JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Secure and Efficient method for Sharing Privacy Images on Social Media

Narayana Rajashekar Reddy, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana
Satyanarayana, Professor, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana
Koraveri Vijay, Professor, Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana

Abstract - With the development of social networking technology, sharing images on online social networks has become a popular way for users to interact with others. However, the abundance of information in the image makes it easy for the viewer to capture sensitive information about what is shown in the image. In recent years, a lot of attention has been paid to how it handles privacy issues that arise when sharing photos. When sharing photos with multiple users, the photographer must take into account the privacy of all users involved. In this document, we recommend a privacy policy based on the credibility of sharing personal photos. The basic idea is to hide the identity of the original image so that users who have lost their privacy as a result of sharing the image will not be identified from the anonymous image. The user's loss of privacy depends on how much he trusts the recipient. Loss of privacy affects consumer trust in publishers. Anonymous image results are verified with the link provided by the publisher. We provide publishers with a careful approach with publishers to strike a balance between anonymity and integrity of information shared by others. The imitation results suggest that a reliable method of sharing images can help reduce drive loss, and the recommended method of adjusting the version value can ensure better distribution to users.

1. INTRODUCTION

Social networks that allow people to interact with the creation and exchange of information have now become an integral part of our daily lives. Users of social networks create a lot of information through texts, digital images or videos. User-generated content is the driving force behind social networks. However, user-generated content often contains confidential information of the producer; in other words, sharing such content may jeopardize the creative unit. How to deal with privacy issues resulting from information sharing has long been an active topic in social media research. An important way to share content on social networks is to share digital images. Some popular social networking sites like Instagram1, Flicker2, and Pinterest3 are designed for photo sharing. Depending on the caption text, images may provide the viewer with more information, posing a privacy risk. Also, future image information can be used by poor viewers to obtain sensitive information. The advantage is that it makes it easy for users to hide sensitive information without destroying it by creating images (like blocks) instead of editing text.

In this article, we explore the privacy issues that arise when sharing images on a social network (OSN). OSN's current privacy policy is primarily concerned with how service providers analyze user information and how users can control how information is shared. Most OSN users offer privacy options. Users, in general, can specify which users can access shared images based on their interactions with others. Please note that images shared by one user may be linked to other users. If the sharing of such images is under the control of a single user, the privacy of other related users may be compromised.

2. LITERATURE SURVEY

Privacy Suites: Shared Privacy for Social Networks

Creating clear and transparent privacy management is a major challenge for social networks. Understanding user privacy settings may result in intentional disclosure of personal information and, in some cases, damage to your home. We offer a new concept that allows users to "easily" set up privacy settings provided by trusted friends or experts and modify them whenever they want. Since most users now maintain the special settings selected by the operator, such a system can significantly improve the privacy of many users with minimal investment.

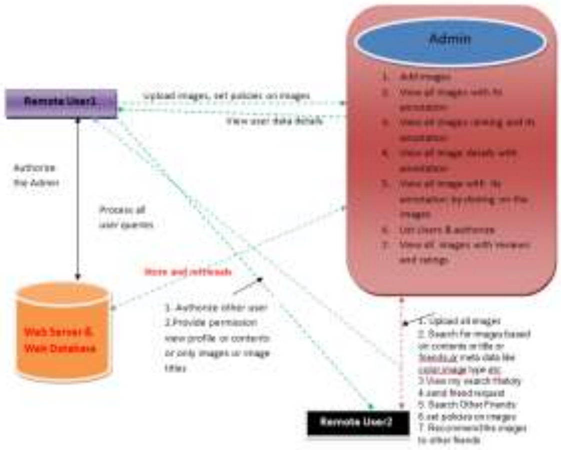
SheepDog – Group and Tag Recommendation for Flickr Photos by Automatic Search-based Learning

Online photo albums have become popular in recent years and have led to more apps enabling photo sharing. In this document, we recommend a system called SheepDog that automatically puts images into matching groups and provides matching tags to Flickr users. We have adopted conceptual definitions to predict related concepts from images. From the moment we collect training data through page search, we recommend two approaches and evaluate the impact of conceptual definitions. Flickr has used the classification method based on some of the available data, not only to provide reliable training data but also to provide useful group/label recommendations for the images contained. We evaluated this system with rich images, the results of which show the impact of our work.

Personalizing Image Search Results on Flickr

The Flickr social network allows users to upload photos, track tags, group posts, and create social networks to connect with other users. Flickr offers several ways to browse or search. Possibility of search tags that return all images that have been identified with a special key. If a keyword contains two keywords, such as a bug or a "bug" machine, the tag search results contain multiple images that are not related to the user's game when asked. We urge users to express their interest in photography through the metadata they add to contact forms and comments on images. We show you how to use this metadata to improve search results for users and thus improve search results. First, we suggest that we can significantly improve search accuracy by filtering user-friendly links or large social networks that will have this link. Second, we present an example of a possibility that uses tag information to identify hidden topics that are not in search results

