Preventing Privacy Leakage and Photo Leakage

Swati Bhadkumbhe,Snehal Jadhav, Ashlesha Rothe , Akash Desai

[1] *Assistant Professor, Computer Department, P.D.E.A'sCOEM, Maharashtra, India*
[2] *Student, Computer Department, P.D.E.A'sCOEM, Maharashtra, India*
[3] *Student, Computer Department, P.D.E.A'sCOEM, Maharashtra, India*
[4] *Student, Computer Department, P.D.E.A'sCOEM, Maharashtra, India*

ABSTRACT

Photo sharing is an attractive feature which popularizes Online Social Networks (OSNs). Unfortunately, it may leak users priv acy if they are allowed to post, comment, and tag a photo freely. We attempt to add ress 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 mechanis m 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.

Keyword : *- Photo Privacy, Social Networks, Friend Lists, Collaborative Learning, etc.*

1. INTRODUCTION

Social sites have become important part of our daily life. Online social networks (OSNs) such as face book, Google are inherently designed to make able people to part personal and public information and make social connections with friends, coworkers, persons having like position, family, and even with strangers. 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 dialectic and dynamic boundary regulations 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 multiparty 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 an 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 co-photos 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 cophoto. FR problems over OSNs are easier than a regular 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' cares 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 as follows. 1) In our paper, the potential owners of shared items (Photos) can be automatically identified With/without user-generated tags. Research Article Volume 7 Issue No. 1 International Journal of Engineering Science and Computing, January 2017 4095 http://ijesc.org/ 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. The rest of this paper is organized as follows. In Section 2, we review the related works. Section 3 presents the formulation of our problem and the assumptions in our study. In Section 4, we give a detailed description of the proposed mechanis m, followed by Section 5, conducting performance analysis of the proposed mechanism. In Section 6, we describe our implementation on Android platform with the Facebook SDK and the extensive experiments to validate the accuracy and efficiency of our system. Finally, Section 7 concludes the paper.

2. RELATED WORK

In, Mavridis et al. study the statistics of photo sharing on social networks and propose a three realms model: "a social realm, in which identities are entities, and friendship a relation; second, a visual sensory realm, of which faces are entities, and co-ccurrence in images a relation; and third, a physical realm, in which bodies belong, with physical proximity being a relation." They show that any two realms are highly correlated. Given information in one realm, we can give a good estimation of the relationship of the other realm. In Stone et al., for the first time, propose to use the contextual information in the social realm and cophoto relationship to do automatic FR. They define a pairwise conditional random field (CRF) model to find the optimal joint labeling by maximizing the conditional density. Specifically, they use the existing labeled photos as the training samples and combine the photo cooccurrence statistics and baseline FR score to improve the accuracy of face annotation. In, Choi et al. discuss the difference between the traditional FR system and the FR system that is designed specifically for OSNs. They point out that a customized FR system for each user is expected to be much more accurate in his/her own photo collections. A similar work is done, in which Choi et al. propose to use multiple personal FR engines to work collaboratively to improve the recognition ratio. Specifically, they use the social context to select the suitable FR engines that contain the identity of the queried face image with high probability. While intensive research interests lie in FR engines refined by social connections, the security and privacy Issues in OSNs also emerge as important and crucial research topics. The privacy leakage caused by the poor access control of shared data in Web 2.0 is well studied. To deal with this issue, access control schemes are proposed in these works, flexible access control schemes based on social contexts are investigated. However, in current OSNs, when posting a photo, a user is not required to ask for permissions of other users appearing in the photo. In, Besmer and Lipford study the privacy concerns on photo sharing and tagging features on Facebook. A survey was conducted in to study the effectiveness of the existing countermeasure of untagging and shows that this countermeasure is far from satisfactory: users are worrying about offending their friends when untagging. As a result, they provide a tool to enable users to restrict others from seeing their photos when posted as a complementary strategy to protect privacy. However, this method will introduce a large number of manual tasks for end users. In, Squicciarinietal. propose a game -theoretic scheme in which the privacy policies are collaboratively enforced over the shared data. Each user is able to define his/her privacy policy and exposure policy. Only when a photo is processed with owner's privacy policy and co-owner's exposure policy

could it be posted. However, the co-owners of a co-photo cannot be determined automatically, instead, potential co-owners could only be identified by using the tagging features on the current OSNs.

