www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 4 April 2016, Page No. 16196-16201

Providing Confidential Policy Conjecture To Images Uploaded By Users On Social Sites

Pushpa Rani, BG Nagar,Mandya.

M.p(4bw14scs09),4th sem M.Tech,Dept of CS&E,BGSIT,

email:cheethu420@gmail.com

Abstract: Today users sharing large volume of images through social sites inadvertently become a major problem of maintaining confidentiality. To help the users to control access to their shared content needs some tools. An Adaptive Privacy Policy Prediction (A3P) used in this paper to address the confidentiality problem.A3P system helps the user to compose confidentiality setting of their images by examine the role of social context, image content and metadata these act as a possible indicators of users privacy preferences.A3P system uses the two-level framework according to users available history on the site to determines the best available privacy policy for users images being uploaded. The solution relies on an image classification framework for image categories which may be associated with similar policies, and on an algorithm which predict the policy to automatically generate a policy for each newly uploaded image, also according to user's social features. The generated policies fallow the evolution of users' confidentiality attitude.

Index Terms- Online information services, web based services.

I Introduction

Now a day's images are one of the key enablers of user's connectivity. Images can be shared both previously established group of known people or social circle and also with the people outside the users social circles. The rich images may reveal the content of sensitive information. Sharing images with in social sites may quickly leads to unwanted disclosure and confidentiality violation[3],[24].The persistent nature of online media makes it possible for other user to collect rich aggregate information about the owner of published content and subjects in the published content[3],[20],[24]. That information can result in unexpected exposure of one's social environment and leads to abuse of one's personal life.

Most content sharing websites allow users to enter their confidentiality preferences. But, recent studies shown that users struggle to set up and maintain such confidentiality settings [1], [11], [22], [33]. One of the main reason to adopting policy recommendation system is the amount of shared information process can be tedious and error-prone

in many websites. Therefore, many have adopting the policy recommendation system which can assist the user to easily and properly configure confidential setting [7], [22], [28], [30]. The existing automated confidentiality setting appears to be inadequate to address the unique confidentiality needs of images [3],[5],[41], due to the amount of information implicitly carried with in images and their relationship with online environment where they are exposed.

In this paper, A3P system is proposing which aim is to provide users a problem free confidential setting experience by automatically generating personalized policies. The A3P system handles the images uploaded by the users and factors in the fallowing criteria. The images confidentiality settings influenced by the criteria:

- The impact of social environment and personal characteristics. The useful information regarding users' confidentiality preference can be provided by the social context of users such as their profile information and relationship with others. For example, user interested in photography may like to share their photo with other photographer, user who has several family members among their social contact may share the images related to family events with them. Users may have different opinion on confidentiality setting on the same type of images. It is important to find out the balancing point between the impact of social environment and individual characteristics of users in order to predict the policy that fulfils the need of each individual.
  Individuals may change their overall attitude towards confidentiality as time passes. In order to develop a personalized policy recommendation system changes on confidentiality opinion should be carefully considered.
- Role of image's content and metadata. Generally similar images often incur similar confidentiality preferences, especially when people appear in the images. For example, one may upload several images of his children's and specify that only his family members can allow to see that images. He may upload some other images of landscape and may set confidentiality preference allowing anyone to view and comment that image.

Analyzing Visual content not be enough to capture users confidentiality preferences. Tags and other metadata are indicative of the social context of the image, including

DOI: 10.18535/Ijecs/v5i4.24

where it was taken and why [4], and synthetic description of the images' provided to complimenting the information obtained from the visual content analysis.

2. A3P Framework

2.1 Preliminary notions

Users can express their confidentiality preferences about their content disclosure preferences with the other users are socially connected with him via confidentiality policies. Confidential policy defined according to Definition 1. This policy inspired by popular social sites (i.e., Face book, Picasa, Flickr), actual implementation depends on specific content management site structure and implementations.