3. SYSTEM ANALYSIS:


Admin
1. Add images
2. View all images with its annotation
3. View all images ranking and its annotation
4. View all image details with annotation
5. View all image with its annotation by clicking on the images
6. List Users & authorize
7. View all images with reviews and ratings
Remote User1
Upload images, set policies on images
View user data details
Authorize the Admin
Process all user queries
Store and retrieve
Web Server & Web Database
1. Authorize other user
2.Provide permission view profile or contents or only images or image titles
1. Upload all images
2. Search for images based on contents or title or friends or meta data like color image type etc
3 View my search History
4 send friend request
5. Search Other Friends
6 set policies on images
7. Recommend the images to other friends
Remote User2

System Architecture

3.1 Existing System

- Yuan et al. have introduced a secure photo-sharing system that uses photo sharing technology to protect user privacy. When printing an image, the proposed system captures the content and frame of the image. [13] Xu et al. has developed a mechanism that allows all relevant photo users to participate in photo sharing decisions. Using facial recognition techniques, they develop distributed reconciliation strategies to make final decisions. [14] Ma et al. based on the encoding algorithm found. offer a valid management plan to verify and eliminate the user configuration to access multilingual data [15].
- With photo production techniques, we can better manage privacy for photo sharing. [16] Ilia et al. An access control structure for image management is proposed, where images are transferred to a set of layers, each with a grid surface. Depending on each user's privacy policy, the final image sent to the viewer will be delivered with a special overlay.
- Lee et al. The proposed framework for multi-image OSN image sharing allows you to gradually adjust the accuracy of access control from the image level to the surface level. In [18] Vishwamitra et al. To share photos on OSN, participants' image management methods are recommended. The proposed approach focuses on personal data (PII) in images and the development of conflict resolution strategies for access control policies at the PII level. The photo-sharing process described in this document is also intended to protect user privacy. Unlike previous research, the approach proposed in this paper does not use access control principles to allow each user to decide whether to share an image. Instead, the provider assesses each affected user's privacy loss and then decides which ones to protect.
- Private Social Networking Sites by Datta et al. [20] Users can inform other more trusted users to maintain their profile. Based on capacity management policies provided by other users, users can decide with whom and with whom to share sensitive information. Dinah [21] Rathore et al. proposed a framework for access management based on the reliability of resource allocation. The model complies with the license requirements for all relevant users. And client trust is used to resolve disputes between different capacity control policies.
- Gay et al. have introduced an access-based management system that allows users to control how their data is distributed. They develop loyalty models to evaluate customer relationships. [23] Yu et al. Deep study principles to determine the privacy settings for photo sharing.

3.1.1 Disadvantages

- There is no access control, according to the ban on sharing photos on social networks.
- Border security due to lack of adequate confidentiality in the exchange of photographs.

3.2 Proposed System

- Under the recommendation, the system focuses on image sharing, where the user, called the printer, decides how the image will be stored to protect each user's privacy. A reasonable process is recommended to help publishers make the right decision. Unlike our previous work [10], editors do not communicate with other relevant users before posting an image. Instead, if the images are shared by specific users, the publisher will lose the privacy of each user.
- A system that monitors trust between users to measure identity loss. The basic premise is that whether a user lets another user know their sensitive information depends on how trustworthy the previous user was. Whether a user wants to protect another user's privacy or not depends on how much trust the user has in advance in the other user. Basically, if the publisher predicts a high level of privacy loss for a relevant user, whom the publisher also

trusts, the publisher "searches" for the user by removing the relevant image space from the image.

- Relevant users are directly involved in the editorial decision-making process. After the image has been processed and sent to a recognized user by the printer, each connected user can assess whether his or her privacy has been compromised. When users lose their privacy, they lose confidence in the publisher. And if you know that a publisher protects their privacy, you can trust him more. Because of the relationship between privacy and trust, editors ignore other users' privacy when sharing images.
- Intuitively, if the editor removes all users from the image, no one will lose their privacy and the editor will be more reliable than others. Thus, the publisher's integrity is respected more than other users'. But after deleting all user information, photo sharing becomes free. The proposed method includes a clause that controls the number of users removed from the image. To find a balance between privacy and image sharing, we offer an approach to personify boundaries and trust relationships between users. The main parts of this work are:
- OSN provides a reliable image-sharing mechanism. User loyalty value is used to determine if users' privacy is protected. Updated trust values based on loss of privacy and recommended systems will prevent users from ignoring other users' privacy.
- To balance image sharing and integrity, we provide static adjustments that determine the number of users that have been removed from an image.
- The system performed a series of simulations to demonstrate the effect of the proposed technology.

3.2.1 ADVANTAGES

- Kir Increased security by not recognizing trusted images and privacy principles.
- There is a frame that controls the number of users that have been removed from the image. To create a balance between privacy and image sharing, the system provides methods for managing data measurement and reliable relationships between users..