3. NEED

Users upload the picture and tag other people even though they are willing or not willing to be part of uploaded image/content. 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.

4. APPLICATIONS

4.1 Photo privacy: In photo privacy can't see the photo to all users without it's permission
4.2 Secure Chat: Secure chat means chatting Is in encrypted format means that chatting cant seen to another users rather than these two chatting people.
4.3 Provide Security: Security is provided for chatting, comments and photo.

5. PROBLEM S TATEMENT

To enable sharing of pictures or images in a secure manner so that privacy is maintained and there will less possibility of loss of information

6. MODULES

6.1 Login

In this module user first do registrations then login in to the system. It provide authentication.

6.2 Registration

In this module users do the registration for login in to the system. Using registration we gather all information about users. For ex. Name, DOB, password, Email-Id.

6.3 Upload Photo

In this module we first select photo and then user upload photo and then send request to each uploaded photo user. If accept that request then view that uploaded photo otherwise blurring image displayed to each user.

6.4 Send Request

In this module user first detect faces then send request to each detected faces in that photo users.

6.5 Accept request

In this module uploaded photo user accept the request and if that person accept request then view that person face otherwise blurring that particular face area.

6.6 Blurring Image

In this module blurring image is displayed to users if uploaded A photo user does not accept the request.

6.7 Comments

In this module two type of comments.
• Private
If comments are private then that comment view to only that particular user.
• Public

If comments are public then that comment view to all users

8. Chatting
In this module chatting is displayed to all users in encrypted format. In that when one person chatting with another person that is in encrypted format means another users can't seen that chatting .

7. SYSTEM ARCHITECHTURE

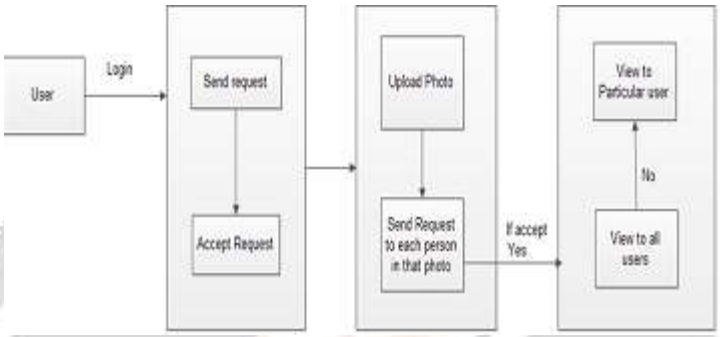

Figure.1. System Architecture

8.IMPLEMENTATION

8.1 Tools and Technology
_ Tools PC,Laptop,Android phone
_ Technology Java and J2EE HTML Java Script CSS

8.2 Methodologies /Algorithm Details

8.2.1 FR training algorithms
Performed routinely and e_ortlessly by humans
Enormous interest in automatic processing of digital images and videos dueto wide availability of powerful and low-cost desktop embedded computing

Applications:
1. biometric authentication,
2. surveillance,
3. human-computer interaction
4. multimedia management

Advantages over other biometric technologies:
_ Natural
_ Nonintruisive
_ Easy to use
Among the six biometric attributes considered by Hietmeyer, facial features scored the highest compatibility in a Machine Readable Travel Documents (MRTD) system based on:
_ Enrollment
_ Renewal
_ Machine requirements
_ Public perception
_ Face recognition
_ Face recognition processing

_ Analysis in face subspaces
_ Technical challenges
_ Technical solutions

8.2.2 Classifier Computation Algorithm
There are two steps to build classifiers for each neighborhood: firstly find classifiers of self, friends for each node, then find classifiers of firiend, friends. 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.

