Volume 2, Issue 12, December 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.821

NAIRJC JOURNAL PUBLICATION

North Asian International Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.821

MY PRIVACY: ON PHOTO SHARING OVER ONLINE SOCIAL NETWORK

PROF. DEEPALI PATIL [1], RUCHIKA GHARAT [2], TEJASHREE JADHAV [3], SHITAL KAMBLE [4] & PRATIKSHA ROKADE [5]

[12345][NMIET], Savitribai Phule, Pune University, Pune, India

ABSTRACT

Photograph sharing is an alluring component which advances Online Social Networks (OSNs). Sadly, it may release clients' security on the off chance that they are permitted to post, remark, and label a photograph openly. In this paper, we endeavor to address this issue and study the situation when a client shares a photograph containing people other than himself/herself (termed co-photograph for short). To anticipate conceivable security spillage of a photograph, we outline an instrument to empower every person in a photograph be mindful of the posting action and partake in the choice making on the photograph posting. For this reason, we require a proficient facial acknowledgment (FR) framework that can perceive everybody in the photograph. Notwithstanding, all the more requesting security setting may restrain the photographs' quantity freely accessible to prepare the FR framework. To manage this issue, our instrument endeavors to use clients' private photographs to plan a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their protection. We additionally add to a disseminated accords based system to diminish the computational many-sided quality and ensure the private preparing set. We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and effectiveness. Our instrument is executed as a proof of idea Android application on Facebook's stage.

1. INTRODUCTION

OSNS have become integral part of our daily life and has profoundly changed the way we interact with each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may

reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people (is a co-photo) or not. 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. However, what if the co-owners of a photo are not willing to share this photo? Is it a privacy violation to share this copho to without permission of the co-owners? Should the co-owners have some control over the co-photos? To answer these questions, we need to elaborate on the privacy issues over OSNs. Traditionally, privacy is regarded as a state of social withdrawal. According to Altman's privacy regulation theory, privacy is a dialectic and dynamic boundary regulation process where privacy is not static but "a selective control of access to the self or to ones group". In this theory, "dialectic" refers to the openness and closeness of self to others and "dynamic" means the desired privacy level changes with time according to environment. During the process of privacy regulation, we strive to match the achieved privacy level to the desired one. At the optimum privacy level, we can experience the desired confidence when we want to hide or enjoy the desired attention when we want to show. However, if the actual level of privacy is greater than the desired one, we will feel lonely or isolated; on the other hand, if the actual level of privacy is smaller than the desired one, we will feel over-exposed and vulnerable. Unfortunately, on most current OSNs, users have no control over the information appearing outside their profile page. In, Thomas, Grier and Nicol examine how the lack of joint privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they suggest Facebook's privacy model to be adapted to achieve multi-party privacy. Specifically, there should be a mutually acceptable privacy policy. Determining which information should be posted and shared. To achieve this, OSN users are asked to specify a privacy policy and a exposure policy. Privacy policy is used to define group of users that are able to access a photo when being the owner, while exposure policy is used to define group of users that are able to access when being a co-owner. These two policies will together mutually specify how a co-photo could be accessed. However, before examining these policies, finding identities in cophotos is the first and probably the most import step. In the rest of this paper we will focus on a RF engine to find identities on a co-photo. FR problem because the contextual information of OSN could be utilized for FR. For example, people showing up together on a co-photo are very likely to be friends on OSNs, and thus, the FR engine could be trained to recognize social friends (people in social circle) specifically. Training techniques could be adapted from the off-the-shelf FR training algorithms, but how to get

enough training samples is tricky. FR engine with higher recognition ratio demands more training samples (photos of each specific person), but online photo resources are often insufficient. Users care about privacy are unlikely to put photos online. Perhaps it is exactly those people who really want to have a photo privacy protection scheme. To break this dilemma, 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 With the training data (private photo sets) distributed among users, this problem could be formulated as a typical secure multi-party computation problem. Intuitively, we may apply cryptographic technique to protect the private photos, but the computational and communication cost may pose a serious problem for a large OSN. 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. Comparing with previous works, our contributions are:

1. In our paper, the potential owners of shared items (photos) can be automatically identified with/without user-generated tags.
2. We propose to use private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user.
3. Orthogonal to the traditional cryptographic solution, we propose a consensus based method to achieve privacy and efficiency.

