

Security Schedule Speculation of User-Uploaded Data in Content Sharing Sites

Krosuri Madhuri^{#1}, Dr K S M V Kumar^{#2}

[#]P.G. Scholar in CSE, [#] Professor & Principal, Department of CSE

Priyadarshini Institute of Technology & Sciences for Women, Tenali, Andhra Pradesh, India

Abstract: Social Network is efficient security and service for content sharing sites (CSS). It is efficient service users communication new attack ground for data hackers they can easily unused the data in the media. Some users over CSS affect user's security on their personal data. An Adaptive Privacy Policy Prediction (A3P) model helps users to compose security model for their data. We put forward this model consisting Adaptive Privacy Policy Prediction (A3P) framework to help users create security model for their data. To provide security for the data automated annotation of images is create the meta data information about the images by using the new model is called Semantic annotated Markova Semantic Indexing (SMSI) for take the data The proposed model automatically annotates the data using hidden Markov model and features extracted is using color histogram and scale invariant feature transform data sharing. We further propose many functions to uses in system recommended functions and provide security models. For user-specified functions We change secret small functions in which security is modify by hiding secret functions/algorithms.

Index Terms: Social networks · Privacy · Game theory · Clarke-Tax, content sharing sites, Meta data, Online social networks,

Photo tags. Semantic Markova Semantic Indexing, hidden Markov model.

1. INTRODUCTION

Social media is the two way communication in Web 2.0 and it means to communicate share, and interact with an individual or with a large audience. Today for every single piece of content shared on sites like Face book every wall post, photo, status update, and video the up loader must decide which of his friends, group members, and other Face book users is access the content. As a result, the model of security sites like Face book is received significant attention in both the research community [1] and the mainstream media [2]. Our goal is to improve the set of security controls and defaults, but we are limited by the fact that there has been no in depth study of users security settings on sites like Face book. While significant privacy violations and insufficient user expectations are likely to exist the extent to which such privacy violations occur has yet to be quantified.

To prevent such kind of unwanted disclosure of personal images, flexible privacy settings are required. Content Based Image Retrieval (CBIR) is model s to organize digital image archives by visual content basis many ranging from an image similarity function to a robust image annotation engine falls under the purview of CBIR.

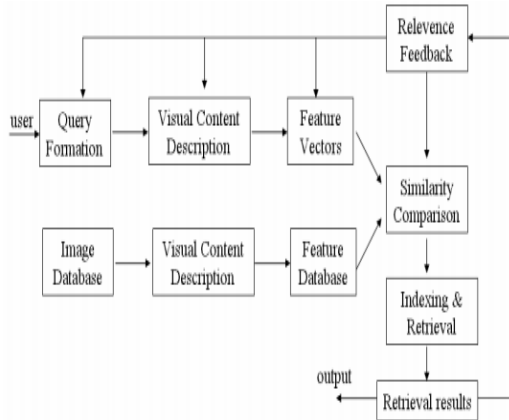


Figure 1: Diagram for content-based image retrieval system

The security strategy of client transferred picture is given in view of the client transferred picture substance and metadata..

2. RELATED WORK

Content-based retrieval [2] is ultimately dependent on the features used for the annotation of data and its efficiency is dependent and robust properties. The Polar Fourier Transform (PFT) is same to the Discrete Fourier Transform in two dimensions uses transform parameters radius and angle rather than the Cartesian coordinates [6]. 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 performance to contemporary model. Equal performance in the images tested while offering significant savings in both the computation required and the complexity of the implementation. Security and privacy in Social networks is generally in Web 2.0 are emerging as important and crucial research topics [7]. SNs have been studied by scholars from different disciplines: sociologists, HCI, computer scientists, economists. Many studies have been conducted to investigate users security attitudes and possible risks

which users face when poorly security their personal data [19] in SNs. Gross et al. [2] provided an interesting analysis of users' security attitudes across SNs. Interestingly [17] have highlighted that on-line friendships is result in a higher level of disclosure due to lack of real-world contact. [17] There is many benefits in social capital as a result of sharing information in a SN that may limit the desirability of extensive privacy controls on content.

