marks will increase if user will refuse to posting appeal negative marks will increase based on group member choice we can decide posting activity.
4. Face detection process
   In face detection process, the openCV technology is utilize for detection of the face in the picture. openCV will study our image record to distinguish the face region. openCV likewise accompanies implemented documents for recognizing profile or frontal faces. In face discovery module from the input picture its crapping face region by using openCV.
5. Face recognition using RANSAC and SURF method
   In this module we are looking at input picture and dataset picture we are finding the number of coordinating points using SURF detection algorithm. After finding the coordinating point update in database. SURF is a re-inspecting method that produces applicant arrangements by utilizing the least number data points needed to determine the underlying model parameters. SURF chooses the minimal number of points needed to discover the model parameters. RANSAC algorithm

used to draw the matching points between the two pictures.

6. Approval method and Decision making
   After differentiate procedure we can find average coordinating points between all the dataset image. That average will achieve threshold and select grouping name and show client name.

IV. RESULTS AND DISCUSSION

Proposed scheme is very functional in securing clients secrecy in photograph posting over online social networks. The result of our framework relies upon the quantity of the training pictures. As the quantity of training pictures expands the recognition of the proprietors and co-proprietors photograph is accomplished more effectively and rapidly.
In the face recognition performance subsection we learn the recognition ratio opposed to the number of companions and the number of outsiders. Face recognition is utilized for face identification and the eigenface is utilized to remove characteristics and vectorize the instructing picture. Fig.2 is face recognition performance which shows the false positive and false negative ratios of our proposed system and existing scheme. In our proposed system we notice that false positive rate is lower than existing system.

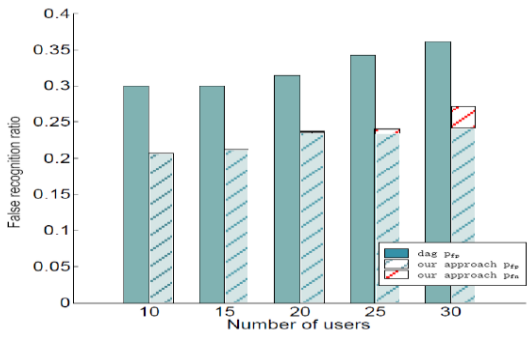

Fig. 2: Face recognition performance

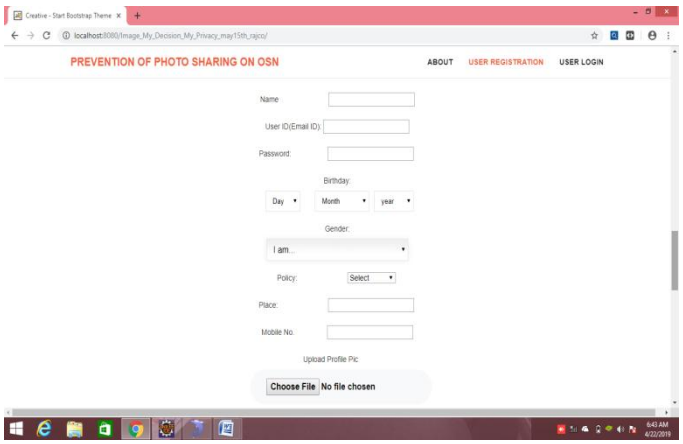

Fig. 3: Registration process

Figure3 shows registration process. Initially a new user needs to register them self with some basic information.

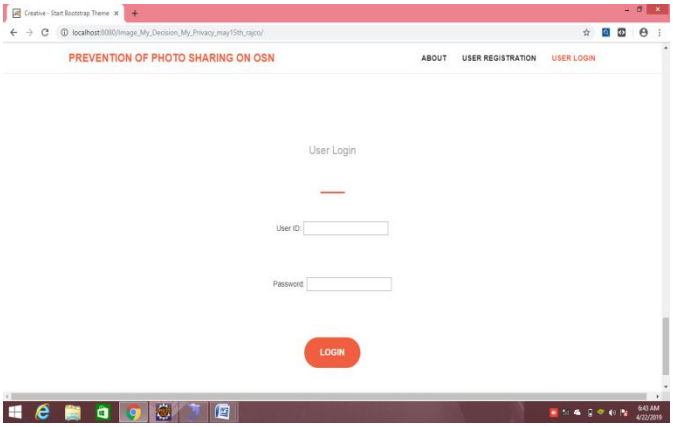

Fig. 4: User login process

Figure 4 indicates user login process. After registration process user needs to login into the system with user id and password.

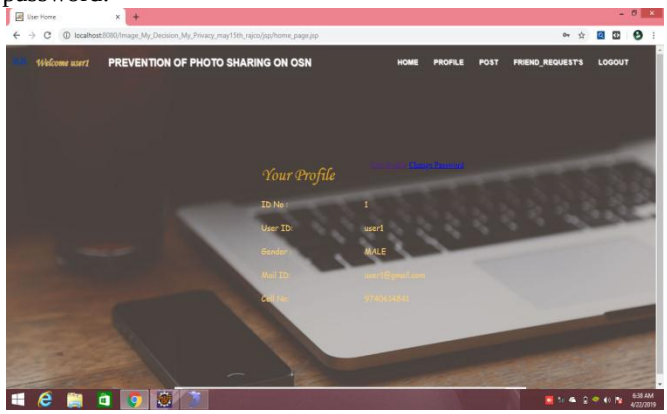

Fig. 5: Profile information

Figure 5 indicates profile information. In this section contains user information and here we can edit our profile and also we can change the password.

