

# Smart Security System for Online Social Networks

**Bhushan Patil<sup>1</sup>, Sagar Chougule<sup>2</sup>, Kiran Thorat<sup>3</sup>, Prof.Monika Dangore<sup>4</sup>**

Student, Computer Dept., D.Y. Patil COE, Pune, India <sup>1-3</sup>

Assistant Prof., Computer Dept., D.Y. Patil COE, Pune, India<sup>4</sup>

**Abstract:** Photo sharing is an attractive feature which popularizes Online Social Networks (OSNS). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. We attempt to address this issue and study the scenario when a user shares a photo containing individuals other than him/her. To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient facial recognition (FR) system that can recognize everyone in the photo. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency.

**Keyword:** Photograph protection, Social media, Secure Multi Calculation, Facial Recognition.

## I. INTRODUCTION

Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users' privacy if they are allowed to post, comment, and tag a photo freely. In this paper, we attempt to address this issue and study the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. For this purpose, we need an efficient Facial Recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, our mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. We also develop a distributed consensus based method to reduce the computational complexity and protect the private training set. We show that our system is superior to other possible approaches in terms of recognition ratio and efficiency. Our mechanism is implemented as a proof of concept Android application on Facebook's platform.

**Problem Definition:** Social sites have become important part of our daily life. Online social networks (OSNS) such as face book, Google and sound of birds are inherently designed to make able people to part personal and public information and make social connections with friends, co-workers, 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. An action is needed to over these many problems of social networks and makes the social networks very secure.

## II. LITERATURE SURVEY

Sr.No	Title	Author	Description
1	Friends with Faces: How Social Networks Can Enhance Face Recognition and Vice Versa	NikolaosMavridis WajahatKazmi, PanosToulis	In Friends with faces discussion Is there all about how social network can recognise faces how can not recognise faces
2	Control of Photo Sharing over Online Social Networks	Kaihe Xu YuanxiongGuo LinkeGuo Yuguang Fang Xiaolin Li	Facial recognition system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system
3	A Survey on Selective Control of Access of Photo Sharing on Online Social Network	Anusha Rao SonalFatangare JyotiRaghatwan	Here author worked on privacy concerns on photo sharing and tagging features on Facebook. A survey is used to study the

			effectiveness of the existing countermeasure of untagging and shows that users are worrying about offending their friends when untagging themselves.
4	What anyone can know: the privacy risks of social networking sites	D. Rosenblum	The privacy leakage caused byThe poor access control of shared data in web 2.0 isWell studied.
5	MPMD: Control of Photo Sharing	Kishor more Tusharkherade Milindpatil Rohitkaklj	Propose to use multiple personal fr engines toWork collaboratively to improve the recognition ratio.Specifically, they use the social context to select the suitableFr engines that contain the identity of the queriedFace image with high probability.
6	Robust Real-time Object Detection	Paul Viola Michael J. Jones	Discussthe difference between the traditional fr system and theFr system that is designed specifically for osns. TheyPoint out that a customized fr system for each user isExpected to be much more accurate in his/her own photoCollections

**Existing system:** In existing online social media sites if someone want to post a group photo then he/she will directly post the photo on his wall. That photo will be available to all his/her friends. In case of login one can easily login to account any person’s account if user name and password get hacked, for this also there is no any kind of strongsecurity.As one can easily post the images due to this next person could go through difficult conditions.

**Drawbacks of Existing system:**

- Posted photo in a party may reveal a connection of a celebrityto a mafia world
- Due to leakage of privacy some security agent are not able to take use of social media.
- If somehow any private person’s password get hacked then secret information about nation could get leaked.
- A married women could get divorce because of misunderstanding due to sharing of her photo by some other person.

**Proposed System:** Photo sharing is an appealing segment which propels Online Social Networks (OSNs). Unfortunately, it might discharge customer's security if they are allowed to post, comment, and name a photo transparently. In this paper, we try to address this issue and concentrate the circumstance when a customer shares a photo containing individuals other than himself/herself (named co-photo for short). We are proposing a framework where photograph can be partaken securely. In proposed System security is going to improvehere by means of OTP then weather one has someone’s password. Privacy of one’s is going to improve by means of taking his/her permission via notification. Problems of user due to posting of personal images on social site like Facebook by other user are resolved

**Advantages:**

- User is able to having account with full security then weather someone has hacked account.
- Any person who is not on social media as because of his/her privacy is getting leaked can have now account because of our proposed work of checking permission by notification.
- One person like national security agent can also now have account on social sites as because of privacy and security.

**Hardware Interfaces**

- Hardware - Pentium
- Speed - 1.1 GHz
- RAM - 1GB
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse

Software Interfaces	
Operating System	: Windows 10
Technology	: Java, J2EE
Web Technologies	: Html, JavaScript, CSS
IDE	: Eclipse Luna
Web Server	: Tomcat
Database	: My SQL
Java Version	: JDK 1.7 / 1.8

#### Technologies to be used

1. Front End : Java
2. Web content : (HTML, CSS, JS)
3. Back End : MYSQL

### III. CONCLUSION

Photo sharing is one of the most popular features in online social networks such as Facebook. Unfortunately, careless photo posting may reveal privacy of individuals in a posted photo. To curb the privacy leakage, we proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed a privacy-preserving FR system to identify individuals in a co-photo. The proposed system is featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiments were conducted to show effectiveness and efficiency of the proposed scheme.

### REFERENCES

1. N. Mavridis, w. Kazmi, and p. Toulis. Friends with faces: how social networks can enhance face recognition and vice versa. In *Computational social network analysis, computer communications and networks*, pages 453–482. Springer London, 2010.
2. Z. Stone, t. Zickler, and t. Darrell. Toward large-scale face recognition using social network context. *Proceedings of the IEEE*, 98(8):1408–1415., z. Stone, t. Zickler, and t. Darrell. Autotagging facebook: Social network context improves photo annotation. In *computer vision and pattern recognition workshops, 2008. CVPRW'08. IEEE Computer Society conference on*, pages 1–8. IEEE, 2008.
3. K. Choi, h. Byun, and k.-a. Toh. A collaborative face recognition framework on a social network platform. In *automatic face gesture recognition, 2008. FG '08. 8th IEEE international conference on*, pages 1–6, 2008.
4. 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.
5. D. Rosenblum. What anyone can know: the privacy risks of social networking sites. *Security privacy, IEEE*, 5(3):40–49, 2007.
6. C. Squicciarini, m. Shehab, and f. Paci. Collective privacy management in social networks. In *proceedings of the 18th international conference on world wide web, WWW '09*, pages 521–530, New York, NY, USA, 2009. ACM.