2. RELATED WORK

We proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed privacy –preserving FR system to identify individuals in a co-photo. The proposed system in featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiment were conducted to show effectiveness and efficiency of the proposed scheme.

3. MOTIVATION

In Mavridis et al. study the insights of photograph sharing on informal communities and propose a three domains show: "a social domain, in which characters are elements, what's more, kinship a connection; second, a visual tangible domain, of which faces are elements, and co-event in pictures a connection; and third, a physical domain, in which bodies have a place, with physical closeness being a connection." hey demonstrate that any two domains are very corresponded. Given data in one domain, we can give a decent estimation of the relationship of the other domain. In Stone et al., interestingly, propose to utilize the logical data in the social domain and co photo relationship to do programmed FR. They characterize a pair wise restrictive arbitrary field (CRF) model to locate the ideal joint maximizing so as to mark the contingent thickness. In particular, they utilize the current marked photographs as the preparation tests and join the photograph co event measurements and standard FR score to move forward the exactness of face annotation.

4. IMPLEMENTATION DETAILS

4.1 System architecture

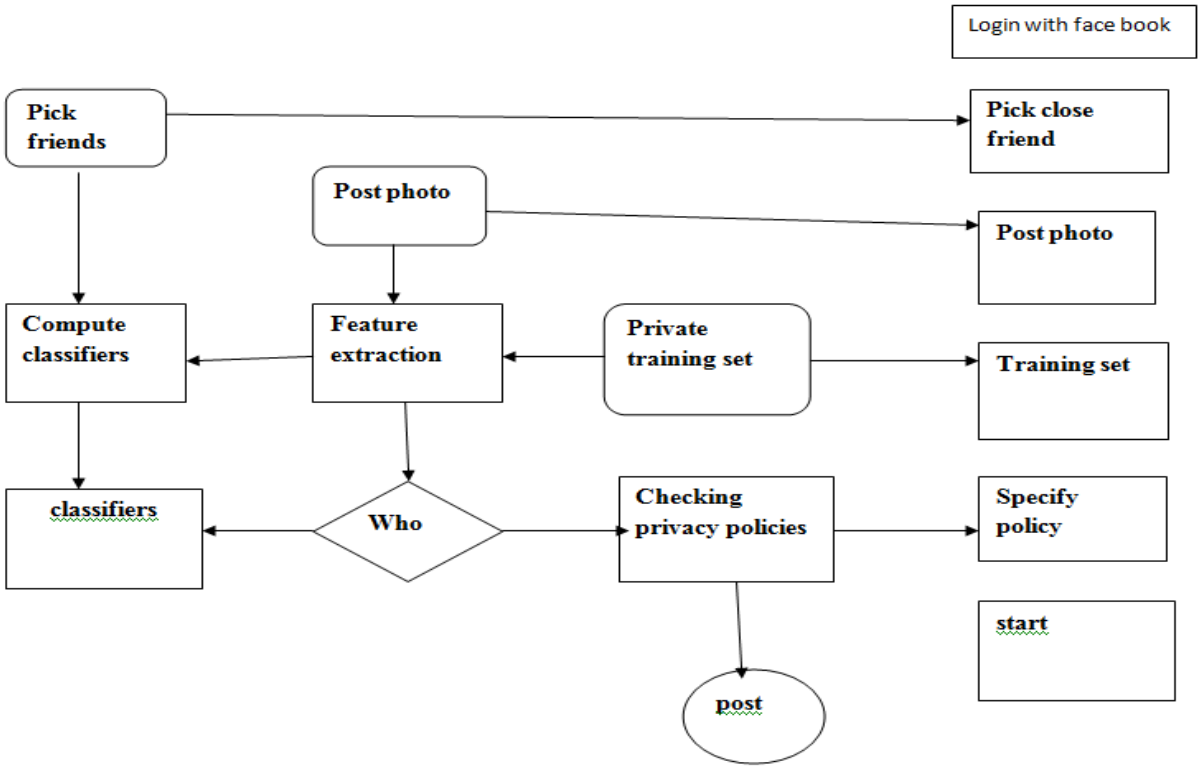
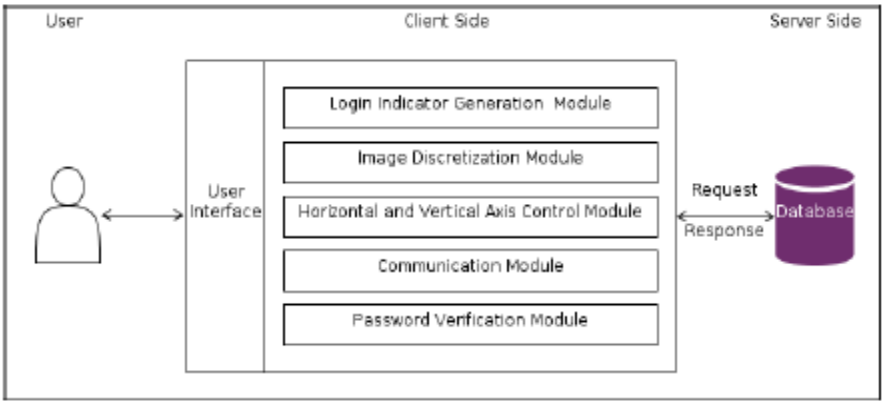


