ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

OUR SECLUSION OUR DECISIVENESS

Dr.R.Sumathi[1], S.Elavarasi[2], A.Geethanjali[3], A.Johncy Arul[4]

[1]Professor, Saranathan College of Engineering
[2,3,4]Student, Saranathan College of Engineering

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 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, an efficient facial recognition (FR) system that can recognize everyone in the photo is needed based on their unique feature . 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 consent based method to protect the private training set with less computational complexity. The theoretical explanation shows our system is superior to other possible approaches in terms of recognition ratio. Our mechanism is implemented as a proof of concept Android application on Social media's platform. The power-law distribution is caused by the preferential attach process, in which the probability of a user A connecting to a user B is proportional to the number of B's existing connections.

Key terms: Co-owner, Facial Recognition, Feature, Privacy, Social Network

1. Introduction

Dependability is a measure of a system's availability, reliability, and its maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security. Security is the ability to provide services that can defensibly be trusted within a time-period. This may also encompass mechanisms designed to increase and maintain the dependability of a system or software. OSN's 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. 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 or not. Currently there is no restriction with sharing of co-photos, on the contrary, social network service providers like Facebook.

Traditionally, privacy is regarded as a state of social withdrawal. According to Altman's[1] 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.

Online Social Network 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 co-photos is the first and probably the most import step. In the rest of this paper we will focus on a face recognition engine to find identities on a co-photo.

2. Literature survey

Altman[1] examined privacy as a generic process that occurs. Privacy is a boundary control process where people sometimes makes themselves open and accessible to others and sometimes close themselves off from others. Dialectic is a process in which oppositional qualities are aspects of a single unity (Rychlak, 1976), forces to be open or closed shift over time and with circumstances. Within the preceding conceptual framework, privacy serves three functions: (a) management of social interaction, (b) establishment of plans and strategies for

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

interacting with others, and (c) development and maintenance of self-identity.

Privacy mechanisms define the limits and boundaries of the self. When the permeability of these boundaries is under the control of a person, a sense of individuality develops. But it is not the inclusion or exclusion of others that is vital to self definition; it is the ability to regulate contact when desired. If I can control what is me and what is not me. if I can observe the limits and scope of my control, then I have taken major step toward understanding and defining what I am. Privacy as a cultural universal, one must realize that this is an area of long standing concern and controversy among anthropologists and other cross-cultural researchers, and that there are many pitfalls and complexities associated with any search for universals.

Before launching into an examination of privacy across cultures, it is important to recognize several problems with such an analysis. First, it is not easy to use ethnographic materials to verify or confirm the framework of this article. Many cultural descriptions are not sufficiently explicit and were not developed with our particular model of privacy in mind. Thus, there may be instances in which a culture is described as having "no privacy," examples are provided. In privacy regulation in individual cultures They examined privacy in three types of bonds: (a) peripheral relationships, such as strangers and acquaintances;(b) more extensive bonds, such as in-laws; and (c)close relationships, between husbands and wives and parents and children.

They propose a framework emphasizing dialectic and boundary control features of privacy, whereby people can make themselves accessible or inaccessible to others. Furthermore, He suggest that privacy regulation involves more than use of the physical environment alone, but includes a variety of verbal, nonverbal, environmental, and cultural mechanisms. Thus, I conceptualize privacy as a complex and molar phenomenon that requires a broader perspective than it has received in the past.

Besmer & Lipford[2] examined privacy concerns and mechanisms surrounding these tagged images. Using a focus group, they explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. Photo tagging is a popular feature of many social network sites that allows users to annotate uploaded images with those who are in them, explicitly linking the photo to each person's profile. They then designed a privacy enhancing mechanism based on our findings, and validated it using a mixed methods approach. Our results identify the social tensions that tagging generates, and the needs of privacy tools to address the social implications of photo privacy management.

Online photo sharing applications are increasingly popular, offering users new and innovative ways to share photos with a variety of people. Many social network sites are also incorporating photo sharing features, allowing users to very easily upload and post photos for their friends and families. Increased access to an individual's photos has led to these images being used for purposes that were not intended. User tagging adds a new twist to this problem in that users are often posting photos of other users. As a result, people have reduced control over their image and its reach. This in turn, can lead to greater risks for embarrassment or humiliation over the content of photos.

Photo privacy may become even more problematic in the future as researchers are discovering effective automated algorithms to identify people in images and tag them. As facial recognition becomes more accurate, it will be easier than ever before to locate individuals in photo collections and link people between different collections. This makes tagging, and thus sharing, images even easier. Yet this further erodes users' abilities to control the disclosure of their images as they could be automatically identified in many more photos, uploaded by many people. They seek to add to the growing literature by providing a greater understanding of privacy concerns and needs of users, in addition to creating a privacy mechanism meant to address those needs. To quote the usability mantra, "know thy users" and then design for them. They believe that by first understanding users' current concerns and behaviors, they can design tools they desire, adopt, and are motivated to use. Other designers will also able to use our results to do the same.