Definition 1: A confidential policy P of user U consists the fallowing components:

- Subject(S): A set of users socially connected to U.
- Data (D): A set of data item shared by U.
- Action (A): A set of action granted by U to S on D.
- Condition (C): a Boolean expression which must be satisfied in order to perform the granted actions.

According to definition users in S can be represented by their identities and roles (e.g., family, co-workers, friends), or organization (e.g., profit organization, or non-profit organization). Set of images in the user profile is D. Each image has the unique ID along with some metadata associated with it like tags "vacation", "birthday". Further images are grouped into albums. As for A consider four common type of action :{ view, comment, tag, download}. C specifies when the granted action is effective. C is Boolean expression on grantees attribute like time, location and age. Example policy is given below.

Example 1: john would like to allow his friends and co-worker to comment and tag images in album named "vacation album" and image named "birthday.jpg" before year 2011. This confidentiality preference can be expressed by the fallowing policy:

P :{{ friends, co-workers},{vacation album, birthday.jpg},{comment, tag},{date<2011}}.

2.2 System overview

Figure 1 shows the A3P system overview, it consist two main components: A3P-core and A3P-social. When images uploaded by the user it first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social.A3P-core uses the historical behaviour of user to predict the policy for the users. A3P-core invokes the A3P-social if one of the two fallowing cases is true:

(i) The user doesn't have enough data for the type of image uploaded to apply policy prediction procedure.
(ii) If any major changes among the users community about their confidentiality setting along with user increase of social network activities.

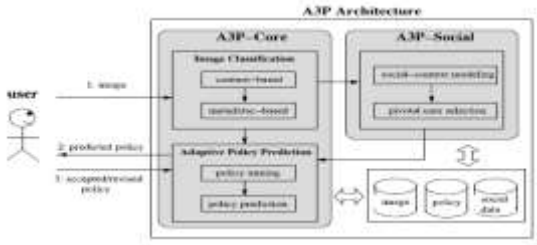

Fig.1: System overview

The A3P social continuously monitor the social group of user. When the A3p social invoked, it automatically identifies the social group of user and send back the information about the group to A3p core for policy prediction. At the end system displays the predicted policy to user. User can accept that policy if he satisfied by that policy otherwise he can choose to revise the policy. When the newly generated policy not accepted by the user it will be stored in policy repository of the system for the policy prediction of further uploads.

3. A3P-core

A3P-core consist two major components:

(i) Image classification and

(ii) Adaptive policy prediction

First user images classified based on the content and metadata. Then, confidential policies for each category of images are analyzed for predicting the policy.

Two-stage approach is adopting for policy recommendation. This approach allows the system to employ the first stage to classify the new image and find the candidate set of images for the subsequent policy recommendation.

3.1 Image classification

Hierarchical image classification is proposed to obtain group of images that may be associated with similar confidential preferences. This image classifier first classifies the image based on their content and then, refines each category into subcategories based on their metadata. Images grouped only by its content, if it doesn't have the metadata. This classification gives a higher priority to image content and minimizes the influence of missing tags.

Figure 2 shows classification of 10 images named as A,B,C,D,E,F,G,H,I and J respectively. The two categories "landscape" and 'kid "created by content based classification. Both the category shows kids playing outdoor, which satisfy the two themes: "landscape" and "kid" so, image C, D, E, and F included in both the categories. In Figure 2, two subcategories are presented under each theme. Image G not shown in any subcategories because it don't have any tag. Image A shown in both subcategories because it has a tag indicating both "beach" and "wood".

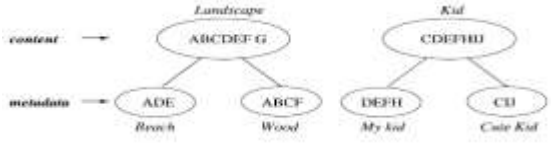

Fig 2: Two-level image classification

3.1.1 Content–Based classification

Efficient and accurate image similarity approach is used for content-based classification. Quantified and sanitized version of Haar wavelet transformation definition is used for image signature. The classification algorithm compares the signature of images. The wavelet transform encodes the frequency and spatial information related to image colour, size, invariant transform, shape, texture, symmetry, etc for each image. Then, it selects the small number of co-efficient to make a signature to image. The distance among the signature of images gives the similarity among the images.