8.2.3 Homomorphic Encryption Algorithm
Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, 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.

8.3 Veri_cation and validation
The application run successfully as per user convinience and requirement without any error. In this application there will be less possibility of loss information.Every users in this application get request while uploading the photo of that users.In this application security is provided using encryption and decryption algorithm

9.FR S YSTEM

We assume that useri 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 With the private training set, each user will have a personal FR engine to identify his/her one-hop neighbours. The personal FR can be constructed as a multi-class classification system, where each class is corresponding to one user (himself/herself or one friend). In the rest of this paper, we use one class interchangeably with the appearance of one user. In the realm of machine learning, usually a multi-class classification system is constructed by combining several binary classifiers together with the one of the following strategies: • One-against-all method uses winner-take-all strategy. It constructs n binary classifiers for each of n classes. The goal of each binary classifier is to distinguish one class from the rest with a decision function. Hence, the ith decision function fi is trained by taking records from user i as positive samples and the records from all the other users as the negative samples. When a testing record x comes, if fi concludes that it belongs to class i, x is labeled as class i. • One-against-one method uses max-voting-win strategy. It constructs n (n − 1)/2 binary classifiers, in which each classifier is aimed to distinguish two classes. The idea is that if we can distinguish any two classes, then we can identify any of them. Hence, classifier uij is constructed by taking records from i as positive samples and records from j as negative ones. Later on when we are trying to identify a test record x, if uij concludes that x is in class i, then the vote of class i is added by one. After testing all the n (n − 1)/2 classifiers, x is assigned to the class with the largest voting value. However, no matter which method we use, it requires a centralized node to access all the training samples from each class, which is conflicting with our promise that the private training samples will not be disclosed during the whole process. In the rest of this paper we will focus on how to build the

personal FR engines without disclosing the private photo sets. Notice that the identification criterion could be asymmetric between different a personal FR engine, which means that the way how David finds out Bob and how Bob finds out David are not the same as shown in Fig. 1. The reason is that, for Bob, his personal FR engine only knows how to find out David from the candidate set (”suspects” for short) of {Bob, David, Eve, Tom}, while for David, his personal FR only knows how to find out Bob from the suspects of {Alice, Bob, David, Tom}. In other words, with different friend sets (friendship graph) at each node, the personal FR engines are trained with different negative training samples.

10.ALGORITHMS

10.1 AES

Step 1. Derive the set of round keys from the cipher key.

Step 2. Initialize the state array with the block data (plaintext).

Step 3. Add the initial round key to the starting state array.

Step 4. Perform nine rounds of state manipulation.

Step 5. Perform the tenth and final round of state manipulation.

Step 6. Copy the final state array out as the encrypted data (ciphertext).

AES(K, W)	Encrypt W using the AES codebook with key K
AES-1(K, W)	Decrypt W using the AES codebook with key K
MSB(j, W)	Return the most significant j bits of W
LSB(j, W)	Return the least significant j bits of W
B1 ^ B2	The bitwise exclusive or (XOR) of B1 and B2
B1 | B2	Concatenate B1 and B2
K	The key-encryption key K
n	The number of 64-bit key data blocks
s	The number of steps in the wrapping process,s=6n
P[i]	The ith plaintext key data
C[i]	The ith ciphertext data block
A	The 64-bit integrity check register
R[i]	An array of 64-bit registers where i = 0, 1, 2, ..., n
A[t], R[i][t]	The contents of registers A and R[i] after encryption step t.

IV The 64-bit initial value used during the wrapping process.

