International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 25th Dec 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-13

Title: **EFFICIENT KEYWORD-AWARE REPRESENTATIVE TRAVEL ROUTE FRAMEWORK**

Volume 07, Issue 13, Pages: 733-739

Paper Authors

[1]**D.PRIYANKA,**

[2]**S.KRISHNA REDDY**

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

MY PRIVACY MY DECISION: CONTROL OF PHOTO SHARING ON ONLINE SOCIAL NETWORKS

[1]YAMANURIPAVANI, [2]M.S.S LAKSHMI LAVANYA

[1]Mtech student, Sree Dattha Institute of Engineering and Science

[2]Professor Sree Dattha Institute of Engineering and Science

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. 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.

1. INTRODUCTION

Photo sharing is an interesting component of Online Social Networks (OSNs)[6]. Users have no control over data residing outside their spaces. Each user has a different privacy concerns about the photos related to them. Each user can tag/share contents to his/her friends. OSNs only allows us to keep or delete the content. A large proportion of photographs contain face images which are associated with the daily lives of the photographers who captured them. Currently, online social networks (OSNs) such as Facebook ,Instagram, Twitter, and Snapchat are prevailing platforms on which people communicate with their social connections such as friends, family members, and colleagues in the real world. Social networks, due to many unfavorable incidents, have been blame for breaching the privacy of their users. Both in academia and in the media, the importance of a user's confidentiality has been rarely discussed. In addition to some proposed technical solutions, there have been a huge number of initiatives to educate users so that they do not provide an excessive amount of personal information. Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam. 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 thing which should be controlled is the availability of the personal informationwhich should be prevented from leakage as it may revealpersonal information of an individual in the form of videos, images or any data. As the popularity of social networks continues to grow, concerns surrounding sharing information online compound. Users regularly upload personal stories, photos, videos, and lists of friends revealing private details to the public. To protect user data, privacy controls have become a central feature of social networking sites but it remains up to users to adopt these features.

Privacy restrictions form a spectrum between public and private data.On the public end, users can allow every Facebook member to view their personal content. On the private end, users can restrict access to a specific set of trusted users. Facebook uses friendship to distinguish between trusted and untrusted parties. Users can allow friends, friends of friends, or everyone to access their profile data, depending on their personal requirements for privacy.

2. PROBLEM STATEMENT

Privacy policy and exposure policy

In this paper, we assume that each user i has a privacypolicy Pi(x) and a exposure policy Vi(x) for a specific photo x. The privacy policy Pi(x) indicates the set of users who can access photo x and exposure policy Vi(x) indicates the set of users who can access x when user I is involved. After people on co-photo x are recognized with our algorithm as a set I, the set of users who follow both the privacy policy and exposure policy could be calculated by:

$S = Pi(x)\backslash\ k \in IVk(x)$ (1)

We assume that our users have defined their privacy policy and exposure policy and these policies are modifiable. The exposure policy is treated as a private data that shall not be revealed, and a secure set intersection protocol is used to find the access policy S in 1. After the access policy S is established, the co-photo x will be shared with users in S.

FR with social contexts

An FR engine for a large-scale social network may require discriminating millions of individuals. It seems to be a daunting task that could never be accomplished. However, when we decompose it into several personal FR engines, the situation will change for better. Social contexts contains a large amount of useful information which could be utilized as a priori knowledge to help the facial recognition. In, Mavridis, Kazmi and Toulis develop a three-realm model to study facial recognition problems on OSN photos. The three realms include a social realm, in which identities are entities, and friendship a relation; a visual sensory realm, of which faces are entities and occurrence in images a relation; and a physical realm, in which bodies belong, with physical proximity being a relation. It is shown that the relationship in the social realm and physical realm are highly correlated with the relationship in the visual sensory realm. In this manner, we can use the social context to construct a priori distribution Pi over the identities on the co-photos for user i. With this priori distribution, while trying to recognize people on the cophotos, the FR engine could focus on a small portion of "close" friends (friends who are geographically close and interacting frequently with user i). We assume that for user i, we can define a threshold on the priori distribution Pi to get a small group of identities consisting of i and his one-hop neighbors (e.g., close friends), denoted as the neighborhood Bi. Then our goal for the personal FR at user i is to differentiate users in Bi.if Bob has a co-photo, we assume that users appear in the photo are among the setof {Divid, Eve, Tom, Bob}.

