Control of Photosharing on Social Networks

Balaji Thangaraj.B[1], Annamalai.P[2], Manjith.R[3], Chakravarthy.P[4], Radha.N[5]
[1, 2, 3, 4] Dept of CSE
[5]Assistant Professor, Dept of CSE
[1, 2, 3, 4, 5] Saranathan college of Engineering,Trichy,Tamilnadu

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. Photos are uploaded in social networks. Sharing such photos is an important feature & most users do that. But this sharing is subjected to be limited to a particular group. However photos are leaked by some malicious users. The focus here is to prevent such photo leaks to unauthorized users. To deal with this dilemma and to prevent privacy leakage of photos of a particular member in a computationally cost effective manner and to devise a mechanism which provides a proper permission granting model before posting the photo. The mechanism attempts to utilize users' private photos to design a personalized 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. The system is superior to other possible approaches in terms of recognition ratio and efficiency.*

I. INTRODUCTION

SNS have become integral part of our daily life 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 co-photo 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 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.

II. LITERATURE REVIEW

2.1 THE PRIVACY RISKS OF SOCIAL NETWOKING SITES: David Rosenblum

For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information.

Autotagging Facebook: Social network context improves photo annotation
Zak Stone ; Todd Zickler ; Trevor Darrell

Most personal photos that are shared online are embedded in some form of social network, and these social networks are a potent source of contextual information that can be leveraged for automatic image understanding. In this paper, we investigate the utility of social network context for the task of automatic face recognition in personal photographs. We combine face recognition scores with social context in a conditional random field (CRF) model and apply this model to label faces in photos from the popular online social network Facebook, which is now the top photo-sharing site on the Web with billions of photos in total. We demonstrate that our simple method of enhancing face recognition with social network context substantially increases recognition performance beyond that of a baseline face recognition system.Zak Stone ; Todd Zickler ; Trevor Darrell.

2.2 COLLABORATIVE FACE REGOGNITION FOR IMPROVED FACE ANNOTATION IN PERSONAL PHOTO COLLECTIONS SHARED ON ONLINE SOCIAL NETWORKS:

Jae Young Choi ; Wesley De Neve ; Konstantinos N. Plataniotis ; Yong Man Ro

Using face annotation for effective management of personal photos in online social networks (OSNs) is currently of considerable practical interest. In this paper, we propose 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, we 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, we devise 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. Further, we demonstrate that our collaborative FR framework has a low computational cost and comes with a design that is suited for deployment in a decentralized OSN.

Rule-Based access control for social networks
Barbara Carminati, Elena Ferrari, Andrea Perego

Web-based social networks (WBSNs) are online communities where participants can establish relationships and share resources across the Web with other users. In recent years, several WBSNs have been adopting Semantic Web technologies, such as FOAF, for representing users' data and relationships, making it possible to enforce information interchange across multiple WBSNs. Despite its advantages in terms of information diffusion, this raised the need of giving content owners more control on the distribution of their resources, which may be accessed by a community far wider than they expected. In this paper, we present an access control model for WBSNs, where policies are expressed as constraints on the type, depth, and trust level of existing relationships. Relevant features of our model are the use of certificates for granting relationships' authenticity, and the client-side enforcement of access control according to a rule-based approach, where a subject requesting to access an object must demonstrate that it has the rights of doing that.

2.3 A COLLABORATIVE FACE RECOGNITION FRAMEWORK ON A SOCIAL NETWORK PLATFORM:

Kwontaeg Choi ; Hyeran Byun ; Kar-Ann Toh

Face recognition has many useful applications spanning surveillance, law enforcement, information security, smartcard and entertainment technologies. Very recently, a learning based face recognition system is also seen to be applied to web platform combining face recognition and web service. However, many existing methods which focused on recognition accuracy cannot cope with the new social network platform because the adopted static learning approach is not adaptive to daily updated photographs among the massive number of users. In this paper, we discuss the difference between a stand-alone based system and a social network based system and propose a new collaborative face recognition framework where a redundant tagging can be avoided via sharing the identification information for efficient update under the social network platform. Our Experiments (including a web stress test) using a public database show that the proposed method records a better accuracy than that of the state-of-the-art classifier SVM adopting a polynomial kernel and has fast execution time for both training and testing.

