ISSN:0975-9646

Privacy Policy Inference of User-Uploaded Photos on Social Networking Sites

Ashwini P Nimbhore , Prof. Aarti P Nimbhore

Abstract:Photo sharing refers to the transfer or publishing of users digital photos online and the website which provides such acquaintances offer services such as hosting, uploading, sharing and managing of photos through online system. This function provides the upload and display of images through both websites and applications. The photo sharing term can be set up and managed by individual users for the usage of online photo galleries including photo blogs. It means that other users can view but not essentially download the photos, users being able to select different copyright options for their photos. Unfortunately, it may reveal users privacy if they are permitted to post, comment, and tag a photo liberally. Online photo sharing applications have become popular as it provides users various new and innovative alternatives to share photos with a range of people. The photo sharing feature is incorporated in many social networking sites which allow users to post photo for their loving ones, families and friends. For users of social networking sites such as Facebook, this system focuses on the privacy concerns and needs of the users, at the same time explores ideas for privacy protection mechanisms. By considering users current concerns and behaviors, the tool can be designed as per the users desire which they can adopt and then can be motivated to use. This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques. In the final step we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences.

Keywords:- Online information services, web-based services.

INTRODUCTION:

Social media is very powerful tool to communicate with each other ,user can communicate with social site to exchange idea ,emotion ,information, happiness. Now every user are connect to each other , there are very high volume which are connect with each other using different sites. Social media is the two way communication in Web and it means to communicate, share, and interact with an individual or with a large audience. Social networking websites are the most famous websites on the Internet and millions of people use them every day to engage and connect with other people. Number of web site like Facebook, Twitter, etc. users are used to communicate, connected with each other, user can upload, post, tweet, download images video and performing number of action.

The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. The Most content sharing websites allows a user to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reason provided is that the amount of shared information this process can be tedious and error-prone. Our goal is to improve the set of privacy controls and defaults, but we are limited by the fact that there has been no in-depth study of users' privacy settings on sites like Facebook.

The proposed work is based on Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, Video and factors in the following criteria that influence one's privacy settings of images and Video.

RELATED WORK

Our work is related to works on privacy setting configuration in social sites, recommendation systems, and privacy analysis of online images.

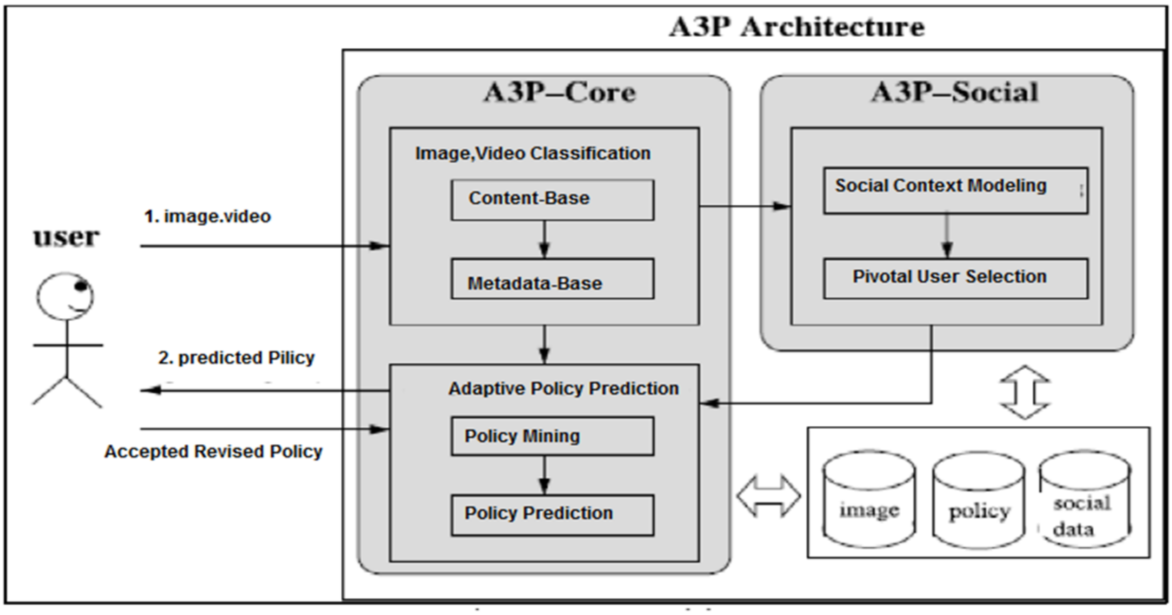
Privacy Setting Configuration: this privacy setting will allow a users to enter their privacy preferences. To acknowledged the need of policy recommendation, which can assist users to easily and properly configure privacy settings.