FR system

We assume that user i has a photo set of size Ni of himself/herself as his/her private training samples (say, stored on his/her own device such as smart phone). From the private photo set, a user detects and extracts the faces on each photo with the standard face detection method. For each face, a vector of size p is extracted as the feature vector. Then, for user i, his/her private training set could be written as xi of size Ni × p. In the rest of this paper, we use one record and one photo interchangeably to refer one row in xi**.**

GOALS

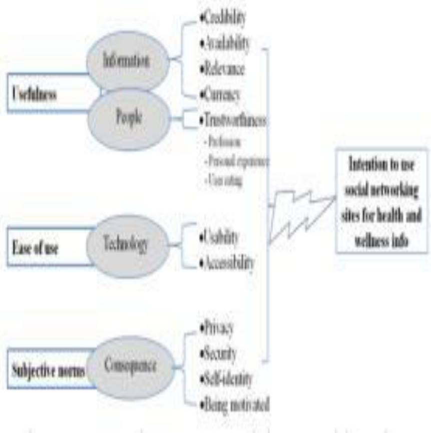
- We can find the potential owners of shared photos automatically even when the use of generated tags is kept as an option in our paper.
- Private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user is proposed in our paper.
- We propose a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

ALGORITHMS USED:

Homomorphic Algorithm

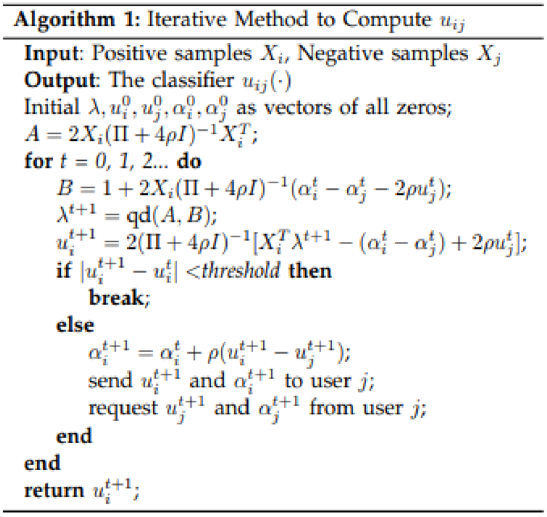
There are two steps to build classifiers for each neighborhood: firstly find classifiers of self, friend for each node, and then find classifiers of friend, friend. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other.

Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services.



Iterate Method of Compute:

Generally, the proposed distributed training scheme of a toy system could be summarized in Algorithm 1. In this Algorithm, uij = F(Xi, Xj) is the computation of classifier uij with Xi as positive training samples and Xj as negative training samples. qd(A, B) is a standard quadratic programming solver that gives the optimal solution of max{−12x T Ax + BT x}, and notice that we omit the constraint of 0 ≤ λ ≤ C for brevity. Threshold is the user-defined stopping criteria, a larger threshold results with fewer iterations while a larger discrepancy between ui and uj .



```
Algorithm 1: Iterative Method to Compute $u_{ij}$
 Input: Positive samples $X_i$, Negative samples $X_j$
 Output: The classifier $u_{ij}(\cdot)$
 Initial $\lambda, u_i^0, u_j^0, \alpha_i^0, \alpha_j^0$ as vectors of all zeros;
 $A = 2X_i(\Pi + 4\rho I)^{-1}X_i^T$;
 for $t$ = 0, 1, 2... do
     $B = 1 + 2X_i(\Pi + 4\rho I)^{-1}(\alpha_i^t - \alpha_j^t - 2\rho u_j^t)$;
     $\lambda^{t+1} = \mathrm{qd}(A, B)$;
     $u_i^{t+1} = 2(\Pi + 4\rho I)^{-1}[X_i^T\lambda^{t+1} - (\alpha_i^t - \alpha_j^t) + 2\rho u_j^t]$;
     if $|u_i^{t+1} - u_i^t| <$ threshold then
         break;
     else
         $\alpha_i^{t+1} = \alpha_i^t + \rho(u_i^{t+1} - u_j^{t+1})$;
         send $u_i^{t+1}$ and $\alpha_i^{t+1}$ to user $j$;
         request $u_j^{t+1}$ and $\alpha_j^{t+1}$ from user $j$;
     end
 end
 return $u_i^{t+1}$;
```

3. PROBLEM SOLUTION:

DISADVANTAGES:

- Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Facebook are encouraging users to post co-photos and tag their friends in order to get more people involved.
- Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page.