Photo sharing is an important component of many general online social network sites. Many researchers have examined how various profile information and social features of these sites are used for managing identity, communicating with social networks, and forming and strengthening relationships. The over disclosures of personal information and potential risks of personally identifiable information on Facebook profiles have also been explored. However, little work investigated privacy specifically in this domain of photo sharing within social network sites or the issues with photos posted by others. While some aspects may be similar to other online photo sharing, they expect that the large social networks that users tend to build, and the inherent linking of photos to other personal information about users, will lead to different concerns, strategies, and needs regarding privacy management.

They introduced the "Restrict Others" tool to address photo privacy. It works by allowing tagged users to send a request to the owner asking that a photo be hidden from certain people. This tool addresses concerns users have and the short comings of the current mechanisms. It does so in a way that we believe minimally impacts the social value users find in photos and uses naturally existing tensions to help manage user privacy. Restrict Others takes previously out of band communication and integrates it into the management and negotiation of privacy settings between the photo uploader and the tagged user.

Restrict others explicitly dealt with the natural tension that arises between the owner of the photo, and those tagged in

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

it. They created a lightweight means for users to negotiate desired sharing, complementing the existing privacy coping mechanisms that users currently employ. In manipulating these ownership tensions, they believe their tool would help users achieve more desired privacy while still maximizing the social value of sharing.

Social Networking is one of the major technological phenomena of the Web 2.0, with hundreds of millions of people participating. Social networks enable a form of self-expression for users, and help them to socialize and share content with other users. In spite of the fact that content sharing represents one of the prominent features of existing Social Network sites, Social Networks yet do not support any mechanism for collaborative management of privacy settings for shared content.

Squicciarini et al[3] modeled the problem of collaborative enforcement of privacy policies on shared data by using game theory. In particular, they propose a solution that offers automated ways to share images based on an extended notion of content ownership. Building upon the Clarke-Tax mechanism, they described a simple mechanism that promotes truthfulness, and that rewards users who promote co-ownership. They integrate their design with inference techniques that free the users from the burden of manually selecting privacy preferences for each picture.

In current SNs, when uploading a picture, a user is not required to ask for permissions of other users appearing in the photo, even if they are explicitly identified through tags or other metadata. Although most social networking and photo sharing websites provide mechanisms and default configurations for data sharing control, they are usually simplistic and coarse-grained. Pictures, or in the more general case, data, are usually controlled and managed by single users who are not the actual or sole stakeholders, raising serious privacy concerns.

They discussed a novel model for privacy management across social networks, where data may belong to many users. They presented a theoretical representation of the collective privacy management problem, and proposed a solution which builds upon well-known game theoretical results. They implemented a tool prototype hosted in Facebook, and carried out performance analysis. Our next step is to conduct extensive user studies, to assess the users' perspective of this type of approach. In a preliminary investigation, they observed high interest from users toward approaches allowing users' control over shared content.

Choi et al[4] proposed face annotation is a effective management of personal photos in online social networks (OSNs) is currently of considerable practical interest. In this paper, they proposed a novel collaborative face recognition (FR) framework, improving the accuracy of face annotation by effectively making use of multiple FR engines available in an OSN. Our collaborative FR framework consists of two major parts: selection of FR engines and merging (or fusion) of multiple FR results. The selection of FR engines aims at determining a set of personalized FR engines that are suitable for recognizing query face images belonging to a particular member of the OSN. For this purpose, they exploit both social network context in an OSN and social context in personal photo collections. In addition, to take advantage of the availability of multiple FR results retrieved from the selected FR engines, they devised two effective solutions for merging FR results, adopting traditional techniques for combining multiple classifier results. Experiments were conducted using 547 991 personal photos collected from an existing OSN. Our results demonstrate that the proposed collaborative FR method is able to significantly improve the accuracy of face annotation, compared to conventional FR approaches that only make use of a single FR engine.

ONLINE social networks (OSNs) such as Facebook and My Space are frequently used for sharing and managing personal photo and video collections. The act of labeling identities (i.e., names of individuals or subjects) on personal photos is called *face annotation* or *name tagging*. *This* feature is of considerable practical interest for OSNs thanks to its high commercialization potential.

It demonstrates that the collaborative use of multiple FR engines allows improving the accuracy of face annotation for personal photo collections shared on OSNs. Finally, in this work, the *Viola-Jones* face detection algorithm was used for detecting face images in personal photos. In practice, however, the accuracy of the *Viola-Jones* face detection algorithm may be problematic depending upon the targeted applications as well as the associated parameter setup.