2.4 FRIENDS WITH FACES : HOW SOCIAL NETWORKS CAN ENHANCE FACE RECOGNITION AND VICE VERSA:

Mavridis, Nikolaos; Kazmi, Wajahat; Toulis, Panos

The "friendship" relation, a social relation among individuals, is one of the primary relations modeled in some of

the world's largest online social networking sites, such as "Facebook." On the other hand, the "co-occurrence" relation, as a relation among faces appearing in pictures, is one that is easily detectable using modern face detection techniques. These two relations, though appearing in different realms (social vs. visual sensory), have a strong correlation: faces that co-occur in photos often belong to individuals who are friends. Using real-world data gathered from "Facebook," which were gathered as part of the "FaceBots" project, the world's first physical face-recognizing and conversing robot that can utilize and publish information on "Facebook" was established. We present here methods as well as results for utilizing this correlation in both directions. Both algorithms for utilizing knowledge of the social context for faster and better face recognition are given, as well as algorithms for estimating the friendship network of a number of individuals given photos containing their faces. The results are quite encouraging. In the primary example, doubling of the recognition accuracy as well as a six fold improvement in speed is demonstrated. Various improvements, interesting statistics, as well as an empirical investigation leading to predictions of scalability to much bigger data sets are discussed.

2.5 MOVING BEYOND UNTAGGING: PHOTO PRIVACY IN A TAGGED WORLD
Andrew Besmer, Heather Richter Lipford

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. In this paper, we examine privacy concerns and mechanisms surrounding these tagged images. Using a focus group, we explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. We 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.

Moving beyond untagging: Photo privacy in a tagged world | Request PDF. Available from: https://www.researchgate.net/publication/221515830_Moving_beyond_untagging_Photo_privacy_in_a_tagged_world [accessed Mar 26 2018].

2.6 Collective privacy management in social networks
Anna Cinzia Squicciarini, Mohamed Shehab, Federica Paci

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. In this paper, we model the problem of collaborative enforcement of privacy policies on shared data by using game theory. In particular, we propose a solution that offers automated ways to share images based on an extended notion of content ownership. Building upon the Clarke-Tax mechanism, we describe a simple mechanism that promotes truthfulness, and that rewards users who promote co-ownership. We integrate our design with inference techniques that free the users from the burden of manually selecting privacy preferences for each picture. To the best of our knowledge this is the first time such a protection mechanism for Social Networking has been proposed. In the paper, we also show a proof-of-concept application, which we implemented in the context of Facebook, one of today's most popular social networks. We show that supporting these type of solutions is not also feasible, but can be implemented through a minimal increase in overhead to end-users.

III. MODULE IMPLEMENTATION

3.1 OSN CONFIGURATION:

The online social media information filtering techniques are used to remove unwanted contents by using customizable content based filtering rules, Machine learning approach; according to user's interest and recommends an item.

A user post (a truncation of the expression weblog post) is a discussion or informational site published on the World Wide Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). All the blog posts were usually the work of a single individual, occasionally of a small group, and often covered a single subject. More recently "multi-author blog posts" (MABs) have developed, with posts written by large numbers of authors and professionally edited.

A majority are interactive, allowing visitors to upload photos each other via GUI widgets on the blogs, and it is this interactivity that distinguishes them from other static websites.

3.2 NEW USER REGISTRATION MODULE

3.2.1 UNIQUE IDENTITY

First the new user who wants to access is given a unique identity. The unique identity provided to each and every user is the problem provided by the new user module. This enables to take the new user to the next step that is key generation. First the users who want to post register in this module. The users give their data like name, address, city, pincode, contact and email id to the form. All the details are stored in the SQL Database Server. So only after the registration is complete a message is delivered to the user that he has been successfully accommodated into the system as a user. The users then may be redirected to the posting module, where they may post contents with title and category. Thus the registration phase is an important part of the user for logging into the system.

3.2.2 KEY GENERATION

A unique secret key for this user is generated and sent to the cloud. The other component We will have to worry about is the actual key that is used to encrypt and decrypt. The key must be such that it is not easily guessed, and since no one is expected to remember it, it may not be a string of human comprehensible characters. It can be just any arbitrary string of characters. The best option to generate a key is using the new code segment DES3GetKey in the package dbms_obfuscation_toolkit. As in all other codes in this package, the DES3GetKey code is also implemented as both a procedure and a function and overloaded with both VARCHAR2 and RAW datatypes. The parameters to the procedure version in the RAW format is then processed.