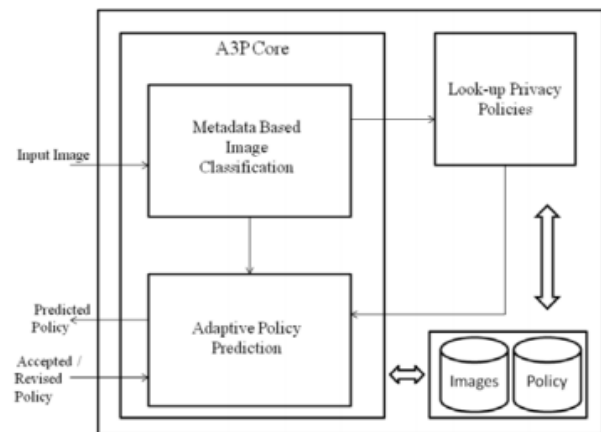


Figure2: Adaptive Privacy Policy Prediction (A3P) system Architecture

A3P Framework

The 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 security settings for their images. In this framework a two level framework is introduced is called as Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle security settings by automatically generating personalized privacy policies.

a. A3P Architecture

A3P stands for Adaptive Privacy Policy security system which helps users to derive the privacy settings for their images The A3P Architecture consists of followings

blocks: A3P Core. 1. Metadata based Image classification. 2. Adaptive policy prediction. 3. Look-Up Privacy Policies 4. Database If similar type of image exist then it looks for all the policies and lets user choose the policies.

b. A3P Algorithm

Access control in the shared location is one of the essential one. Access control mechanism (ACM) is one of the security conserve one. ACM permit users to oversee access to data controlled in own spaces users have no control over data be inherent in outside their spaces data [15, 16]. In large-sample scenery the protection suite model favored by BIC if possible communicate to the competitor model which is a posteriori most probable the model which is provides most plausible by the data at hand.

c. Algorithm:

1 Let y denote the observed data.
 2 Assume that y is to be described using a model M_k selected from a set of neighbour models $M_{k_1}, M_{k_2}, \dots, M_{k_L}$.
 3 Assume that each M_k is uniquely parameterized by a vector θ_k , where θ_k is an element of the parameter space $\Theta(k)$ ($k \in \{k_1, k_2, \dots, k_L\}$).
 4 Let $L(\theta_k | y)$ denote the likelihood for y based on M_k .
 Note: $L(\theta_k | y) = l(y | \theta_k)$.
 5 Let $\hat{\theta}_k$ denote the maximum likelihood estimate of θ_k obtained by maximizing $L(\theta_k | y)$ over $\Theta(k)$.
 6 We assume that derivatives of $L(\theta_k | y)$ up to order two exist with respect to θ_k , and are continuous and suitably bounded for all $\theta_k \in \Theta(k)$.
 7 The motivation behind BIC can be seen through a Bayesian development of the model selection problem.
 8 Let $\pi(k)$ ($k \in \{k_1, k_2, \dots, k_L\}$) denote a discrete prior over the models $M_{k_1}, M_{k_2}, \dots, M_{k_L}$.
 9 Let $g(\theta_k | k)$ denote a prior on θ_k given the model M_k ($k \in \{k_1, k_2, \dots, k_L\}$).
 Applying Bayes' Theorem, the joint posterior of M_k and θ_k can be written as

$$h(k, \theta_k | y) = \frac{\pi(k) g(\theta_k | k) l(\theta_k | y)}{m(y)}$$
 where $m(y)$ denotes the marginal distribution of y .
 The term involving $m(y)$ is constant with respect to k ; thus, for the purpose of model selection, this term can be discarded.

In Bayesian applications is comparisons many models is over and over again based on Bayes factors. The model which is a posteriori most likely is determined by

whether the Bayes factor is less than or greater than one [17].

3. PROPOSED ALGORITHM

The proposed model is introduced Semantic annotated Markova Semantic Indexing (SMSI), many semantic retrieval of images is done based on Hidden Markov model based annotated images. Annotation based image retrieval phase give user query and then finds similar terms for the query with the help of Word Net. Also discover the similarity many the query and images in annotated image database. Then find similarity many matching images. The system carries two major approaches.

- Automatic image annotation
- Annotation based image retrieval

Automatic image annotation phase is use of a manually annotated training set taken to generate an annotated image database. Annotation based image retrieval phase gets a user query Also find the similarity many the query and images in annotated image database.