3.SYSTEM ARCHITECTURE

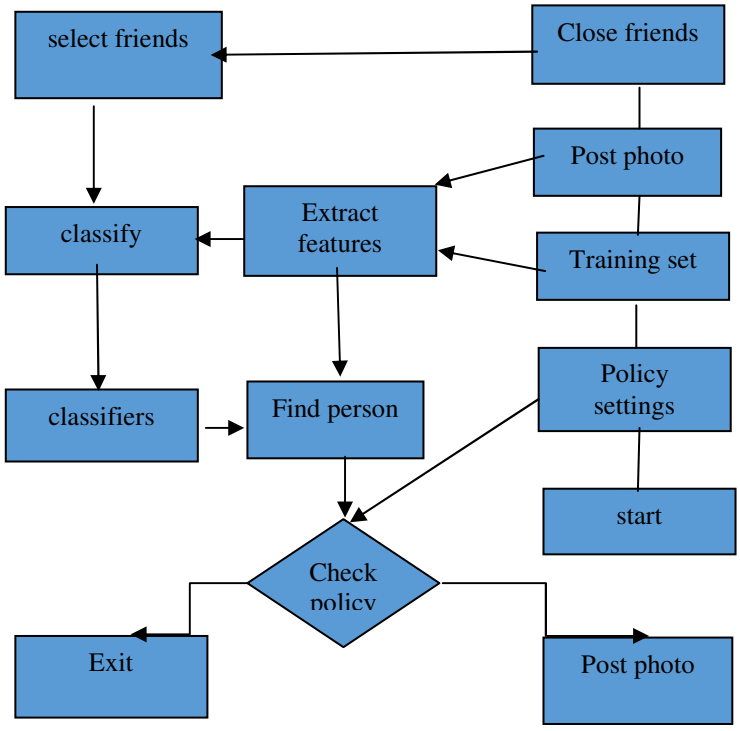

Fig1: Proposed System Architecture

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

4.Proposed system

A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works in three modes: a setup mode, a sleeping mode and a working mode. Running in the setup mode, the program is working towards the establishment of the decision tree. For this purpose, the private training set Xi and neighborhood Bi need to be specified. Xi could be specified by the user with the button "Private training set". When it is pressed, photos in the smart phone galleries could be selected and added to Xi. To setup the neighborhood Bi, at this stage, a user needs to manually specify the set of "close friends" among their Facebook friends with the button "Pick friends" as their neighborhood. According to the Facebook statistics, on average a user has 130 friends, we assume only a small portion of them are "close friends". In our application, each user picks up to 30 "close friends". Notice that all the selected friends are required to install our application to carry out the collaborative training. With Xi and Bi specified, the setup mode could be activated by pressing the button "Start". Key operations and the data flow in this mode are enclosed by a yellow dashed box on the system architecture.

During the training process, a socket is established exchange local training results. After the classifiers are obtained, decision tree is constructed and the program switches from the setup mode to the sleeping mode. Facebook allows us to create a list of friends such as "close friends" or "Acquaintances". We can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner's privacy policy and co-owners' exposure policies. However, in Facebook API, friend lists are read-only items, they cannot be created or updated through the current API. That means we cannot customize a friend list to share a co-photo. Currently, when the button "Post Photo" is pressed, co-owners of x are identified, then notifications along with x are send to the co-owners to request permissions. If they all agree to post x, x will be shared on the owner's page like a normal photo. In this sense, users could specify their privacy policy but their exposure policies are either everybody on earth or nobody depending on their attitude toward x. The data flow for a photo posting activity is illustrated by the solid red arrows. After the requests are sent out, the program will go back to the sleeping mode. If Xi or Bi is modified, the program will be invoked to the setup mode. In this case, the operations in the yellow dashed box will be performed again and decision tree will be updated.

Privacy policy and exposure policy:

In this paper, we assume that each user i has a privacy policy $P_i(x)$ and a exposure policy $V_i(x)$ for a specific photo x. The privacy policy $P_i(x)$ indicates the set of users who can access photo x and exposure policy $V_i(x)$ 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:

$$S = P_i(x) \backslash {}_{k2I} V_k(x)$$

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 [6] 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.

Face Recognition 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 [7]. 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 neighbors. 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[8]:

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.

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

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

large amount of useful information which could be utilized as a priori knowledge to help the facial recognition[9]. In [10], 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 co photos, the FR engine could focus on a small portion of "close" friends (friends who are geographically close and interacting frequently with user i).

5. Experimental Outputs:

The outputs taken in various stages during the implementation are presented below.