5.2.3 CLASSIFY

In content based filtering to check the user's interest and previous activity as well as item uses by users best match is found . For example OSNs such as Facebook, Orkut used content based filtering policy. In that by checking users profile attributes like education, work area, hobbies etc. suggested friend request may send. The main purpose of content based filtering, the system is able to learn from user's actions related to a particular content source and use them for other content types.

In collaborative filtering information will be selected on the basis of user's preferences, actions, predicts, likes, and dislikes. Match all this information with other users to find out similar items. Large dataset is required for collaborative filtering system. According to user's likes and dislikes

In policy based filtering system users filtering ability is represented to filter wall messages according to filtering criteria of the user. Twitter is the best example for policy based filtering. In that communication policy can be defines between two communicating parties.

It is in this module that the abusive posts and words are entered and the system is trained to filter the posts in the social media using these words as rules. The Filtering Rules are customizable by the user. User can have authority to decide what contents should be blocked or displayed on his wall by using Filtering rules. For specify a Filtering rules user profile as well as user social relationship will be considered. Author is a person who defines the rules. User Spec denotes the set of OSN user. Content Spec is a Boolean expression defined on content.

3.2.4 IDENTIFY

If the photos content is not found to be shared by the owner then they are not shown. A message by is sent to the user of the post. The list is maintained for the words which have been trained by the users to get hold of the abusive and explicitly destructive content which should not be seen and may cause damage to other users. It may also lead to unnecessary altercations and erupt into full-fledged clashes. Thus blacklisting helps in reducing such notoriety from spreading its wings.

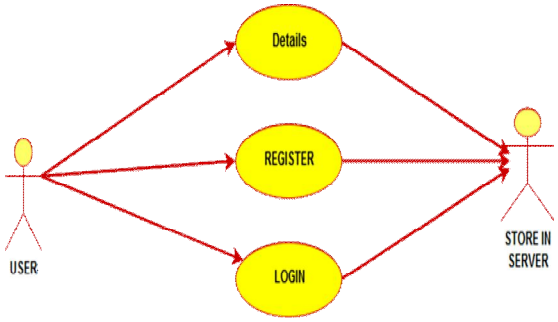
3.2.5 SHARE AND REVOKE

Such photos will be deleted by the admin of the social network system. Further continuance by the users to be abusive will be dealt with severely by terminating all their posts. The post and its contents along with the title will be removed permanently from the system and other users will not be able to see it. The users will further be scrutinized so that they do not cause any damage to the system. The posts thus revoked will be deleted from the SQL Server table also so that it may not crop up in the future. Cloud Servers store all the secret key components of SK except for the one corresponding to the dummy attribute AttD. Such a design allows Cloud Servers to update these secret key components during user revocation as we will describe soon. As there still exists one undisclosed secret key component (the one for AttD), Cloud Servers cannot use these known ones to correctly decrypt ciphertexts. Actually, these disclosed secret key components, if given to any unauthorized user, do not give him any extra advantage in decryption as we will show in our security analysis. Here the key is verified for the user. It is in this module that the absolute verification is done to ensure the secure transmission of the data. If verification fails than the transmission is stopped and further processing is aborted.

IV.SOFTWARE REQUIREMENTS

USE CASES:

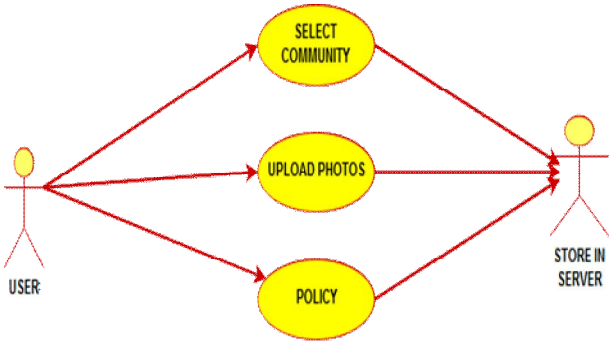
1. User Registration In Webserver



DESCRIPTION

First the users register themselves in the system by providing their details which are stored in the data store. The users are provided ids using which they login to the web server. The server then allows the registered user to upload data and other content like photos.