11. FLOWCHART

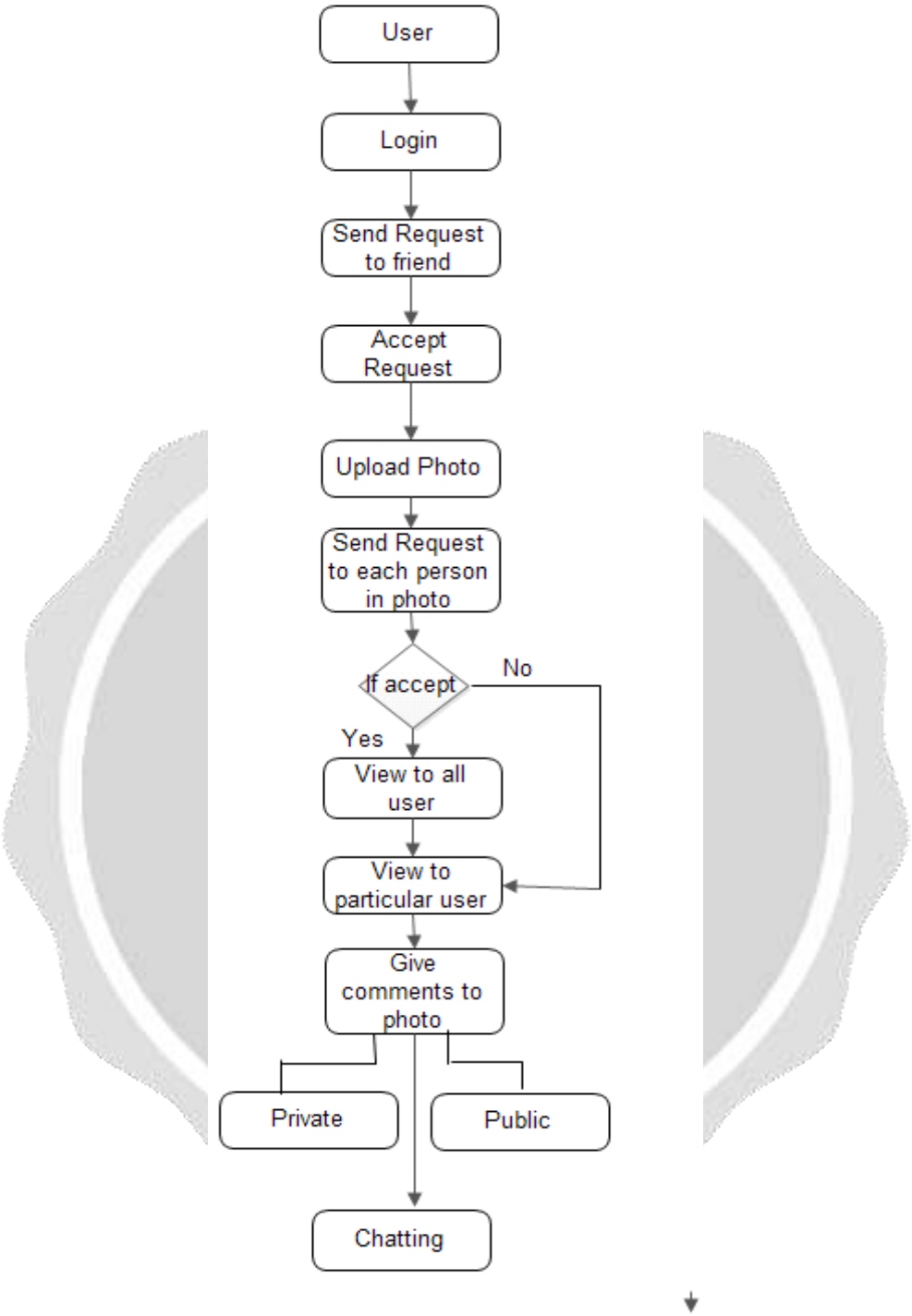

Fig -2: Flowchart

12.MATHEMATICAL MODEL

S= s, F, d, C

S = Face Recognition.

