International Journal of Research in Advent Technology (E-ISSN: 2321-9637) Special Issue
National Conference "NCPCI-2016", 19 March 2016
Available online at www.ijrat.org

Privacy Policy Recommendation for Images On SNS

Jayashree Walunj[1], Bharat Burghate[2]
Department of Computer Engineering[1,2,3]
BhivrabaiSawant Institute of Technology & Research Pune, India
Email: jayashree_patait@yahoo.co.in[1]
bharatburghate@gmail.com[2]

Abstract: In this era, there is an increasing wave of image sharing via social media sites. Though image sharing is the need of users or most favorite activity of users on social networking sites, ensuring the privacy of images is becoming critical.There have been many recent reported occurrences where users unintentionally shared personal data. By looking at the increasing rate of such incidents there is a high need for tools to provide privacy to the content that user share on social media sites. For this need, we tend to propose a system which recommends Privacy Policies for user-uploaded images on social media sites.We tend to examine the role of social context, image content, and Metadata as potential indicators of user's privacy preferences. We tend to propose a two-level framework that in keeping With the users accessible history determines the most efficient privacy policy for the user's pictures being uploaded. Our resolution depends on an image classification framework for image classes which can be related to similar policies, And on a policy prediction algorithmic program to automatically generate a policy for every freshly uploaded image, additionally in keeping with users social options. We also propose Decision Voting system to recommend the Privacy Policies at the individual level for the further security of images, Image Encryption is proposed. This ensures Conflict Resolution while assigning the policies at the individual level.

Keywords: Online information services, web-based services .

1. INTRODUCTION

In these days, Images are one of the key enablers of user's connectivity. Most of the times image sharing occur with known personnel like friends /families/coworkers etc. Sometimes it occurs with social groups or unknowns as well like Picasa, Flickr, Google+ circles. Using sharing with social groups, one tries and explores new individuals and also tries to know more about their likings or social aspects. It has been observed that content rich images reveal sensitive information. Consider a photograph of employees excellence annual award function 2016.It could be shared with friends/family over Facebook, Flicker group or Google+ circle. Although such photograph may superfluously uncover an employee's family members and friends. Thus, image sharing over social networking sites may rapidly lead to inappropriate exposure and privacy violations. Online Social sites follow the determined approach and hence makes it feasible for different users to gather rich summarized information about the proprietor of the shared images and it's content features. Such extracted information can unleash one's social characteristics and lead to exploitation of one's personal details. These days social media sites facilitate user to enter their privacy inclinations.Current systems that automate the privacy setting seemto be insufficient to handle the distinct privacy requirements of images, because of the intense inbuilt information within images, and their association with the online sites wherein they are shared. This paper elaborate and Adaptive Privacy Policy Recommendation system which is meant to facilitate users with efficient privacy setting.

2. LITERATURE SURVEY

A. Privacy Configuration

It has been seen that in last few years there is drastically high growth in subscriptions to social media sites such as Facebook, Myspace, etc. All these social media sites facilitate users with fascinating ways of getting social over the net. It has exponentially increased communications amongst people. But at the same time, they have shared the concern of one's privacy while sharing the information. It has done deep dive into privacy concerns and its impact on users social behavior.Through the means of the survey, it has gathered user's stated behavior and noted the actual behavior post the privacy related information exposure.[1][2]These days' users have moved from annotations to tags. Although there are many uses of annotations like in Flicker, it is used for social and personal use. Such annotations are also referred in recall and retrieval. Due to all these benefits, there is a high use of tagging. Here it analyzes different factors that users consider while tagging the pictures. An outcome of this analysis advises the implications for the design of the applications built on user based annotations. [3] Extensive research is conducted on benefits of social media sites for

sharing content. Few have done research on privacy issues of sharing images on social media. This research outcome is then used as a base to build the mechanism to provide the privacy to images shared via social networks. It explains several methods to enhance the privacy. Also, it does further research on how current privacy is not consistent with user's actual expectations. [4]

B. Privacy Prediction Systems

The system is proposed named Sheepdog which assists to put the pictures automatically into respective groups and then it recommend the appropriate tags for users on Flicker. They use concept detection to predict relevant concepts (tags) of an image. [5] Here it proposes recommendation system to connect picture content with online groups over social media site.It considers three different types of image features such as social interaction; text tags are given by users, visual characteristics. By considering this aspect it recommends most appropriate group for pictures uploaded. [6]It proposes automated recommendation system which recommends appropriate groups for images uploaded by users. There is a lot of research was done on customization and personalization of tag based Information Retrieval. This technique refers association rule mining. Also, it evaluates many collaborative filtering algorithms for the recommendation on groups for Flicker users. [7]