Symmetry, shape, texture and SIFT [25] are the criteria to select similarity. Sometime, colour and size are also considered. The system begins with five generic classes of image: (a) explicit (e.g., nudity, violence, drinking, etc), (b) adult, (c) kids, (d) scenery (e.g., beach, mountains), (e) animals. Initially for each class number of images assigned by taking images from Google images. Each class may approximately contain 1000 of images. System contains a large data set of images. Then, signature generated to all images in the data set and stored them into data base.

To evaluate the accuracy of content classifier some preliminary tests are conducted. The classifier tested against a ground-truth data set, image-net.org [17]. Over 100 million of images are collected and classified according to the structure of wordnet in image-net. The first half of images taken as training data set in each image class and classify the next 800 images. The result of classification was recorded as true if the direct hypernym or synset's search term is returned as class. The average accuracy A3P-core classifier is above 94 percent.

When the image uploaded by the user it used as input query image. The classifier compares the signature of newly uploaded image with the signature of images in the current database. It first finds the m closest matches to uploaded image to determine the class of the new image. Based on which class the majority of m images belongs are considering classifying to which class the new uploaded image belongs to. The policy prediction for the new image turns out correct. Then, that image will be included in corresponding image class in the system data base, to help refine future policy prediction. The A3P system sets m as 25.

3.1.2 Metadata-Based classification

The group of images classified into sub categories by the metadata-based classification. This process consist three main steps:

1. First step extract the keyword from the metadata associated with an image.
2. Second step derives respective hypernym from each metadata vector.
3. Third step finds subcategories that an image belongs to.

In the first step tags, comments and caption associated with the images are considered as metadata. In A3P-core metadata vector are used which stores the all noun, verb, adjective in the metadata such as $\Upsilon_{noun}=\{t_1, t_2,...., t_i\}$, $\Upsilon_{verb}=\{t_1, t_2,...., t_j\}$ and $\Upsilon_{adj}=\{t_1, t_2,...., t_k\}$, where i, j and k are total number of noun, verb and adjectives respectively.

The second step based on wordnet classification [39] hypernym. It retrieves and obtain hypernym list for each t_i in metadata vector. Π= $\{(v_1, f_1), (v_2, f_2).....\}$, where v is hypernym and f is its frequency. For example, consider Υ = {"cousin", "first-step", "baby boy"} as metadata vector. System finds that "baby boy" and "cousin" have the "kid" as hypernym and "initiative" as the hypenym for "first-step". So, corresponding hypernym list Π={(kid,2), (initiative,1)}. System selects the highest frequency hypernym to be the representative hypernym, e.g., kid. If more tha one hypernym have the same frequency then system selects the hypernym which is most relevant to baseline class. For example, Π={(kid,2), (cousine,2), (initiative,1)}, then system will selects "kid" to be representative hypernym because it is closest to baseline class "kids".

In third step finding subcategories is incremental procedure. At the beginning, subcategory of image form by itself and representative hypernyms of the image become the subcategories representative hypernyms then, system compute the distance between representative hypernymsof new image and each existing subcategories. Let, h_n, h_a and h_v are respective representative hypernyms in metadata vector corresponding to noun, adjective and verbs respectively of new image. For each subcategory C, h_n^c, h_a^c and h_v^c are representative hypernyms of noun ,adjectives and verb respectively. The weighted sum of edit distance [38] between corresponding pair of representative hypernyms as shown in equation 1 used to compute the distance between image and subcategories. Where, D is edit distance and W is weight.