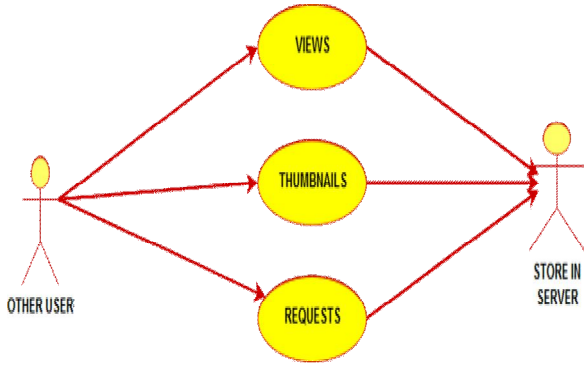
2. Join Community and Upload Data



DESCRIPTION

The registered users upload photos in the server. They may select community for which they have interest and join the groups. The photos are uploaded and stored in the server. The users may set policies for their groups which they join.

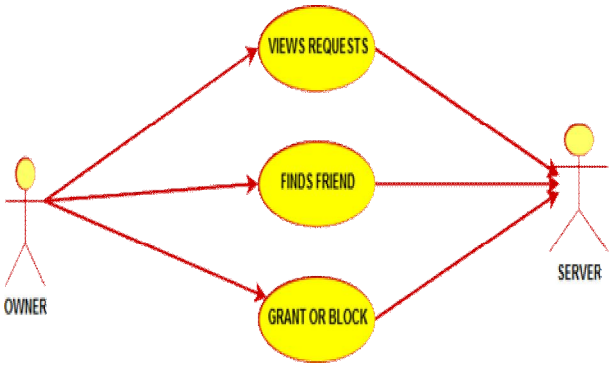
3. USERS VIEW DATA OF OTHER GROUPS AS THUMBNAILS



DESCRIPTION

The other users upload when they join groups may view the photos as thumbnails. If they like the thumbnail they may request. The requests are sent to the server. The requests are sent to the owner of the photo data.

4. PROCESS REQUEST AND GRANT OR REVOKE POLICY



DESCRIPTION

The owner views requests and the algorithm generates policies based on the friend of friend requests or to which community they belong. The policy verifies if the request is a friend or unknown quantity or a affiliated group.

3.4 FUNCTIONAL REQUIREMENTS:

1. User Registration In Webserver

Use case name	User Registration In Webserver
User	Details are registered
Register	Data are stored in the server
Login	The users login to the system.
Reference	Fig 1

2. **Join Community and Upload Data**

Use case name	Join Community and Upload Data
Community	Selects Community or groups
Uploads Photos	Uploads data and photos
Policy	User fixes policy
Reference	Fig 2

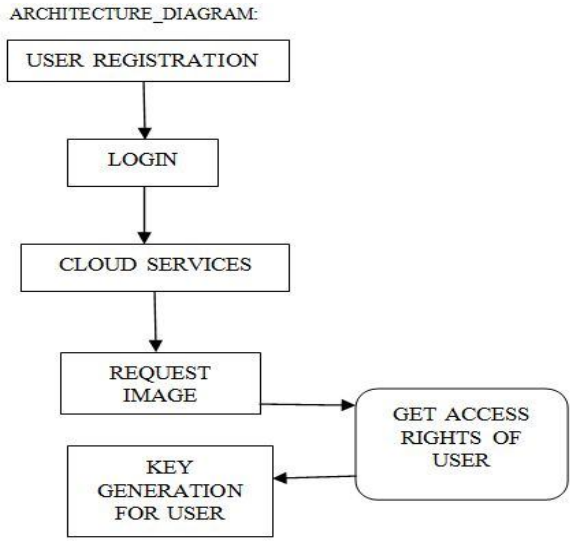
3. Other users view Photos and Request

Use case name	Other users view Photos and Request
Views	Views Similar Content Uploaded by users
Thumbnails	Views other users photos as thumbnails.
Requests	If required places request
Reference	Fig 3

4. PROCESS REQUEST AND GRANT OR REVOKE POLICY

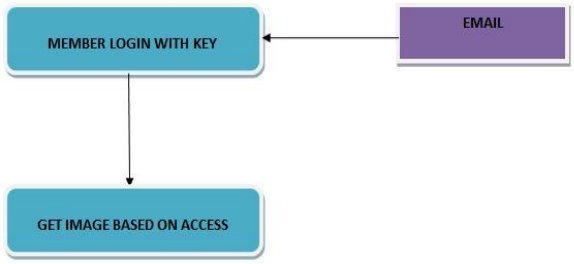
Use case name	Process Request And Grant Or Revoke Policy
View Requests	The system views the requests
Find Friends	Finds if the request is a friend of friend or not.
Grant or Block	The system grants the request or blocks based on the algorithm.
Reference	Fig 4

V. DESIGN MODEL



:

GET KEY FROM EMAIL:



VI. TESTING

6.1 INTEGRATION TESTING:

Integration Testing means set of components interaction between the modules. In this system perform the integration testing on the one module to another module.