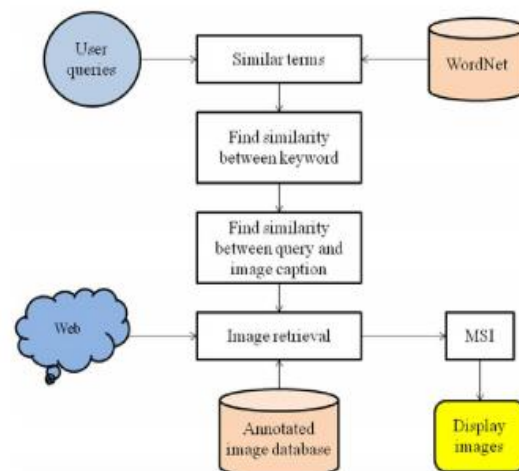


Figure 3 System Architecture

1. Color Histogram Feature

Color histogram is simplest and most frequently used to represent color. A number of color spaces have been used such as

RGB, LUV, and HSV. Once the color space is specified color feature can be extracted from images. Then the histogram values are computed for gray level variations. According to histogram values, images are extracted from the database.

2. Textures Feature Extraction

In this section, Texture feature is extracted by using SIFT (Scale-invariant feature transform) descriptor [10]. Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to find and describe texture features in images

3. SIFT Descriptors

SIFT analysis involves detecting salient locations in an image and extracting descriptors that are distinctive yet invariant to changes in viewpoint illumination. The standard SIFT interest point detector and the standard SIFT histogram-of-gradients descriptor is used. These 128 dimension descriptors can be thought of roughly as summarizing the edge information in an image patch centered at an interest point. This global descriptor is a frequency count of the quantized local descriptors.

4. Database updation with HMM annotated images

Hidden Markov Model is provides [8] Estimating the parameters of the model from annotated image+ caption pairs. and Computing the like lipoid of a caption-word stating present in an image Let a collection of image+ caption pairs is provided and consider the problem of developing a stochastic generative model that jointly describes every pair.

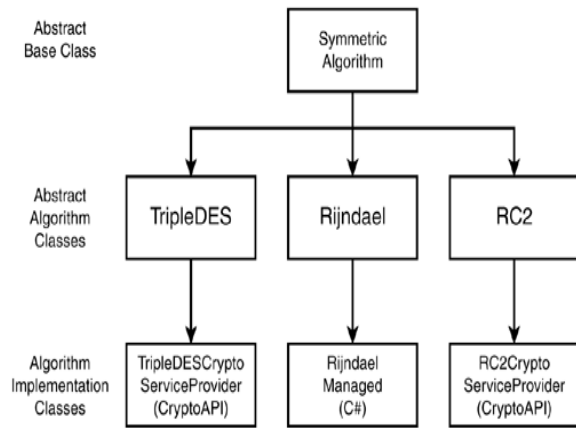
5. Modeling Social Context

We observe the users with similar background tend to have similar security

concerns in previous research studies and also confirmed in our collected data. The social context modeling algorithm consists of two main steps. The first step is to identify and formalize potentially important factors that may be informative of one's security settings. The second step is to group users based on the identified factors. First we model each user's social context as a list of attributes: {sc1, sc2, ..., scn} where sci denote a social context attribute and n is the total number of distinct attributes in the social networking site.

RIJNDAEL'S ALGORITHM

Rijndael (pronounced rain-dahl) is the algorithm is selected by the U.S. National Institute of Standards and Technology (NIST) as the candidate for the Advanced Encryption Standard (AES). It was selected from a list of five finalists that were themselves selected from an original list of more than 15 submissions. Rijndael will begin to supplant the Data Encryption Standard (DES) and later Triple DES - over the next few years in many cryptography models. The algorithm is designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen, whose surnames are reflected in the cipher's name. Rijndael has its origins in Square. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks in excess of AES design criteria, the block sizes is mirror those of the keys. The blocks can be interpreted as one-dimensional arrays of 4-byte vectors.



A. Collective Privacy Decisions

The most intuitive model is aggregate users decisions is to let owners iteratively disclose their preferred settings and explicitly agree in possible viewers each owner proposes to include. This method is hardly applicable in that it requires all the owners to agree on a single set of security policies which may sometimes be an endless task. Since SN users typically access the network independently this model is pretty simplistic and fails to leverage the individuals' preferences within the co-owners group. In addition to the identified drawbacks main and ranking based model such as the ones described is proved to be unfair in that astute individuals may manipulate outcomes to their advantage [20].