Policy Recommendation system: A recommendation framework to connect image content with communities in online social media for automatically to predict relevant concepts (tags) of photos.

Privacy analysis of online images: this analysis can detect and identify the object matching of face detection technique.

SYSTEM ARCHITECTURE:-

A Content-Based Classification: it classifies image contents and then refine each category into subcategories with the help of hierarchical classification which gives higher priority to image content and minimize the influence of missing tags.



B Adaptive Policy Prediction : The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user's privacy concerns.

Problem Statement:-
Suppose user want to share any images and video so user may or may not want to share this data to all level, user must want to provide some assurance where user will place data and provide some type of security on traveling data. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.

PROPOSED SYSTEM:-

1) A3P-CORE
2) A3P-SOCIAL

A3P-CORE:

There are two major components in A3P-core: (i) Image, Video classification and (ii) Adaptive policy, predefined prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images and Video 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 Image classification: Groups of images that may be associated with similar privacy preferences. we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images do not have metadata will be grouped by content.
Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags. Note that it is possible that some images are included in multiple categories as long as they contain the typical content features or metadata of those categories.

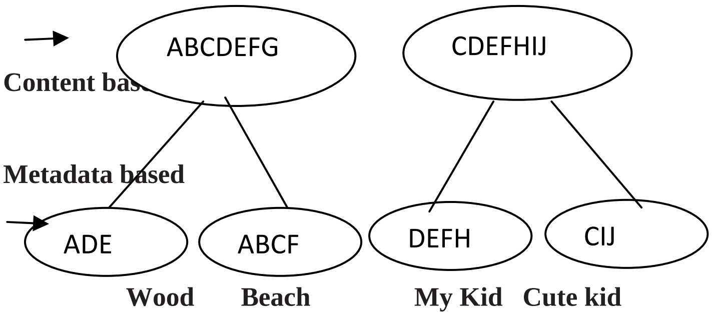


Fig 1 Image Classsification

Example:
Image Classification for 10 images named as A, B, C, D, E, F, G, H, I, J, respectively.
The content-based classification creates two categories: "landscape" and "kid". Images C, D, E and F are included in both categories as they show kids playing outdoor which satisfy the two themes: "landscape" and "kid". These two categories are further divided into

subcategories based on tags associated with the images. As a result, we obtain two subcategories under each theme respectively. Notice that image G is not shown in any subcategory as it does not have any tag; image A shows up in
both subcategories because it has tags indicating both "beach" and "wood"

The adaptive policy prediction process consists of three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

1) Policy normalization: The policy normalization is a simple decomposition process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set.

2) Policy mining: hierarchical mining first look for popular subjects defined by the user, then look for popular actions in the policies containing the popular subjects, and finally for popular conditions in the policies containing both popular subjects and conditions.

3) 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. To model the user's privacy tendency, we define a notion of strictness level. The strictness level is a quantitative metric that describes how "strict" a policy is.

A3P-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.

Social Context Modeling: The social context modeling algorithm consists of two major steps. The first step is to identify and formalize potentially important factors that may be informative of one's privacy settings. The second step is to group users based on the identified factors.

Contribution:-

Base Paper is focus on the image data only. Base paper provides the facility of Image policy mining in the form of Subject(Whom),Action(Action perform),
Condition(Time period). A new approach we also consider images as well as video data. (Refer architecture).Because video is more integral part on social media, Because of Increasing a ration of Mobiles phones user are taking very high interest into capture and upload video, So consider this point we Providing a Privacy Policy Inference of User-Uploaded Images and Video on Content Sharing Sites. To this contribution we are focus on the user uploads videos and predict policy to this video with using our architecture.