$$Dist_m = w_n.\mathrm{D}\ (h_n,\ h_n^c) + w_a.\mathrm{D}\ (h_a,\ h_a^c) + w_v.\mathrm{D}\ (h_v,\ h_v^c) \quad (1)$$

Where $w_n+w_a+\ w_v=1$ and $w_n>w_a>\ w_v$. The noun in equation (1) has highest hypernym weight because noun is very close to baseline class. Adjectives taken the Second highest weight because, they are refining the base class criteria. Verbs are considered as final hypernym weight .by default, w_n=0.5, w_a =0.3 w_v= 0.2 are taken.

After finding closest subcategory to new image system will check that subcategory has the distance value less than threshold value ϵ. I distance value less than ϵ then, new image include in that subcategory and update the representative hypernymsof subcategory by keeping highest frequency with hypernyms. Otherwise, new subcategory constructed for that new image.

3.2Adaptive policy prediction

Confidential policy for newly uploaded image by the user is predicted and provided by the policy prediction algorithm. Users confidentiality concern reflected in the predicted policy. The process of policy prediction consists three main phases:

(i) Policy normalization
(ii) Policy mining and
(iii) Policy prediction

A simple decomposition process of converting users policy into a set of atomic rules in which the data(D) component is single element set is called as policy normalization.

3.2.1 policy mining

Hierarchical mining approach used for policy mining. Within the same category of the new image because images

DOI: 10.18535/Ijecs/v5i4.24

Policy mining is carried. When user uploaded an image he first decides who can access the image, then thinks about what specific access rights (e.g., view only or download) can be given , and finally define the access conditions. 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.

- **Step 1:** conduct association rule mining on the same category of the new image, the subject component of polices. Let S1, S2; . . ., denote the subjects occurring in policies. Each resultant rule is an implication of the form X ⇒ Y, where X, Y ⊆ S1, S2, . . . } , and X ⊂Y= Ø .we select the best rules according to one some interestingness measures, i.e., the generality of the rule, defined using support and confidence as introduced in [16]. The most popular subjects (i.e., single subject) or subject combinations (i.e., multiple subjects) in policies indicated by the selected rules. we consider policies which contain at least one subject in the selected rules in further steps set of such policies denoted as Υ_i^{sub} and corresponding to a selected rule r_i^{sub}

Example 2. Assume there are six images in the same category of the newly uploaded image "park.jpg" and P2, P5, P9, P13, P18 and P22 are corresponding policies . Table 1 shows what subjects are mentioned in each policy. Mining data in Table 1 may return a best association rule like r_i^{sub} : {family} ⇒ {friend}, meaning that when the user specifies a policy for his family members, he tends to grant the same access right to his friends. In other words, {family}⇒ { friend} is a popular combination appearing in policies. According to r_i^{sub} , P2 will be removed for further consideration since it does not contain any subject in r_i^{sub}

- **Step 2:** In each policy set Υ_i^{sub}, association rule mining conduct on the action component. The result will be in the form of a set of association rules X ⇒ Y, where X, Y ⊆ {open, comment, tag, download}, and X ∩Y = Ø ;. Similar to the first step, we will select the best rules according to the generality interestingness. This time, the selected rules indicate the most popular combination of actions in policies with respect to each particular subject or subject combination. We remove the policy which don not contains any action. Given a selected rule r_j^{act},

Table 1
Example

PolicyID	Familly	friend	coeorker	Other
P2	0	0	1	0
P5	1	1	0	0
P9	1	1	0	0
P13	1	1	0	0
P18	0	1	1	1
P22	1	0	0	0

Υ_j^{act} , denotes the reaming policies , and $\Upsilon_j^{act} \subset \Upsilon_j^{sub}$

Table 2: Example of action components

Policy ID	View-only	comment	tag	download
P5	0	1	1	0
P9	1	0	0	0
P13	0	1	1	0
P18	0	1	1	1
P22	0	1	1	1