3. 2P RECOMMENDATION ARCHITECTURE

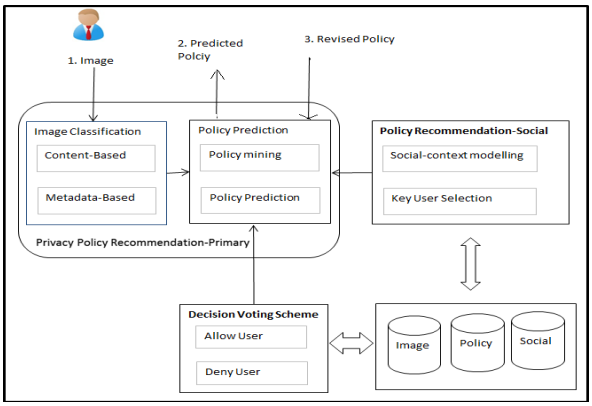
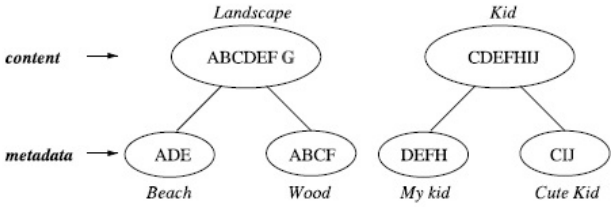


Fig 3. System Architecture

The 2P architecture system consists of two main components: 2P Recommendation-Primary and 2P Recommendation-social. Architecture functional flow is explained as below. User uploaded image will be first submitted to the 2P Recommendation -Primary. To begin with Image classification, categorize image and also decide if there is any necessity to call 2P Recommendation-social. Most of the times the 2P Recommendation -Primary analyze the user's history and predicts the privacy policies for the users uploaded images. The 2P Recommendation social will be called in below cases only (i) When there is not much history for given user to predict the policies (ii) When it detects major changes in user's privacy settings or when there is an increase in user's social activities like the heavy addition of new friends etc. In all these situations, it would be valuable to let the user know about the current privacy patterns of social groups which have a similar background as the user.

4. 2P RECOMMENDATION -PRIMARY

Within the Privacy Policy Recommendation-Primary there are two major components (i) Image classification and (ii) Policy prediction. Images uploaded by users on the social media site are grouped as per the content and metadata of the respective images. Later for each such group, privacy policies are analyzed for further prediction



A. Image Classification

Image classification follows the hierarchical image classification methodology where images are scanned for their content first as the first level of classification. In the second level, these images are further scanned for metadata. This method enables to extract image classes and further refined subclasses.

1) Content-Based Classification

Content-based classification is the first step where we derive classes as per the image contents. If the images do not have metadata, then it follows only contents for classification. In such manner, it minimized the impact of missing metadata.Image Classification techniques use the image color, shape, size, etc. features for classification. Also, then it calculates the similarity with existing image set and will determine the class for given image.

2) Metadata-Based Classification

This type of classification refines the images classes at second level if Hierarchical images classification process. To begin with keywords which are linked with given image are extracted. Then from the metadata vector, it determines the representative hypernym (h). Then at the end, it figures out the image subclass.

B. Adaptive Policy Prediction

Policy Prediction involves three important stages as follows: (i) policy normalization; (ii) policyMining; and (iii) policy prediction. This is responsible to predict the privacy policies for images uploaded by users. This algorithm also considers the privacy changes made by users from time to time.

1) Policy Mining

Privacy Policy mining follows association rules mining to find out repeating patterns in policies. Images in the same class usually carry similar privacy protection levels. This is Hierarchical mining which refers the sequential steps that users follows while defining the policies. These steps are nothing but to define who shall access the images (Subjects), what access privileges will be given to whom (actions) and at last whether there are any access conditions or restriction (conditions).

2) Policy Prediction

The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user. Thus, we present an approach to choose the best candidate policy that follows the user's privacy tendency.

5. 2P RECOMMENDATION-SOCIAL

The Privacy Policy Recommendation-social utilizes a multi-criteria inference mechanism that builds candidate policies by utilizing key information with respect to user's social context and his inclination towards privacy.

A. Modeling Social Context

Past research studies or surveys have derived that users who have common likings or common profile attributes have inclined to have similar privacy policies. Here it forms the social groups (SG) by mining the profile attributes progressively.