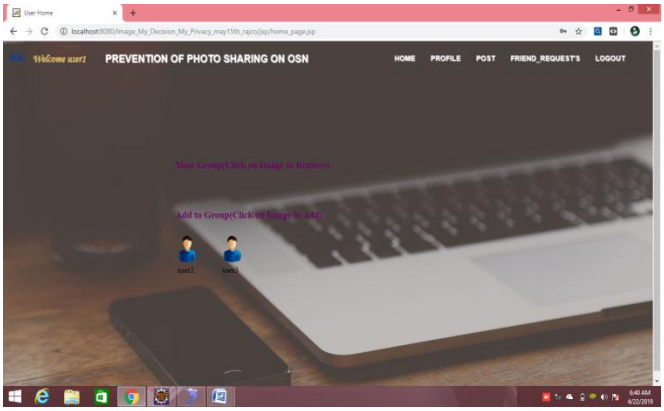

Fig. 6: Friend management process

Figure 6 shows the friend management process. In this a user can send the friend request to another users. After accepting the friend request they all will be added into the friend list of the user.

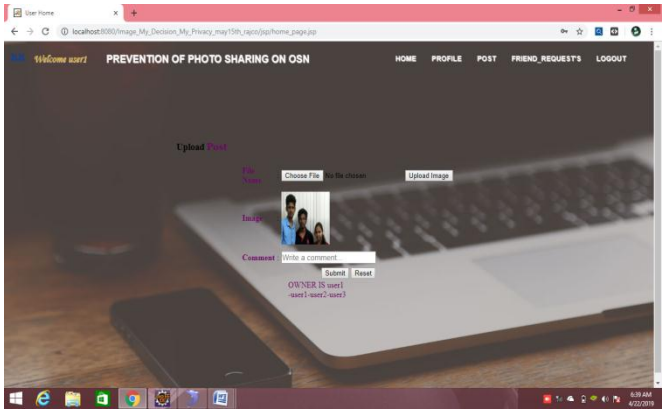

Fig. 7: Posting process

Figure 7 shows the posting process in which user can post the photos by choosing the file and user can also write the comment. In this process the owner of the shared photo can automatically identified.

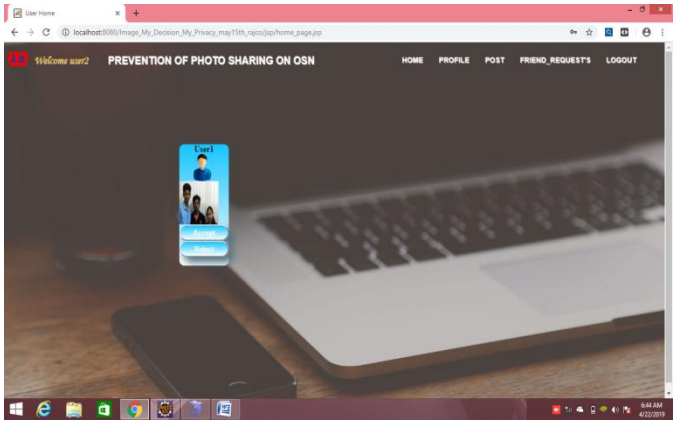

Fig. 8: Notification process

Figure 8 indicates how to get the notification of posting photo to the user when another user tries to post the photo on online social networks.

V. CONCLUSION

Photo posting on online social networks like facebook become very popular so, it may reveal the users secrecy when user permit to post the photo. To avoid this issue or to curb the protection leakage we proposed a system which allow every person in the photo to give the approval before posting a co-photo. We proposed a privacy preserving face recognition framework which is used to identify every person in a co-photo. Our proposed framework is presented with low computation cost and confidentiality of training data set. We anticipate that our proposed plot be helpful in securing users secrecy when photo posting over online social networks.

REFERENCES

[1] 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, PAGES 1563-1572, New York, NY, USA, 2010. ACM.

[2] 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 Transaction on*, 13(1):14-28, 2011.

[3] N. Mavridis, W. Kazmi, and P. Toulis. Friends with faces: How social networks can enhance face recognition and vice versa. In *Computational Social Networks Analysis*, Computer Communications and Networks, pages 453-482. Springer London, 2010.

[4] I. Altman. Privacy regulation: Culturally universal or culturally specific? *Journal of social issues*, 33(3):66-84.

[5] A. C. Squiccarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In *Proceeding of the 18th International Conference on World Wide Web*, WWW '09, pages 521-530, New York, NY, USA, 2009. ACM.

[6] Z. Stone, T. Zickler, and T. Derrell. Toward large-scale face recognition using social network context. *Proceeding of the IEEE*, 98(8):1408-1415.

[7] Z. Stone, T. Zickler, and T. Derrell. Autotagging facebook: social network context improves photo annotation. In *Computer Vision and Pattern Recognition Workshop, 2008. CVPRW'08. IEEE Computer Society Conference on*, pages 1-8. IEEE, 2008.

[8] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, Xiaolin Li. My Privacy My Decision: Control of Photo Sharing on Online Social Networks, I*EEE Transaction on Dependable and Secure Computing*, April 2017.