Example 3. Let us consider the remaining policies from Example 2. Table 2 shows the action components in these policies (actions "comment", "tag" and "download" imply the "view" action). After mining the action component, we may obtain association rules as follows:
r_1^{act}:{tag } ⇒{comment}
r_2^{act}:{download} ⇒ {comment}
r_1^{act} means that when the user allows someone to tag an image, he usually also allows the person to comment on the image. r_2^{act} means that if one has the "download" right of an image, he/she is most likely to also have the comment right. Suppose that the best rule is r_1^{act} according to the interestingness measure. Then, policy P9 will be removed.

- **Step 3:** We proceed to mine the condition component in each policy set Υ_j^{act} . Let attr1, attr2, ..., attrn denote the distinct attributes in the condition component of the policies in Υ_j^{act} The association rules are in the same format of X ⇒ Y but with X, Y ⊆ {attr1,attr2, . . . , attrn}. Once the rules are obtained, we again select the best rules using the generality interestingness measure. The selected rules give us a set of attributes which often appear in policies. Similarly, we denote the policies containing at least one attribute in the selected rule r_k^{con} Rcon Υ_k^{con} and $\Upsilon_k^{con} \subseteq \Upsilon_j^{con}$ The next task is to determine the actual condition of these attributes. Specifically, in eachΥ_k^{con} , we will choose the most frequent conditions for the selected attributes.

Example 4. Let us continue with Example 3. Table 3 lists attributes occurring in the condition component of the remaining policies.
The best association rule may be:
r_k^{con}: {age} ⇒{time}.
It indicates that this user usually mentions age and time together in policy conditions. Consequently, policy P22 will be removed. Suppose that the majority of the policies (both P5 and P13) specify that people with age older than 18 will be granted access right before year 2012. Then, these conditions will be considered for generating candidate policies in the following Step 4.

- **Step 4**: This step is to generate candidate policies. Given $\Upsilon_k^{con} \subseteq \Upsilon_j^{act} \subseteq \Upsilon_i^{sub}$, we consider each corresponding series of best rules: r_{kx}^{con} , r_{jy}^{con} and r_{iz}^{con}

Table 3
Example of condition component

PolicyId	age	loction	time	affiliation
P5	1	1	1	0
P13	1	0	1	0

P18	1	0	1	0
P22	0	0	0	1

Candidate policies are required to possess all elements inr_{kx}^{con} , r_{jy}^{con} and r_{iz}^{con} . that candidate policies may be different from the policies as result of Step 3. This is because Step 3 will keep policies as long as they have one of the attributes in the selected rules.

Example 5. From Example 2, 3 and 4, we obtained the following set of best association rules:

r_1^{sub}:{family}⇒ {friend}

r_1^{act}: {tag}⇒ {comment}

r_1^{con} : {age}⇒ {time}

For the new image park.jpg, one candidate policy could be:P_{can}: [{family,friend}, {park.jpg}, {comment,tag}, (age > 18∧time< 2012)]

3.2.2 Policy Prediction

Several candidate policies generated in the policy mining step. the goal of our system is to return the best policy to the user. Thus, we present an approach to choose the best candidate policy that follows the user's privacy preference

3.3 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 situations. 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.we first present the types of social context considered by A3P-Social, and then present the policy recommendation process.

4.Experimental Settings

We collecting the data sets by performing two type of expreiments

(i) survey-based study and

(ii) direct user evaluation.

Survey-based study and data collection: We collected two sets of actual user-specified policies to be used as ground truth for our evaluation.

Direct user evaluation: The x experiment is performed to test the acceptability our systems, i.e., whether users would consider the predicted policies reasonable, and inline with their overall preferences. We asked participants to input policies for a few images at first for training purposes. To bootstrap the algorithm three images from a given class are sufficient. Next, participants enter privacy settings for a set of images that they would upload in their fictitious profile. Upon showing the image, privacy settings for it are suggested to the user. The participant has the option to accept the predicted policy as is, revise some components of it, or disagree with the predicted result and he re-enter preferred settings.