Algorithms:-

1 Policy Prediction Algorithm.

2 Data mining Algorithm.

1. Select Dataset (News Dataset)
2. Preprocessing Data
3. Remove Stopword
4. Stamming Data
5. Find Out Term(Related Name Entities)
6. Match Data On Terms Basis
7. Select Matching friends nm

Image Comparison Algorithm :

There are many scenarios where tried to compare images but failed to compare them. Image comparison is a very deep concept where there involved lot many complex algorithms . In brief for Two images to be same we need to compare the two images pixel by pixel so i came across Pixel Grabber class in java and started using it which gave a positive result, but not accurate.

1.Select Image
Convert image into bitmap
Select target image to matching from friend list(profile)
Convert into bitmap
2. Convert bitmap into byte array
3. Sort both bite array in basis of bytes
4. Compare every bit of byte array
If both array match then select matching profile of friend into policy.

OpenCv Algorithm for Face recognition-

Pre-process the image, if needed (e.g. to enhance contrast, filter noise, etc.).

A Image Segmentation, process in which the image is converted to regions which contains pixels that are similar to pixels in the same region and different from pixels to other regions. This can be done using region-growing, mathematical morphology, clustering or classification algorithms. There are many algorithms to do that, just google for "image segmentation" and other keywords to get more information.

With the regions, create descriptors for them. Descriptors are calculated from the region and can include shape, area, perimeter, number of holes, general color of the region, texture, orientation, position, etc.

If needed, do a Re-Segmentation of the image, process in which regions are merged if they can be considered as belonging to the same object. Note that this step may require some high-level knowledge of the objects and the task in general, seldom being fully automatic and often being task-dependent.

If needed, filter the regions that seem relevant to the task in hand, eliminating small regions or regions which are deemed unrelated to the task (again this may require some knowledge about the task).

Store the image's regions' descriptor for further processing.

Repeat those steps for other images.

Use the descriptors for comparison of the contents of the images, using some of many algorithms for pattern matching.

Experimental Results:

Matching Policy: Experimental Description of Matching policy is based on image classification for content base, Metadata & Both policies to find policy and ratios.

Table 1

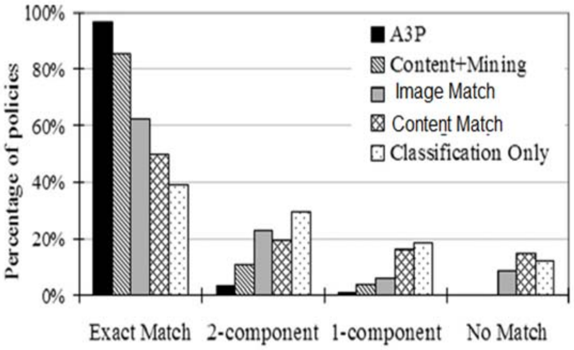
Matching Policy	Experiment	Find Policy	Ratio
Content Base	100	15	15%
Metadata Base	100	40	40%
Both	100	60	60%

Table 2 : Comparison among various features between existing and proposed method A3P Core

Method	View	Comment	Tags, Notes, Download	Overall Policy
A3P-Core(Own)	92.48%	92.48%	92.63%	92.53%
Propagation	66.12%	66.82%	68.64%	66.84%
Tag Only	87.54%	87.03%	86.03%	87.01%

Result Of Direct User Evaluation

Item Type	Count	Ratio
Total Policies	500	92.1%
Exact Matching Policies	450	90%
Policies with 1 error	35	6.4%
Policies with 2 error	7	1.1%
Policies with 3 error	2	0.4%



Most importantly, the generated policy will follow the trend of the user's privacy concerns evolved with time. We have conducted an extensive user study and the results demonstrate effectiveness of our system with the prediction accuracy around 90%.

CONCLUSION:-

An algorithm creates new framework for Images and Videos that are uploaded on Social site. Social network is an upgrading media for information sharing through internet. It provides a content sharing like text, image, audio, video, etc… With this emerging E-service for content sharing in social sites privacy is an important issue. This algorithm provides a predefined or automated privacy prediction policy where user gets Subject(To whom Data will be share), Action(What action will be performed by selected user i.e. Comment, View, Download) and Condition(Time period on which action should be perform) for Uploaded images or videos which provide a privacy policy prediction and access restrictions along with blocking scheme for social sites and improve the privacy level for the user in social media.

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] R. da Silva Torres and A. Falc~ao, “Content-based image retrieval: Theory and applications,” Revista de Inform_atica Te_orica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.

[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] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter, “Tag, you can see it!: Using tags for access control in photo sharing,” in Proc. ACM Annu. 99615.94