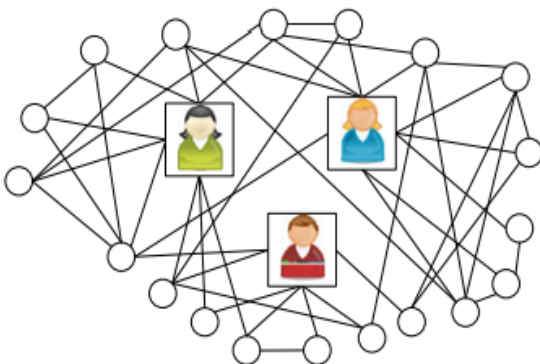


Fig. 5 Example of combined co-owner graph

B. IMPROVING PRIVACY TOOLS

As our final point of analysis we examine the potential for assisting users in managing

their security. Specifically we focus on friend lists, a mechanism for users to group their friends that is same to the Circles feature of Google+. We explore every friend lists could be automatically populated using community detection algorithms [16] over the social network. To verify the extent to users in friend lists form closely connected communities we examine the normalized conductance [11] of the existing friend lists whose value ranges from -1 to 1, with strongly positive values indicating significant community structure. We analyzed the conductance values for our 233 friend lists and we found a significant positive bias. Over 48% of the friends lists have values larger than 0.2, suggesting that a large fraction of friend lists could be automatically inferred from the social network.

C. Social-graph visualization

It would help users make more well-informed and better decisions about their security settings This interface is a series of tabbed pages every page presents a separate audience view of a profile many controls is taken. Authors is currently iteratively prototyping their proposed interface. In first iteration the audience view is created and examined without any model for modifying settings similar to Orkut interface. This access verifying that this visual feedback is useful and provides guidance for continued design. The prototype, shown in Fig. 2 and Fig. 3, adds a set of tabs for each audience

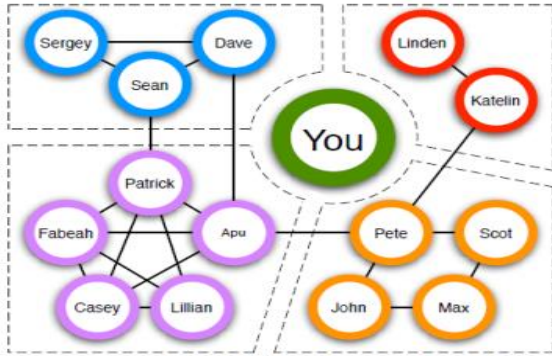


Figure 6: Visualization of social circle [7]

4. EXPERIMENTAL EVALUATION

The comparison between existing and the proposed system (see figure 3.0). In the proposed system is access of the pages is limited and compared to existing system. This based type of model is generates access-control policies from photo administration tags. Every photo is integrated with an access grid for mapping the photo with the participant's friends. The contestant is select a suitable partiality and access the information. Photo tags is categorized as directorial or forthcoming based on the user needs

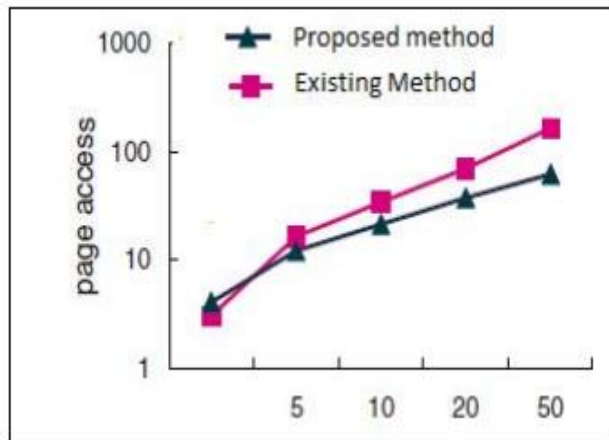


Figure 7: Difference between Existing and Proposed

5. CONCLUSION

Social network is an upgrading media for data sharing through internet. We have studied and approached towards adaptive

privacy policy prediction users for maintaining the security of their uploaded images by automatically recommending security policies. The present work proposes Semantic annotated Markova Semantic Indexing (SMSI) a semantic image retrieval is done and its result is improved by incorporating an automatic annotation system. Automatic annotation of images in database is using a proposed Hidden Markov model extracted features (color and texture) where all states represent the concepts. Semantic same image retrieval can be done with the use of Natural language processing tool namely Word Net where conceptual similarity between natural language terms were done. Comparative result users better result for proposed system rather than existing retrieval system of framework.

