Shared Image Privacy Preserving Using Adaptive Prediction

Mohini Shinde[1], **Tanuja Dhope**[2]

Department of Computer Networks, G.H.Raisoni College of Engg and Mangmt, Pune

Abstract: ***Now images are one of the key enablers of user's connectivity. With increasing volume of the images users share through social sites, maintaining privacy has become a major problem. In light of these incidents, the need of tools to help users control access to their shared content is apparent. An Adaptive Privacy Policy Prediction (A3P) system helps users to compose privacy settings for their images. A two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded. A3P system aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user.***

Keywords: Adaptive Privacy Policy Prediction (A3P), Online social networks (OSNs), Content Based Image Retrieval (CBIR)

1. Introduction

With the increasing volume of users shared images 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. In light of these incidents, the need of tools to help users control access to their shared content is necessary. Images are now one of the key enablers of users connectivity. Sharing takes place both between previously established groups of known people or social circles and also increasingly with people outside the users social circles. With the increasing volume of images users share through social sites, maintaining privacy has become a major issue. Online social networks (OSNs) have experienced huge growth in recent years and become a de-facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy problems. In light of these incidents, the need of tools to help users control access to their shared content is necessary.

Content Based Image Retrieval (CBIR) is any method that helps to organize digital image archives by visual content basis. By this definition, anything ranging from an image similarity function to a robust image annotation engine falls under the purview of CBIR. The most common form of CBIR is an image search depend on visual Content- based image retrieval, in this technique, use visual contents to search images from large scale image databases according to users interests Content-based image retrieval, such as color, shape, texture, and spatial layout to represent and index the image. In typical content-based image retrieval systems (Figure 1), the visual contents of the images in the database are extracted and described by multi-dimensional feature vectors.

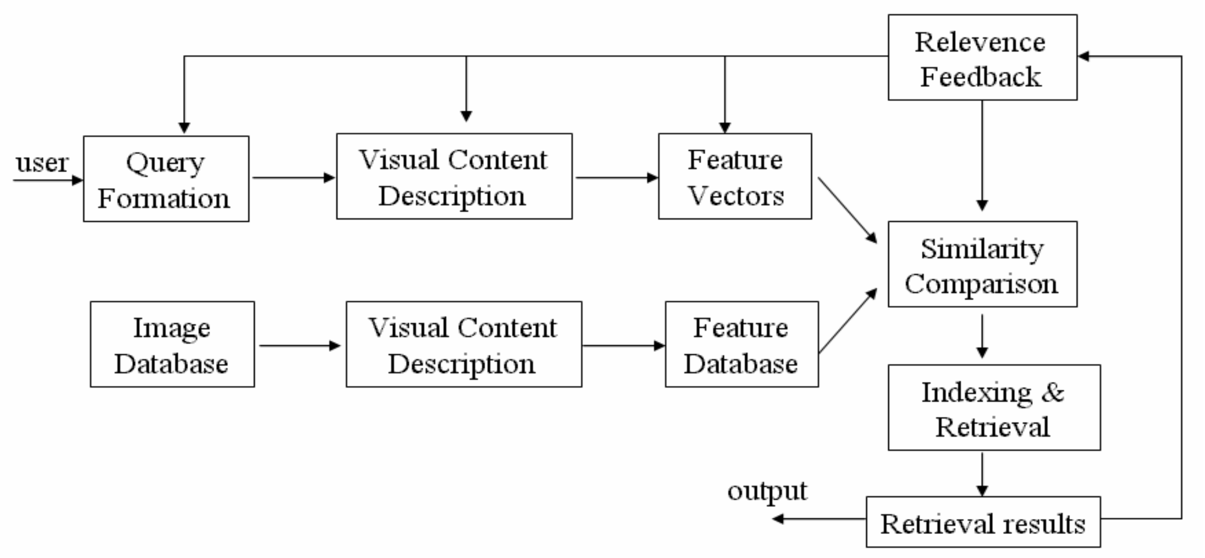

Figure 1: Diagram for content-based image retrieval system

2. Related Work

A privacy protection framework is proposed for large-scale content-based information retrieval. It offers two layers of protection. First, robust hash values are used as queries to prevent revealing original content or features. Second, the client can choose to omit certain bits in a hash value to further increase the ambiguity for the server. The results show that the privacy enhancement slightly improves the retrieval performance.[3]