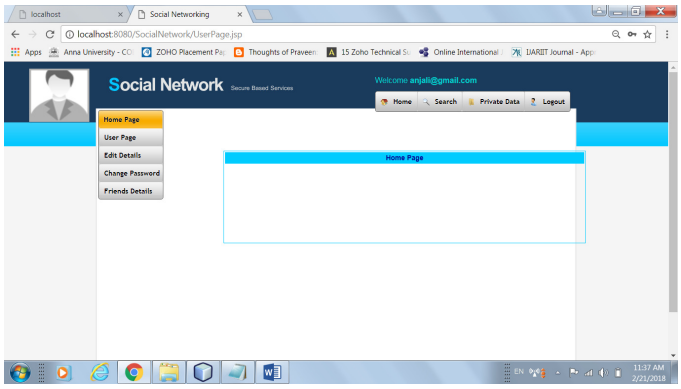

Fig 2. Home Page of the Proposed System

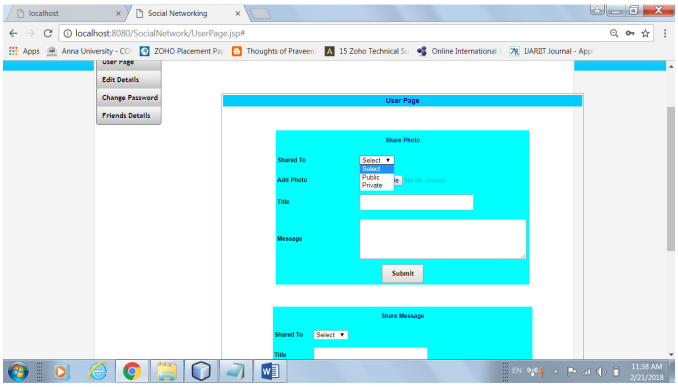

Fig 3. Sharing Photo's and message's

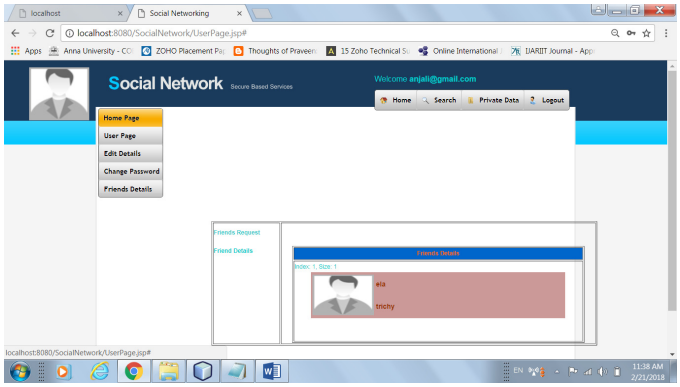

Fig 4. Friend's details

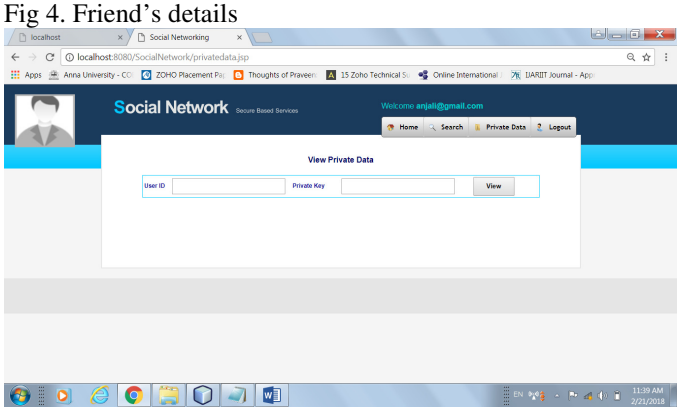

Fig 5. Extract the private data

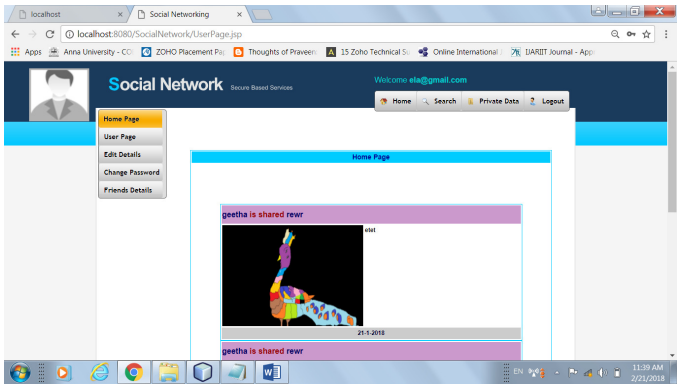

Fig 6. View the private data

6. Conclusion

The very big issue that everyone of us is facing in social media is privacy. The mechanism is implemented as a proof of concept Android application on Social media's platform.This system is mainly developed for the security of womens.

7.References

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. IV, Issue III, March 2018

[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 SIGCHIConference on Human Factors in Computing Systems, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM

[3] 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.

[4] 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.

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

[6] 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

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

[8] 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.

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

[10] 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