Test Report:

Module Name 1: **PICTURE UPLOAD** Module name 2: **PICTURE DISPLAY**

Sno	Input(s)	Expected Output	Obtained Output	Error details	Type of error	Solution
1.	Picture	Display and View Uploaded Pictures	Displayed Pictures	No Error	Nil	Correctly Integrated Pictures and Displayed

6.2 Validation Testing:

Validation is the checking or testing of items, includes software, for conformance and consistency with an associated specification. Validation is the process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Module: User Login and User Menu

S.No	Input	Description	Expected output	Actual output
1.	User Id	Invalid User Id	Valid / invalid	Wrong Id
2.	Password	Invalid Password	Valid / Invalid	Wrong Password Error

PROPOSED MODEL

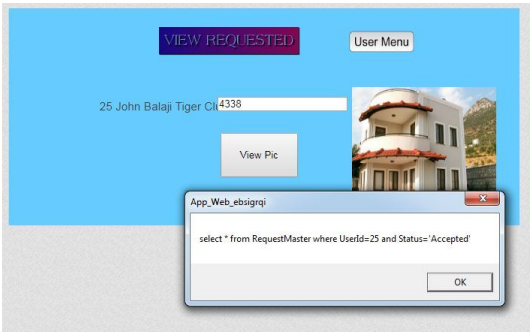
Users are classified as friends. So essentially a friend is a friend of a friend theory is established. A user needs to coordinate all friends to build classifiers in a OSN. This classifier acts as a bridge between them. A Self friend and friend known to the two. This ensured that friends only communicate with each other. So any unknown person will not be able to misuse shared data. Thus privacy is preserved. 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.

VIII. CONCLUSION

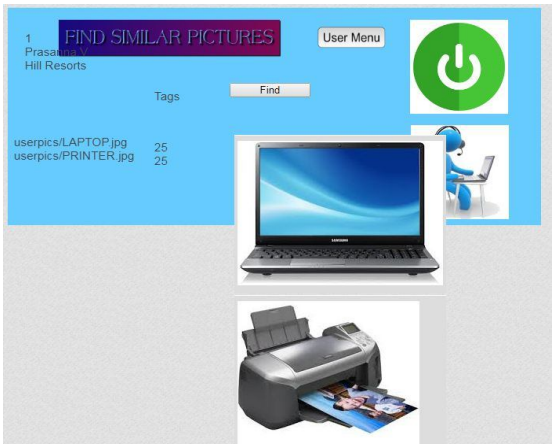
Thus the proposed model is very effective for OSN users. Helps in data privacy of the individual. The decision to share the photo or data rests with the user. Provides a mechanism for effective control over what is to be shared and between whom using classifiers. Photo sharing is one of the most popular 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, proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. The proposed privacy-preserving system is novel and has less computational overheads. 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. The proposed scheme is very useful in protecting users' privacy in photo/image sharing over online social networks. However, there always exist trade-off between privacy and utility. Latency introduced in this process will greatly impact user experience of OSNs.

SCREENSHOTS OF MODULE:

REQUESTED IMAGE MODULE



CODE REQUEST FOR IMAGE



SIMILAR PICTURES MODULE

REFERENCES

[1] A. Besmer, H. Richter Lipford, "Moving beyond untagging: Photo privacy in a tagged world", *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, pp. 1563-1572, 2010.
Show Context Access at ACM

[2] S. Boyd, N. Parikh, E. Chu, B. Peleato, J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers", *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1-122, Jan. 2011.
Show Context CrossRef

[3] B. Carminati, E. Ferrari, A. Perego, "Rule-based access control for social networks", *Proc. Int. Conf. On Move Meaningful Internet Syst. Workshops*, pp. 1734-1744, 2006.
Show Context CrossRef

[4] J. Y. Choi, W. De Neve, K. Plataniotis, Y.-M. Ro, "Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks", *IEEE Trans. Multimedia*, vol. 13, no. 1, pp. 14-28, Feb. 2011.
Show Context View Article Full Text: PDF (1731KB)

[5] K. Choi, H. Byun, K.-A. Toh, "A collaborative face recognition framework on a social network platform", *Proc. 8th IEEE Int. Conf. Autom. Face Gesture Recog.*, pp. 1-6, 2008.
Show Context