A privacy recommender system, proposed helps users make more appropriate decisions with regards to their privacy. The recommender tool uses an ontology engine for parsing and comprehension of privacy policy statements, privacy settings, and user needs that are provided either directly by the user or from users' past behaviors. Privacy Recommender system analyzes the privacy policies of social media websites using ontologies.[8]

An approach to enable the protection of shared data associated with multiple users in OSNs was introduced. Based on this formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism.[1]

A systematic solution to facilitate collaborative management of shared data in OSNs was provided. This Begin by examining how the lack of multiparty access control (MPAC) for data sharing in OSNs can undermine protection of the user data. An architecture (called Hummingbird) that offers a Twitter-like service with increased privacy guarantees for tweeters and followers alike. Hummingbird architecture mirrors Twitter's, which involve one central server and an arbitrary number of registered users, that can publish and retrieve short text-based messages. Publication and retrieval is based on the set of hash tags that are appended to the message or specified in the search criteria.[2]

3. A3P Framework

There is a need of tools to help users control access to their shared content is necessary. Toward addressing this, propose an Adaptive Privacy Policy Prediction (A3P) system to help users to compose privacy settings for their images. In this framework a two level framework is introduced called as Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hasslefree privacy settings by automatically generating personalized privacy policies.

System Architecture

A two level framework is introduced called as Adaptive Privacy Policy Prediction(A3P) system which aims to provide users a hasslefree privacy settings experience by automatically generating personalized policies. The A3P system consists of two main components as A3P-core and A3P-social(Figure 2). The overall data flow is the following. When user uploads an image, the image will be directly sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to involve the A3P-social. The A3P-social devides users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When theA3P-social is invoked, it automatically find outs the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the last, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, user can just accept it. Otherwise, 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 the future uploads by user.

Policy Mining

A hierarchical mining approach for policy mining is used. Policy mining is carried out within the same category of the new image. The basic idea of this is to follow a natural order in which a user defines a policy. The 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.

Policy Prediction

It is an approach to choose the best candidate policy that follows the user's privacy tendency. To model the user's privacy tendency, define a notion of strictness level. The strictness level is a quantitative metric that describes how "strict" a policy is. a strictness level L is an integer with minimum value in zero, wherein the lower the value, the higher the strictness level.

4. Result

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. The results of A3P framework are Recommend better images according to user history and Search image effectively using content or metadata search query.

5. Conclusion

The proposed system i.e. Adaptive Privacy Policy Prediction (A3P) system which helps users automate the privacy policy settings for their uploaded images. The A3P system provides a privacy framework to infer privacy preferences based on the information available for a given user. It also effectively handle the issue of cold-start, leveraging social context information. The A3P is a practical tool that provides significant improvements over current approaches to privacy.