Conclusion

We are using the Adaptive Privacy Policy Prediction (A3P) system .that generate the Automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework that takes users social environment and personal characteristics, the role of image's content and metadata. 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.

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] A. Kaw and E. Kalu, Numerical Methods with Applications: Abridged., Raleigh, North Carolina, USA: Lulu.com, 2010.
[20] 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. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.
[21] K. Lerman, A. Plangprasopchok, and C. Wong, "Personalizing image search results on flickr," CoRR, vol. abs/0704.1676, 2007.
[22] H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.
[23] D. Liu, X.-S. Hua, M. Wang, and H.-J. Zhang, "Retagging social images based on visual and semantic consistency," in Proc. 19th ACM Int. Conf. World Wide Web, 2010, pp.1149–1150.
[24] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proc. ACMSIGCOMMConf. Internet Meas. Conf., 2011, pp. 61–70.
[25] D. G. Lowe, (2004, Nov.). Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vis. [Online]. 60(2), pp. 91–110. Available: http://dx.doi.org/10.1023/B: VISI.0000029664.99615.94
[26] G. Loy and A. Zelinsky, "Fast radial symmetry for detecting points of interest," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 8, pp. 959–973, Aug. 2003.
[27] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the Facebook platform," in Proc. Web 2.0 Security Privacy Workshop, 2009.
[28] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.
[29] M. Rabbath, P. Sandhaus, and S. Boll, "Analysing facebook features to support event detection for photo-based facebook applications," in Proc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012, pp. 11:1–11:8.
[30] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[31] A. Singhal, "Modern information retrieval: A brief overview," IEEE Data Eng. Bullet., Speicial Issue on Text Databases, vol. 24, no. 4, pp. 35-43, Dec. 2001.
[32] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive policy prediction for shared images over popular content sharing sites," in Proc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp.261–270.
[33] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.
[34] X. Su and T. M. Khoshgoftaar, "A survey of collaborative filtering techniques," Adv. Artif. Intell., vol. 2009, p. 4, 2009.
[35] X. Sun, H. Yao, R. Ji, and S. Liu, "Photo assessment based on computational visual attention model," in Proc. 17th ACM Int. Conf. Multimedia, 2009, pp. 541–544. [Online]. Available: http:// doi.acm.org/10.1145/1631272.1631351
[36] H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev, "Multimedia semantics: Interactions between content and community," Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.
[37] A. Vailaya, A. Jain, and H. J. Zhang, (1998). On image classification: City images vs. landscapes. Pattern Recog. [Online]. 31(12), pp. 1921–1935. Available: http://www.sciencedirect.com/ science/article/pii/S003132039800079X
[38] R. A. Wagner and M. J. Fischer, "The string-to-string correction problem," J. ACM, vol. 21, no. 1, pp. 168–173, 1974.
[39] Wordnet - A lexical database for the English language. [Online]. Available: http://wordnet.princeton.edu/
[40] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in Proc. Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963
[41] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.
[42] J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.
[43] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.
[44] S. Zerr, J. H. Stefan Siersdorfer, and E. Demidova, (2012). Picalert! data set. [Online]. Available: http://l3s.de/picalert/
[45] N. Zheng, Q. Li, S. Liao, and L. Zhang, "Which photo groups should I choose? A comparative study of recommendation algorithms in flickr," J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010.
[46] J. Zhuang and S. C. H. Hoi, "Non-parametric kernel ranking approach for social image retrieval," in Proc. ACM Int. Conf. Image Video Retrieval, 2010, pp. 26–33. [Online]. Available: http://doi.acm.org/10.1145/1816041.1816047 Anna Cinzia Squicciarini
[47] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede,"privacy policy inference of user uploaded image on content sharing sites", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 1, JANUARY 2015 193