PROPOSED SYSTEM:

- We propose a privacy-preserving distributed collaborative training system as our FR engine. In our system, we ask each of our users to establish a private photo set of their own. We use these private photos to build personal FR engines based on the specific social context and promise that during FR training, only the discriminating rules are revealed but nothing else.
- In this paper, we propose a novel consensus based approach to achieve efficiency and privacy at the same time. The idea is to let each user only deal with his/her private photo set as the local train data and use it to learn out the local training result. After this, local training results are exchanged among users to form a global knowledge.
- In the next round, each user learns over his/hers local data again by taking the global knowledge as a reference. Finally the information will be spread over users and consensus could be reached.
- We show later that by performing local learning in parallel, efficiency and privacy could be achieved at the same time.

4. CONCLUSIONS

Photograph sharing is a standout amongst the most famous elements in online informal communities, for example,Facebook. Lamentably, imprudent photograph posting may uncover protection of people in a posted photograph. To check the protection spillage, we proposed to empower people conceivably in a photograph to give the authorizations before posting a co-photograph. We composed a protection saving FR framework to distinguish people in a co-photograph. The proposed framework is included with low calculation cost and privacy of the preparation set. Hypothetical investigation and tests were directed to show adequacy and effectiveness of theproposed conspire. We expect that our proposed plan beextremely helpful in ensuring clients' security in photograph/picture sharing over online informal communities. Be that as it may, there dependably exist exchange off amongst security and utility. For instance, in our present Android application, the co-photograph must be post with consent of all the co-proprietors. Inertness presented in this procedure will extraordinarily affect client experience of OSNs. More over, neighborhood FR preparing will deplete battery rapidly. Our future work could be the manner by which to move the proposed preparing plans to individual mists like Dropbox as well as icloud.

REFERENCES

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

[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, pages 1563–1572, New York, NY, USA, 2010. ACM.

[3] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan. 2011.

[4] 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.

[5] 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.

[6] 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.

[7] K.-B. Duan and S. S. Keerthi. Which is the best multiclass svm method? an empirical study. In Proceedings of the 6th international conference on Multiple Classifier Systems, MCS’05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.

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

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

[10] L. Kissner and D. Song. Privacy-preserving set operations. In IN ADVANCES IN CRYPTOLOGY – CRYPTO 2005, LNCS, pages 241–257. Springer, 2005.

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

[12] 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.

[13] R. J. Michael Hart and A. Stent. More content - less control: Access control in the web 2.0. In Proceedings of the Workshop on Web 2.0 Security and Privacy at the IEEE Symposium on Security and Privacy, 2007.

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

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

[16] J. C. Platt, N. Cristianini, and J. Shawe-taylor. Large margin dags for multiclass classification. In Advances in Neural Information Processing Systems 12, pages 547–553, 2000.

[17] D. Rosenblum. What anyone can know: The privacy risks of social networking sites. Security Privacy, IEEE, 5(3):40–49, 2007. Vol-3 Issue-3 2017 IJARIIE-ISSN(O)-2395-4396 5207 www.ijariie.com 918

[18] 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.

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

[20] Z. Stone, T. Zickler, and T. Darrell. Autotaggingfacebook: 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.

[21] K. Thomas, C. Grier, and D. M. Nicol. unfriendly: Multi-party privacy risks in social networks. In M. J. Atallahand N. J. Hopper, editors, Privacy Enhancing Technologies, volume 6205 of Lecture Notes in Computer Science, pages 236–252. Springer, 2010.

[22] M. Turk and A. Pentland. Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1):71–86, 1991.

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

[24] D. J. Watts and S. H. Strogatz. Collective dynamics of “smallworld” networks. nature, 393(6684):440–442,

1998.

[25] H. Yu, X. Jiang, and J. Vaidya. Privacy-preserving svm using nonlinear kernels on horizontally partitioned data. In Proceedings of the 2006 ACM symposium on Applied computing, SAC ’06, pages 603–610, New York, NY, USA, 2006. ACM.