MODULES:

1. System Construction Module
2. Content-Based Classification
3. Metadata-Based Classification
4. Adaptive Policy Prediction:

MODULES DESCRIPTION:

System Construction Module

The A3P framework has two main components: A3P-based and A3P-social. The information flow usually looks like this. When the user uploads an image, the first image is sent on an A3P basis. Distributes important A3P images and identifies the need for A3P social networks. A3P often implements policies for large users based on their historical characteristics. If one of the following two conditions is met, the A3P key activates A3Psocial: (i) the user does not have sufficient information about the type of image sent to predict the policy; (ii) A3P-core recognizes significant changes in the user community due to increased user activity on social networks (but adding new friends, new profile posts, etc).

Content-Based Classification

To find image groups that are associated with the same privacy settings, we recommend a high-level image analysis that first sorts the image by its content and then filters each type according to its metadata in subgroups. Images without metadata are only collected by content. This standard analysis further reflects the image content and minimizes the effects of lost waves. Note that some images may fall into more than one category if they have common content properties or metadata of that type.

Our approach based on fairness in content distribution is effective and accurate. Specifically, our shared code collects image signals that are identified by a numerical and enhanced version of the Haar wave conversion. For each image, file transfer depends on color, size, conversion variation, shape, texture, symmetry, and so on. Encrypts the frequencies associated with location information from the image. A small number of partners are then selected to create an image profile. The similarity in the content between the images is then determined by the distance between the image signatures.

Metadata-Based Classification

The metadata-based classification of images is based on the main categories defined above in subcategories. The process consists of three main steps. The first step is to get the keywords from the metadata associated with the image. The metadata considered in our case are tags, profiles, and comments. The next step is to obtain a representative hyperbole (defined by h) from each metadata vector. The third step is to search for subcategories that contain images. This is an additional process. First of all, the first image as an image itself constitutes a category and represents the image in the form of a hypernum to represent the category definition.

Adaptive Policy Prediction

The policy prediction code contains the predicted policy for the new image sent to the user for reference. More importantly, the proposed policy indicates any changes to user privacy. The forecasting process consists of three main steps: (i) policy validation; (ii) mining policy; and (iii) policy forecasting.

4. OUTPUT RESULTS:

Fig 4.1: Admin Page

Fig 4.2: User Tweets Page

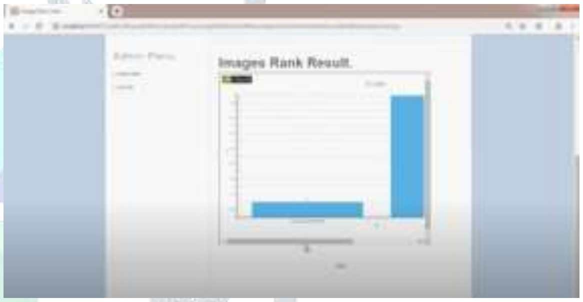


Fig 4.3: Image Rank Results Page

5. CONCLUSION

Sharing photos of friends on OSN can compromise the privacy of many users. To solve this privacy issue, we provide a secure image sharing mechanism in this document that uses trusted values to judge how to encrypt images. Your service provider temporarily saves the image you want to share. Based on the trust relationship between users, the provider assesses the level of work associated with the loss of image privacy. By comparing the loss of integrity with the limits set by publishers, service providers decide to remove people from the picture. After sharing the photos, each participant assesses the loss of privacy and exchanges confidence in it with the editor accordingly.

This trust approach encourages publishers to stick together. However, anonymous operations may result in the loss of shared information. Since publisher standards manage the balance between confidentiality and information sharing, we propose a vendor-assisted approach to help publishers achieve higher standards. Using standard network data and real-time network data, we create a series of simulations to test the proposed image sharing process and constrained installation techniques. The false results suggest that incorporating trust values into the privacy process helps reduce user privacy and requires maximum tuning to help publishers create a balance between privacy and photo sharing. In this lesson, we will focus primarily on the relationship between the publisher and the recipient. Since users often share photos with multiple users at the same time, we want to explore one or more examples in future posts.

The proposed method of setting higher standards can be seen as policing, whereby publishers are more likely to choose fast bandwidth for distribution. Due to the relationship between unit loss and reliability value, the maximum current choice affects the dealer's future distribution. In our future work, we want to explore how reduction techniques can be adapted to achieve better results.

REFERENCES

[1] W. G. Mangold and D. J. Faulds, “Social media: The new hybrid element of the promotion mix,” Business horizons, vol. 52, no. 4, pp. 357–365, 2009.

[2] A. M. Kaplan and M. Haenlein, “Users of the world, unite! the challenges and opportunities of social media,” Business horizons, vol. 53, no. 1, pp. 59–68, 2010.

[3] J. A. Obar and S. S. Wildman, “Social media definition and the governance challenge-an introduction to the special issue,” 2015.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, “Information security in big data: Privacy and data mining,” IEEE Access, vol. 2, pp. 1149–1176, 2014.

[5] S. K. N, S. K, and D. K, “On privacy and security in social media a comprehensive study,” Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211

[6] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, “What (or who) is public?: Privacy settings and social media content sharing,” in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.

[7] A. C. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.

[8] H. Hu, G.-J. Ahn, and J. Jorgensen, “Detecting and resolving privacy conflicts for collaborative data sharing in online social networks,” in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.