Review on Photo and video sharing privacy based on multiclass classifier in OSN

Ms.Devyani P Khambekar, Prof.Shaikh I.R

Abstract-Message sharing, photo sharing video sharing are the important aspects of online social network. Sharing such data requires security. There need to have a system that provide security to such shared data based on the content of post. Post may have different format such as text, image, video etc. There should be some mechanism that enables the user to participate in decision making activity of his/her photo and video sharing on any users wall. By analyzing post data and based on user policies decision can be taken to share or block the content. In case of multimedia data System automatically detects the user form shared images and video using efficient facial recognition FR technique. In this paper I am analyzing multiple systems and their contribution in this OSN security domain.

Index Terms- Image processing, video processing, FR technique, Social network, photo privacy

I Introduction

OSN is a social networking service. It is a package of an online service, platform, or site that concentrates on promoting the building of social networks or social relations with people. OSN provides platform for people to share interests, activities, backgrounds, or real-life connections. And hence it is very natural that people may post many contents like, photos, videos, political views, and financial reference etc. but sometimes people forgot that their uploaded information will be used by others i.e. enemies or criminal for the purpose that they never expect. Nowadays if we like any photo/videos on social sites, we immediately share that photo without thinking that shared photo may contain other people (is a co-photo) or not. There is no restriction with sharing of co-photos.
But problem is that, if co-partner involved in that photo/video may not will to share their photo/video on OSN, also OSN suffered from problems like, inaccuracy, subjectivity etc. Currently, many OSN users do not have control over the information which is appearing outside of their profile page of OSN. In [12], Thomas, Grier and Nicol determine that how to reduce the common privacy control inadvertently admit the sensitivity of user information.
To address this they recommend facebook's privacy model. Facebook's privacy model achieve multi-party privacy, this privacy is globally accepted to determine which information is uploaded and shared. Privacy policy helps co-partner to specify the users group where they are tagged.
FR problems are used with OSN; it may helps to utilized environmental information of social networking services. In regular FR system more training samples are required to generate high recognition ratio, but problem with this regular FR system is that sometime online photo assets are minimum. In this paper I propose to establish private photos set of the own user. And these private photos are used to model a personal FR system based on social background. Training data set i.e. set of private photos of user are distributed over the network could be formulated as typical secure multi-party computation problem as well as to achieve the efficiency and privacy we propose novel consensus based approach.

II Literature Survey

Privacy Regulation: Culturally Universal or Culturally Specific?[2] This paper proposes Altman's privacy regulation theory [1][15], this theory tells that privacy is a dialectic and dynamic i.e. privacy is changeable but it having control of accessing to self. Where "dialectic" means exploring self to other group and dynamic means level of privacy changes at some level. In this paper an analysis of the privacy is define as dynamic, dialectical and traditionally universal process. Thus privacy is pervasive and unique at certain levels of analysis.

Rule-Based Access Control for social networks[3] This paper introduced WBSN i.e. an access control model. In that policies are specified in terms of type of data and belief of relationship. Social Network Management Systems (SNMSs) allow users to state whether specific information e.g., personal data and resource should be public or private.
In this paper simple strategy has straightforward approach but, they are not flexible enough in denoting authorized users because they may grant access to non-authorized users.

Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks[4] This paper represents key idea of an OSN that are strongly correlated real-world activities i.e. By computing the correlation between the personal context models of the OSN members, the accuracy of event-based image annotation can be significantly improved. In this paper authors mainly did the personalize image search, a tag-based query only for retrieving images.

A collaborative face recognition framework on a social network platform[5] In this paper, authors were discussing about difference between a stand-alone based system and a social network based system where they propose a new collaborative face recognition technique. This technique avoids the redundant tagging by sharing the identification information for efficient update under the social network platform

Which Is the Best Multiclass SVM Method? An Empirical Study[6]_This paper proposed methods of multiclass that are competitive with each other and there is no clear superiority of one method over another.

These methods are:

- WTA SVM
- MWV SVM
- Pairwise Coupling

These methods are highly recommended as the best kernel discriminant methods for solving multiclass problems.

On Private Scalar Product Computation for Privacy-Preserving Data Mining[7]In this paper authors were represent private scalar product protocol based on standard cryptographic techniques and also proved that this technique is more secure.

Optimization technique is used to make result of proposed system more efficient

_Privacy-Preserving Set Operations[8]In this paper, authors proposed following set techniques for solving privacy issues in OSN:

1. Privacy-Preserving Set Operations
2. Set Operations Using Polynomial Representations
3. Operations with Encrypted Polynomials

This paper introduces two standard adversary models: honest-but-curious adversaries and malicious adversaries. In this authors were design efficient methods to enable privacy preserving computation of the union, intersection, and element reduction1 multiset operations.

The structure and function of complex networks[9]This paper reviews on structure and function of social networked systems. Work in this paper is motivated from real-world networks like, Internet, the World Wide Web, social networks, collaboration networks, citation networks, and a variety of biological networks.

In this paper, behavior and function of the networked systems is determined.

Unpacking "Privacy" for a Networked World[10]This paper represents researchers and practitioners to understand the better privacy by unpacking the more specific statements.

Authors do this by forming privacy regulation theory developed by social psychologist Irwin Altman [6, 7].

This paper proposed that how privacy management process is conducted in the presence of information technology.