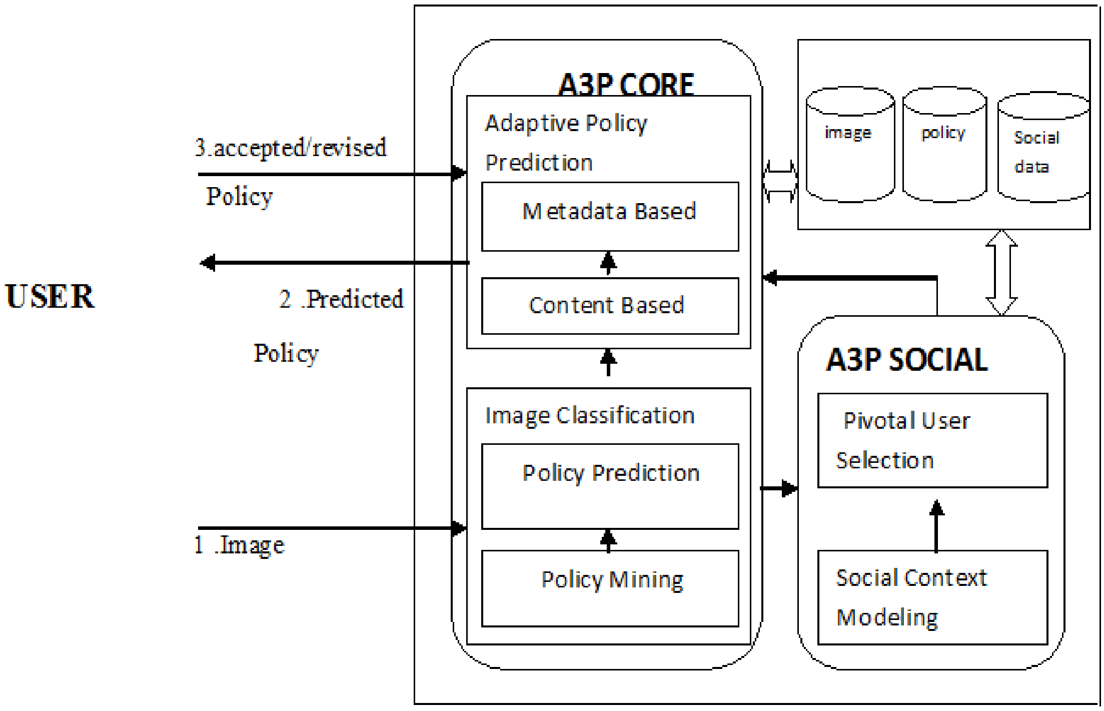

Figure 2: Adaptive Privacy Policy Prediction (A3P) system Architecture

By correcting mismatched policies, system's accuracy increases. It is also expected that with more user data and a longer execution of the A3P system, the prediction accuracy will be further increased, as the system adapts to users' privacy preferences.

References

[1] "Multiparty Access Control for Online Social Networks: Model and Mechanisms"- Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Jan Jorgensen IEEE transactions on knowledge and data engineering, vol. 25, no. 7, july 2013

[2] Emiliano De Cristofaro *PARC,* Claudio Soriente *ETH Zurich* , Gene Tsudik Andrew Williams *UC Irvine UC Irvine* 2012 IEEE Symposium on Security and Privacy "Hummingbird: Privacy at the time of Twitter"

[3] "A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval"-Li Weng, *Member, IEEE*, Laurent Amsaleg, April Morton, and Stéphane Marchand-Maillet IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015

[4] Dong Liu, Shuicheng Yan, *Senior Member, IEEE*, Xian-Sheng Hua, *Member, IEEE*, and Hong-Jiang Zhang, *Fellow, IEEE* "Image Retagging Using Collaborative Tag Propagation" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 13, NO. 4, AUGUST 2011

[5] Yongdong Wu, Zhuo Wei, and Robert H. Deng - "Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks" IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013

[6] Jianping Fan, Daniel A. Keim, Yuli Gao, Hangzai Luo, and Zongmin Li *"JustClick*: Personalized Image Recommendation via Exploratory Search From Large-Scale Flickr Images "IEEE transactions on circuits and systems for video technology, vol. 19, no. 2, february 2009

[7] "Privacy Preserving Policy-Based Content Sharing in Public Clouds"- Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE-IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 11, NOVEMBER 2013

[8] Curtis Rasmussen School of Computer Science University of Guelph, Guelph, Canada crasmuss@uoguelph.ca "Empowering Users through Privacy Management Recommender Systems" Rozita Dara, Member, IEEE School of Computer Science University of Guelph, Guelph, Canada drozita@uoguelph.ca 2014 IEEE Canada International Humanitarian Technology Conference - (IHTC) 978-1-4799-3996-1/14/$31.00 ©2014 IEEE

[9] Image Processing: Principles and Applications—Tinku Acharya and Ajoy K. Ray (Hoboken, NJ: Wiley, 2005, pp. 448, ISBN: 0-471-71998-6). *Reviewed by Francesco Camastra, Book Reviews* IEEE transactions on neural networks, vol. 18, no. 2, march 2007