6. FURTHER WORK

We plan is implement our analysis concerning the systems modify is elaborating on colluding users. Currently users can choose to undo the auction and update the security preferences. In this paper different methods is studied which make privacy setting easier for user. User social environment and characteristics and image content and its metadata is useful to predict security policy for user. Using all this content and above methods privacy recommendation is easier.

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] 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.

[3] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. CHI, 2007.

[4] Sangeetha. J, Kavitha. R, “An Improved Privacy Policy Inference over the Socially Shared Images with Automated Annotation Process”

[5]. Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, “Tag, You Can See It! Using Tags for Access Control in Photo Sharing”, Conference on Human Factors in Computing Systems, May 2012.

[6] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, “Capturing social networking privacy preferences,” in Proc. Symp. Usable Privacy Security, 2009.

[7] K. A. Raftopoulos, K. S. Ntalianis, D. D. Soutlas, and S. D. Kollias, Mining user queries with markov chains: Application to online image retrieval," Knowledge and Data Engineering, IEEE Transactions on, Vol. 25, 2013.

[8] A. Ghoshal, P. Ircing, and S. Khudanpur, Hidden markov Models for automatic annotation and content-based retrieval of images and video," in Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval. ACM, 2005.

[9] D. M. Blei, A. Y. Ng, and M. I. Jordan, Latent dirichlet allocation, The Journal of machine Learning Research, Vol. 3, 2003.

[10] F. Yu and H. H.-S. Ip, “Automatic semantic annotation of images using spatial hidden markov model," in Multimedia and

Expo, 2006 IEEE International Conference on IEEE, 2006

[11] 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.

[12] 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.

[13] 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

[14] R. Datta, D. Joshi, J. Li, and J. Wang. Image retrieval: Ideas, influences, and trends of the new age. ACM Computing Surveys (CSUR), 40(2):5, 2008.

[15] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei. What does classifying more than 10,000 image categories tell us? In 11th European conference on Computer vision: Part V, ECCV’10, pages 71–84, Berlin, Heidelberg, 2010. Springer-Verlag.

[16] A. K. Fabeah Adu-Oppong, Casey Gardiner and P. Tsang. Social circles: Tackling privacy in social networks. In Symposium On Usable Privacy and Security, 2008.

[17]. R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, “Capturing social networking privacy preferences,” in Proc. Symp. Usable Privacy Security, 2009.

[18]. 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



[19] 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.

[20] A. Mazzia, K. LeFevre, and A. E., "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012

AUTHOR DETAILS

Krosuri Madhuri born in Thummapudi, Duggirala, Guntur Dt, AP. I received MCA from K.Chandhrakala P.G College, Nelapadu, Tenali, Guntur dt, AP, ANU Guntur in the year 2011. Presently she is pursuing M.TECH in CSE from Priyadarshini Institute of Technology & Science for Women, Chinthalapudi, Duggirala Md, Guntur Dt, and Andhrapradesh, India.



Dr. K S M V KUMAR is presently a Professor of Computer Science & Engineering, Principal (PRIYADARSHINI INSTITUTE OF

TECHNOLOGY AND SCIENCE, TENALI) and Executive Council Member, Advanced Computer Machinery (ACM) India Chapter. He served and held several Academic and Administrative positions including VICE principal, Dean Academics and Administration HOD for CSE Head of the Department, He did his 10th standard from Z.P.H.S. Parimella, Intermediate from Dr.G.G.Degree college, T.P gudem, Andhra Pradesh in 1989, B.E.(ECE) from Nagarjuna University College of Engineering, Guntur in 1997, M.Tech from Jawaharlal Nehru

Technological University(JNTUH), Hyderabad in 2002 and Ph.D from Jawaharlal Nehru Technological University, Hyderabad in 2014. He is the recipient of 3 Pride of Asia International Award, International Intellectual Development Award and Mother Teresa Award for Outstanding Services, Achievements, Contributions, Meritorious Services, Outstanding Performance and Remarkable Role in the field of Education and Service to the Nation. He is a Member on the Editorial Boards for five International Journals., 35 M.Tech, more than 100 B.Tech projects and he has published 22 research papers at International/National Journals/Conferences including IEEE, ACM, Springer, Elsevier and Inder Science. He has 22 years of Teaching and Research experience.