.____Collective privacy management in social networks[11]Authors were describing a simple mechanism that promotes truthfulness, and that rewards users who publish co-partnership. They also combine their design with inference techniques that free the users from the burden of manually selecting privacy preferences for each picture. This paper also show a proof-of-concept application, which is implemented in the context of Facebook.

Toward Large-Scale Face Recognition Using Social Network Context Technique Used: MRF[12]__In this paper author proposed MRF technique for face recognition, where the large photo collection are on the web. Outputting the practice of users can produces large labeled image, to reduce enrollment burden.

Auto tagging Facebook : Social Network Context Improves Photo Annotation[13]In this paper for improving recognition performance, proposed method combines image data with social network background in a conditional random field model

Technique used: CRF model (Conditional Ramdom Fields)

CRF technique will be most effective when social network backgroud is available about all of the people who are likely to appear in a photographer's photos, but this information may not be available from Facebook for many reasons.

In this paper authors expect that their context-based labeling technique would perform far better with complete access to Facebook's data.

_unFriendly: Multi-Party Privacy Risks in Social Networks[14**]**In this paper, authors were examining how the lack of multi-party privacy controls for shared content can undermine a user's privacy. For process purpose threat model is used to classify properties of user information.

It unthinkingly exposed due to privacy conflicts. In this paper authors assume some parties involved are marketers, political groups, and monitoring agencies who have the resources, sophistication, and motivation to glean as much information from social networks as possible.

Robust Real-time Object Detection[15] In this paper following techniques are used to gain the privacy on OSN:

- object detection
- Speed of the Final Detector
- Image Processing
- Scanning the Detector

  In this paper **object detection** technique is used to minimize computation time to achieve high accuracy. The approach was used to construct a face detection system. The data sets included in the paper faces many conditions like, illumination, scale, pose, and camera variation.

III Proposed System

By analyzing the previously done our contributions in this domain is as follow:

1. Without generating tag the shared photos/videos are automatically identified.
2. I use private photos for privacy-preserving and some social context to get personal FR engine for specific user.
3. The system proposes novel consensus based approach, which may oppose to previous cryptographic solution.
4. Auto Blocking: if user always try to post video of certain person without his/her permission more than 3 times then that user will get automatically blocked.
5. confidentiality of the training set
6. Low computation cost for overall processing

From my contributions in this paper, I expect that my proposed personal FR engine be very useful for user to protect their privacy in social network. Latency or inactivity determine in this process will produce greater impact of user experience of OSN.

IV Conclusion

Multimedia data sharing is most popular and usual trend in current online social network. Such kind of data sharing may reveal user's privacy. We analyzed the previous work done in - user privacy in social network domain and concluded to have a system that enable individual to define a permission set for his/her photo sharing in online social network. An automatic face recognition system that detects user photograph from co-photo or from video and apply permission filter before sharing the data.

ACKNOWLEDGMENT

We are glad to express our sentiments of gratitude to all who rendered their valuable guidance to us. We would like to express our appreciation and thankful to Prof. S.R.Durugkar, Head of Department, Computer Engineering., S.N.D. College of Engineering. and Research Center, Nashik. We thank the anonymous reviewers for their comments

References

[1] My Privacy My Decision: Control of Photo Sharing on Online Social Networks
Kaihe Xu, Student Member, IEEE, Yuanxiong Guo, Member, IEEE, Linke Guo, Member, IEEE, Yuguang Fang, Fellow, IEEE, Xiaolin Li, Member, IEEE

[2] I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977.

[3] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.

[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] 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.

[6] P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663–1707, August 2010.

[7] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik?inen. On private scalar product computation for privacy-preserving data mining. In In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag, 2004.

[8] L. Kissner and D. X. Song. Privacy-preserving set operations. In V. Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 241–257. Springer, 2005.

[9] M. E. Newman. The structure and function of complex networks. SIAM review, 45(2):167–256, 2003.

[10] L. Palen. Unpacking privacy for a networked world. pages 129– 136. Press, 2003.

[11] A. 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.

[12] Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE, 98(8):1408–1415.

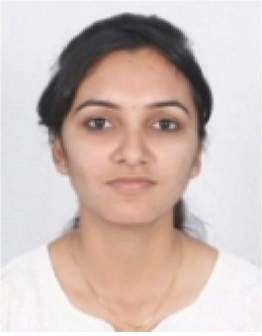
[13] Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE

[14]Computer Society Conference on, pages 1–8. IEEE, 2008.
[21] K. Thomas, C. Grier, and D. M. Nicol. unfriendly: Multi-

party privacy risks in social networks. In M. J. Atallah and N. J. Hopper, editors, Privacy Enhancing Technologies, volume 6205 of Lecture Notes in Computer Science, pages 236–252. Springer, 2010.

[15] P. Viola and M. Jones. Robust real-time object detection. In International Journal of Computer Vision, 2001.

Authors



Ms.Devyani P. Khambekar received the B.E. degree in Information Technology from Matoshri College of engineering & research centre,Nashik in 2014. She is currently pursuing her Masters degree in Computer Engineering from S.N.D. College of Engineering and Research Centre, Savitribai Phule Pune University Former UOP.This paperis published as a part of the research work done for the degree of Masters.

Prof. I. R. Shaikh is a professor in Department of Computer Engineering, S.N.D. College of Engineering and Research Centre, Savitribai Phule Pune University.