International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Privacy Strategy Prediction of User- Images on Content Sharing Online Social Networking

[1]V.Alekhya & [2]K. Kalyani

[1]M.Tech Student, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA , Andhra Pradesh, India

[2]Assistant Professor in Dept. of CSE, , ALITS Engineering College, Affiliated to JNTUA, Andhra Pradesh, India

Abstract

User Image sharing social site maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need an Adaptive Privacy Policy Prediction system to help users compose privacy settings for their images. The solution relies on an image classification framework for image categories which may be associated with similar policies and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to user's social features. Image Sharing takes place both among previously established groups of known people or social circles and also increasingly with people outside the users social circles, for purposes of social discovery-to help them identify new peers and learn about peers interests and social surroundings, Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

Keywords: Adaptive Privacy Policy Prediction; Online information services; web-based services.

I. INTRODUCTION

An A3P system that helps users automates the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold start, leveraging social context information. A3P-core: (I) Image classification and (ii) Adaptive policy prediction. User images are first classified based on content and metadata. Privacy policies of each category of images are analyzed for the policy prediction. Content-based classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. Metadata-based classification groups images into subcategories under aforementioned baseline categories. A3P-social multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user's social context. Images searching for content based and image based the result found for each image privacy policy set of user privacy in sharing site. Content-based classification is based on an efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. The Image encodes frequency and spatial information related to image color, size, and texture. The small number of coefficients is selected to form the signature of the image.

II. RELATED WORK

Content-based retrieval is ultimately dependent on the features used for the annotation of data and its efficiency is dependent on the invariance and robust properties. The Polar Fourier Transform (PFT) is similar to the Discrete Fourier Transform in two dimensions but uses transform parameters radius and angle rather than the Cartesian co-ordinates. To improve implications for content based retrieval of natural images where there will be a significantly higher number of textures.

Local radial symmetry is to identify regions of interest within a scene. A facial feature detector and as a generic region of interest detector the new transform is seen to offer equal or superior performance to contemporary techniques. The method has been demonstrated on a series of face images and other scenes, and compared against a number of contemporary techniques from the literature. Equal or superior performance on the images tested while offering significant savings in both the computation required and the complexity of the implementation.

The refining process is formulated as an optimization framework based on the consistency between "visual similarity" and "semantic similarity" in social images. An image retagging scheme that aims at improving the quality of the tags associated with social images in terms of content relevance.

III. SYSTEM OVERVIEW

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified

true, A3P-core will invoke A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc). In above cases, it would be beneficial to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy. The actual policy will be stored in the policy repository of the system for the policy prediction of future uploads.

IV. IDENTIFYING SOCIAL GROUPS

The policy recommendation process based on the social groups that a user U uploaded a new image and the A3P-core invoked the A3P-social for policy recommendation. The A3P-social will find the social group which is most similar to user U and then choose the representative user in the social group along with his images to be sent to the A3P-Core policy prediction module to generate the recommended policy for user U.

Given that the number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group. In order to speed up the group identification process and ensure reasonable response time, we leverage the inverted file structure to organize the social group information. The inverted file maps keywords (values of social context attribute) occurring in the frequent patterns to the social groups that contain the keywords. Specifically, in first sort the keywords (except the social connection) in the frequent patterns in an alphabetical order. Each keyword is associated with a link list which stores social group ID and pointers to the detailed information of the social group.

V. A3P CORE

There are two major components in A3P-core: (i) Image classification and (ii) Adaptive policy prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction. Adopting a two-stage approach is more suitable for policy recommendation than applying the common one-stage data mining approaches to mine both image features and policies together.

Recall that when a user uploads a new image, the user is waiting for a recommended policy. The two-stage approach allows the system to employ the first stage to classify the new image and find the candidate sets of images for the subsequent policy recommendation. As for the one-stage mining approach, it would not be able to locate the right class of the new image because its classification criteria need both image features and policies whereas the policies of the new image are not available yet.

Moreover, combining both image features and policies into a single classifier would lead to a system which is very dependent to the specific syntax of the policy. If a change in the supported policies were to be introduced, the whole learning model would need to change.

A. Content-Based Classification:

Content-based classification is based on an efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. The Image encodes frequency and spatial information related to image color, size, and texture. The small number of coefficients is selected to form the signature of the image.