B. Identifying Social Group

Above step provide the social group (SG) for given user. Here it finds out the representative user from the identified social group. And then it sends out this User, his images, policies to Policy Prediction.

6. DECISION VOTING SYSTEM

This facilitates the privacy policy recommendation at individual level as well. If any exclusion at individual level is taken then that is considered for further policy prediction. This helps to provide more meaningful prediction. Here DV is decision voting value and Evaluation (p) represents the policy p decision.

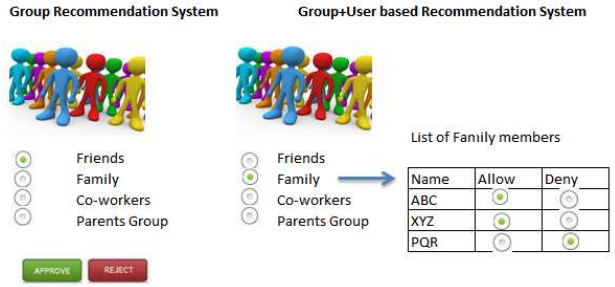


Fig. Decision Voting Mechanism

7. MATHEMATICAL MODEL

Let S is the Whole System Consist of
S = {I, P, O}
I = Input.
I = {U, Q, D, IMG}
U = User
U = {u1, u2 …. un}
Q = Query Entered by user
Q = {q1, q2, q3…qn}
D = Dataset.
IMG = Images
IMG = {img1, img2....img n}
P = Process:
P={PPR-CORE,PPR-Social,CBC,MBC,APP,PM,PP,SCM,PUS}
CBC = Content-Based Classification
MBC = Metadata-Based Classification
APP = Adaptive Policy Prediction
PM= Policy Mining
PP=Policy Prediction
SCM= Social Context Modelling
PUS=Pivotal User Selction
[Step1:] User enters the Query(Image).
[Step2:] Privacy Policy Recommmedation Primary (Classification and policy prediction)
[Step3:] Content Based Classification.
[Step4:] Metadata Based Classification.
[Step5:] Policy mining
[Step6:] Policy prediction
[Step7:] Social Context modelling.
[Step8:] Pivotal user selection.

8. CONCLUSION

Privacy Policy Recommendation enables users to automate privacy policies for images that users upload on content sharing sites. This system gives a comprehensive structure to infer privacy preferences based on historical information available for the users. This system handles the cold-start issue by utilizing the social context information. Existing system provides the recommendation to social groups like friends, family, co-workers, etc. Whereas the proposed system with Decision Voting scheme facilitates privacy recommendation for individual users. This works on conflict resolution as well.Also, to this, we are encrypting images while saving to ensure security to contents of the images. As a future scope, we can integrate the existing system with business intelligence and data warehousing solution which can provide strategic as well as operational analysis for further refinement of privacy policies or strategies.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[2] R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[3] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile

photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.
[4] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.
[5] A. Besmer and H. Lipford, "Tagged photos: Concerns, perceptions, and protections," in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.
[6] D. G. Altman and J. M. Bland ,"Multiple significance tests: The bonferroni method," Brit. Med. J., vol. 310, no. 6973, 1995.
[7] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
[8] J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., 2009, pp.249–254.
[9] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu, and J.-L. Wu, "Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning," in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.
[10] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, "Connecting content to community in social media via image content, user tags and user communication," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.
[11] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.
[12] Ricardo da Silva Torres Alexandre Xavier Falcão , "Content-based image retrieval: Theory and applications," Ricardo da Silva Torres Alexandre Xavier Falcão , vol. 2, no. 13, pp. 161–185, 2006.13.
[13] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age," ACM Comput. Surv., vol. 40, no. 2, p. 5, 2008.
[14] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, "What does classifying more than 10,000 image categories tell us?" in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp. 71–84. [Online]. Available: http:// portal.acm.org/citation.cfm?id=1888150.1888157
[15] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.
[16] L. Geng and H. J. Hamilton, "Interestingness measures for data mining: A survey," ACM Comput. Surv., vol. 38, no. 3, p. 9, 2006.
[17] Image-net data set. [Online]. Available: www.image-net.org, Dec. 2013.
[18] S. Jones and E. O'Neill, "Contextual dynamics of group-based sharing decisions," in Proc. Conf. Human Factors Comput. Syst., 2011, pp. 1777–1786. [Online]. Available: http://doi.acm.org/ 10.1145/1978942.1979200
[19] A. Kaw and E. Kalu, Numerical Methods with Applications: Abridged., Raleigh, North Carolina, USA: Lulu.com, 2010.