s = set of input symbols = Video File, image, character information

F = set of output symbol = Match Found then notification to user, Not Found

d =

1. Start

2. Read training set of images
3. Resize image dimensions to
4. Select training set of Dimensions, M: number of sample images
5. Find average face, subtract from the faces in
the training set, create matrix A Where,
= average image,
M= number of images, and
i= image vector.
F i = i
Where, i = 1, 2, 3, , M.
A = [F1, F2, F3....FM]
6. Calculate covariance matrix: AA'
7. Calculate eigenvectors of the c covariance matrix.
8. Calculate eigenfaces = No. of training images no. of classes (total number of people) of eigenvectors.
9. Create reduced eigenface space- The selected set of eigenvectors are multiplied by the A matrix to create a reduced eigenface
10. Calculate eigenface of image in question.
11. Calculate Euclidian distances between the image and the eigenfaces.
12. Find the minimum Euclidian distance.
13. Output: image with the minimum Euclidian distance or image unrecognizable
C = The system will not process the audio data, Eigenfaces will generate the grayscale images, The algorithm will run only on key frames.

13.RESULTS

13.1

Figure 2: Start page

13.2

Figure 3: Registration page

13.3

Figure 4: Login page

13.4

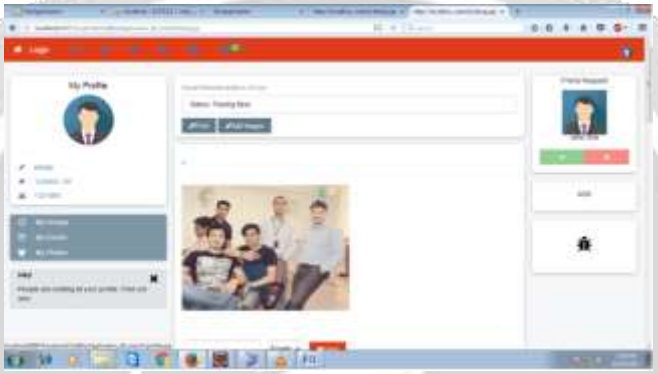

Figure 5: Home page

13.5

Figure 6: Photo upload

13.6

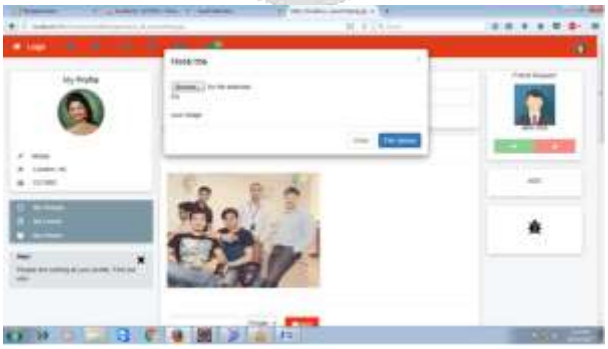

Figure 7: Photo add image

13.7

Figure 8: Select image

13.8

Figure 9: Face detect and Add tag

13.9

Figure 10: Enter key and Submit name

13.10

Figure 11: Check request

13.11

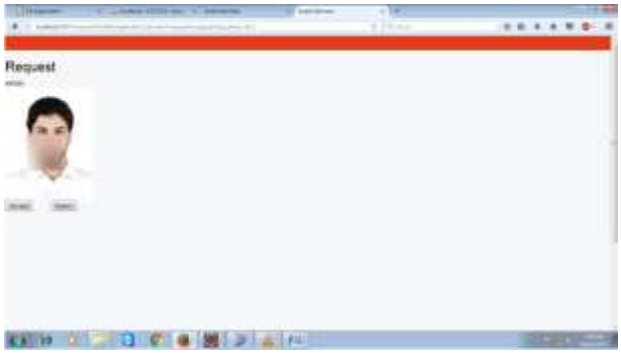

Figure 12: Bluring image

14. 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. We expect that our proposed scheme be very useful in protecting users privacy in photo/image sharing over online so cial networks. However, there always exist trade-o between privacy and utility. For example, in our current Android application, the co-photo could only be post with permission of all the co-owners. Latency introduced in this process will greatly impact user experience of OSNs. Moreover, local FR training will drain battery quickly. Our future work could be how to move the proposed training schemes to personal clouds like Dropbox and/or icloud.

15. REFERENCES

[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 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.