Image selected similarity criteria include texture, symmetry, shape the image color and size. User uploads an image; it is handled as an input query image. The signature of the newly uploaded image is compared with the signatures of images in the current image database. The class of the uploaded image is then calculated as the class to which majority of the m images belong. If no predominant class is found, a new class is created for the image. Later on, if the predicted policy for this new image turns out correct, the image will be inserted into the corresponding image category in our image database.

B. Metadata-Based Classification:

The metadata-based classification groups images into subcategories under aforementioned baseline categories. Extract keywords from the metadata associated with an image metadata vector frequency find a subcategory that an image belongs to. This is an incremental procedure. The privacy approach with in same category of the new image user defines a policy same category of the new image, conduct association rule mining on the subject component of polices.

Extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. Retrieve the hyponym for each it a metadata vector. Select the hyponym with the highest frequency. Subcategory that an image belongs to, this is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hyponyms of the image becomes the subcategory's representative hyponyms. Compute the distance between representative hyponyms of a new incoming image and each existing subcategory.

VI. Adaptive Privacy Policy Prediction Social

The A3P-social employs a multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user's social context and his general attitude toward privacy. As

mentioned earlier, A3Psocial will be invoked by the A3P-core in two scenarios.
One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer meaningful and customized policies. The other is when the system notices significant changes of privacy trend in the user's social circle, which may be of interest for the user to possibly adjust his/her privacy settings accordingly. In what follows, we first present the types of social context considered by A3P Social, and then present the policy recommendation process.

Social Image Privacy Policy and Searching Image:

The image data collection, To image predict policies and compare it with a base-line algorithm which does not consider social contexts but bases recommendation only on social groups that have similar privacy strictness of images information. Using the base-line approach, we note that regardless of the individual privacy inclination of the users, the best accuracy is achieved in case of explicit images and images dominated by the appearance Image.

Users maintain more consistent policies, and our algorithm is able to teach them effectively. Images searching for content based and image based the result found for each image privacy policy set of user privacy in sharing site. Uploaded a new image and the A3P-core invoked the A3P-social for policy recommendation. The number of users in social network may be huge and that users may join a large number of social groups, it would be very time consuming to compare the new user's social context attributes against the frequent pattern of each social group.

VII. CONCLUSION

Our solution relies on an image classification framework for image categories which may be associated with similar policies and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user The generated policies will follow the evolution of user's privacy attitude.

REFERENCES

[1] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age" IEEE Transaction on Cloud Computing, Vol. 2, NO. 4, OCTOBER-DECEMBER 2014.

[2] P.R. Hill, C.N. Canagarajah and D.R. Bull, "Rotationally Invariant Texture Based Features" IEEE Computer Society 1089-7801/15/$31.00 c 2015 IEEE.

[3] Kaitai Liang, Joseph K. Liu, Rongxing Lu, Duncan S. Wong, "Privacy Concerns for Photo Sharing in Online Social Networks"
IEEE Computer Society 1089-7801/15/$31.00 c 2015 IEEE.

[4] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, "Tag, you can see it!: Using tags for access control in photo sharing" IEEE Transaction on Engineering Management, Vol. 62, NO. 3, AUGUST 2015.

[5] D. Liu, X.-S. Hua, M. Wang, and H.-J. Zhang, "Retagging social images based on visual and semantic consistency" IEEE Transaction on Image Processing, VOL. 24, NO. 11, NOVEMBER 2014.

[6] G. Loy and A. Zelinsky, "Fast radial symmetry for detecting points of interest"
IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, NO.8, AUGUST 2014.

[7] Linke Guo, Chi Zhang, and Yuguang Fang, "A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks" IEEE Transaction on Dependable and Secure Computing, Vol. 12, NO. 4, JULY/AUGUST 2015.

[8]

[9] Xueming Qian, Xian-Sheng Hua, Yuan Yan Tang, and Tao Mei "Social Image Tagging With Diverse Semantics" IEEE Transaction
on Cybernetics, Vol. 44, NO. 12, DECEMBER 2014.

[10] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search" IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, NO. 8, AUGUST 2014.

[10] J. Zhuang and S. C. H. Hoi, "Non-parametric kernel ranking approach for social image retrieval" IEEE Transaction on Knowledge and Data Engineering, Vol. 26, NO. 1, JANUARY 2014.