Fig.1: System Architecture

4.2 Module



4.2.1 Image Discretization Module.

This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, an image is divided into a 7 *11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices.

.

4.2.2 Login Indicator Generator Module.

This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7*11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called.

The generated login indicator can be given to users visually or acoustically in our system we are sending this patterns on users email.

4.2.3 Horizontal and Vertical Axis Control Module.

There are two scroll bars: a horizontal bar with a sequence ofletters and a vertical bar with a sequence of numbers.

4.2.4 Communication Module.

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

4.2.5 Password Verification Module.

This module verifies the user password during the authentication phase. A pass Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green).square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

4.3 Proposed work

In this paper, we proposed to empower people conceivably in a photograph to give the constants before posting a co-photograph. We outlined a security protecting FR framework to distinguish people in a co-photograph. The proposed framework is highlighted with low calculation expense and classification of the preparation set. Hypothetical investigation and analyses were directed to show adequacy and proficiency of the proposed plan. We expect that our proposed plan be extremely helpful in ensuring clients' security in photograph/picture sharing over online informal communities. Then again, there dependably exist exchange off in the middle of protection and utility. For instance, in our present Android application, the co-photograph must be post with consent of all the co-proprietors. Dormancy presented in this procedure will incredibly affect client experience of OSNs. Moreover, nearby FR preparing will deplete battery rapidly.

4.4 Algorithm

Algorithm Classifier Computation Algorithm

Initial as $\mathcal{C}_i = \emptyset, \forall i \in \mathcal{N}$;
for $i \in \mathcal{N}$ **do**
  for $j \in \mathcal{B}_i$ **do**
    if $u_{ij} \notin \mathcal{C}_i$ **then**
      $u_{ij} = F(X_i, X_j)$;
      $u_{ji} = -u_{ij}$;
      $\mathcal{C}_i = \{u_{ij}, \mathcal{C}_i\}$; $\mathcal{C}_j = \{u_{ji}, \mathcal{C}_j\}$;
    end
  end
end
for $i \in \mathcal{N}$ **do**
  for $k, j \in \mathcal{B}_i \parallel k \neq j$ **do**
    if $u_{kj} \notin \mathcal{C}_k$ **then**
      $u_{kj} = F(X_k, X_j)$;
    else
      Request u_{jk} from user j;
    end
    $\mathcal{C}_i = \{u_{jk}, \mathcal{C}_i\}$;
  end
end

According to Algorithm 1, there are two steps to build classifiers for each neighborhood: firstly find classifiers of {self, friend} for each node, 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. For this consideration, when building classifiers of {friend, friend}, all the local training results are send to the neighborhood owner, who will coordinate the collaborative training processes by forwarding local training results to right collaborators. In this manner, friends need not to know who they are working with and how to talk with them.

5. ACKNOWLEDGEMENT

We would like to take this opportunity to thank Prof. Deepali Patil for giving us all the help and guidance we needed. We are greatful to them for their kind support. Their valuable suggestions were very helpful.

6. CONCLUSION

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations, for example, Facebook. Lamentably, imprudent photograph posting may uncover security of people in a posted photograph. To control the security spillage, we proposed 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. Then again, there dependably exist exchange off in the middle of protection and utility. For instance, in our present Android 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 Dropbox and/or icloud.

7. REFERENCE

1. I. Altman. 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 privacy-preserving 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 in Computer Science, pages 241–257. Springer, 2005.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com