International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Segregation Approach for User Sending Data on Content Sharing Sites

Thalakola Syam Sundara Rao [#1], **O Srinivas** [*2]
[#] *M. Tech student in CSE, PNC & VIJAI Institute of Engineering & Technology, Repudi, Phirangipuram, Andhrapradesh, India*
[*] *Assistant Professor, Dept. of CSE*
PNC & VIJAI Institute of Engineering & Technology, Repudi, Phirangipuram, Andhrapradesh, India

Abstract: Social Network is an emerging E-service for content sharing sites (CSS). It is efficient service which users communication through this communication a 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. The need of tools to help users control access to their shared data is separate. 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 measures for their data. The role of images and its metadata are changed as a measure of user security models. The Framework determines the best security approach for the uploaded data. To provide security for the data, automated annotation of images is introduced to create the meta data information about the images by using the new approach is called Semantic annotated Markova Semantic Indexing (SMSI) for retrieving 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.. The collations data result in unexpected exposure of one's social locations and lead to abuse of one's personal information. We further propose different functions to uses in system recommended functions and provide a security models. For user-specified functions we change secret small functions in which security is enhanced 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.*

I. 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. 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. Twitter, Face book, LinkedIn and Google Plus seems to be the most popular Social networking websites on the Internet. 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 should be able to access the content. As a result, the issue of privacy on sites like Face book has received significant attention in both the research community [1] and the mainstream media [2]. 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 Face book. While significant privacy violations and mismatched 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. In recent years, such privacy settings are made available but setting up and maintaining these measures. 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, Online social networks (OSNs) have experienced huge growth in recent years and become a de-facto portal for hundreds of millions of Internet users.

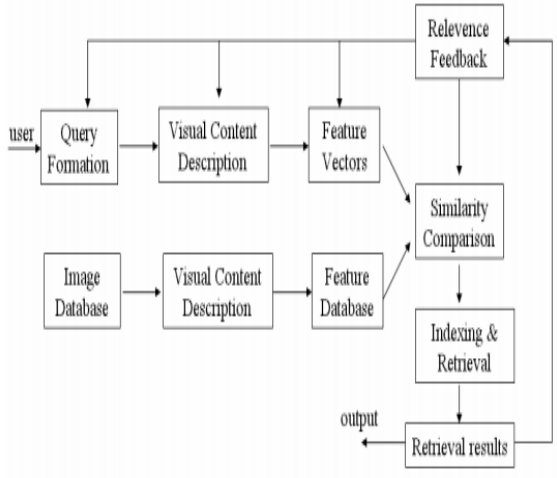


Figure 1: Diagram for content-based image retrieval system

The protection strategy of client transferred picture can be given in view of the client transferred picture's substance and metadata. A progressive picture arrangement which orders images initially in light of their substance and afterward refine every classification into subcategories in light of their metadata Images that don't have metadata will be assembled just by substance.

II. RELATED WORK

Content-based retrieval [2] 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.[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 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. Security and privacy in Social networks and more 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 etc. In this section, we overview some of previous work that is most relevant to collective privacy management for SNs Several studies have been conducted to investigate users' privacy attitudes and possible risks which users face when poorly protecting their personal data [19] in SNs. Gross et al. [2] provided an interesting analysis of users' privacy attitudes across SNs. Interestingly [17] have highlighted that on-line friendships can result in a higher level of disclosure due to lack of real-world contact. [17], there are benefits in social capital as a result of sharing information in a SN that may limit the desirability of extensive privacy controls on content. Following such considerations, the approach we present in this work does not simply block users' accessibility to shared data

III. 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 hassle free privacy settings by automatically generating personalized privacy policies.

a. A3P Architecture

A3P stands for Adaptive Privacy Policy Prediction 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

A3P Core classifies the images with the help of the Metadata and also predict the policies depending upon the behavior of the user. The Look-up Privacy Policy looks if the image or similar type of image already exists which can be given with similar privacy policies. If similar type of image doesn't exist then it looks for all the policies and lets user choose the policies.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

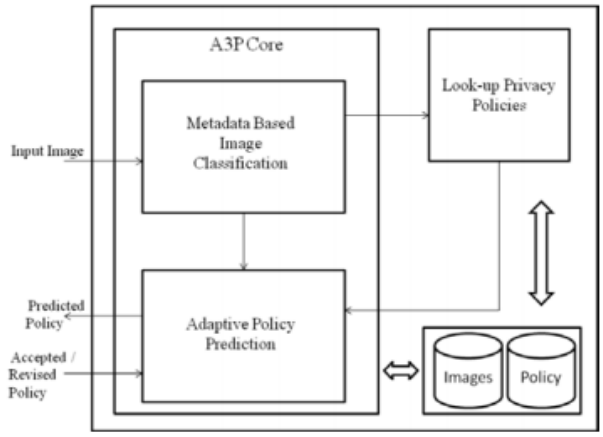


Figure2: Adaptive Privacy Policy Prediction (A3P) system Architecture

b. A3P Algorithm

Access control in the shared environment is one of the essential one. To supply a secure access we have to limit the unauthorized user in these networks. Access control mechanism (ACM) is one of the privacy conserve one. ACM permit users to oversee access to information controlled in own spaces, users, unhappily, have no control over data be inherent in outside their spaces [15, 16]. For example, Facebook allows label users to eliminate the tags associated to their profiles or report contravention asking Facebook managers to eliminate the contents that they do not want to split among the public In large-sample scenery the en suite model favored by BIC if possible communicate to the competitor model which is a posteriori most probable the model which is provide 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 $M_{k_1}, M_{k_2}, \ldots, M_{k_L}$.
3 Assume that each M_k is uniquely parameterized by a vector θ_k, where θ_k is an element of the parameter space $\Theta(k)$ $(k \in \{k_1, k_2, \ldots, k_L\})$.
4 Let $L(\theta_k \mid y)$ denote the likelihood for y based on M_k.
Note: $L(\theta_k \mid y) \quad f(y \mid \theta_k)$.
5 Let θ_k denote the maximum likelihood estimate of θ_k obtained by maximizing $L(\theta_k \mid y)$ over $\Theta(k)$.
6 We assume that derivatives of $L(\theta_k \mid y)$ 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 $\pi(k)$ $(k \in \{k_1, k_2, \ldots, k_l\})$ denote a discrete prior over the models $M_{k_1}, M_{k_2}, \ldots, M_{k_l}$.
9 Let $g(\theta_k \mid k)$ denote a prior on θ_k given the model M_k $(k \subset \{k_1, k_2, \ldots, k_L\})$.
Applying Bayes' Theorem, the joint posterior of M_k and θ_k can be written as

$$h((k, \theta_k) \mid y) = \frac{\pi(k)\, g(\theta_k \mid k)\, l(\theta_k \mid y)}{m(y)},$$

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, pair wise comparisons between models are over and over again based on Bayes factors. Presumptuous two candidate models are regarded as equally probable a priori, a Bayes factor correspond to the ratio of the posterior likelihood of the models. The model which is a posteriori most likely is determined by whether the Bayes factor is less than or greater than one [17].

IV. PROPOSED ALGORITHM

The proposed system introduced Semantic annotated Markovian Semantic Indexing (SMSI), a novel semantic retrieval of images is done based on Hidden Markov model based annotated images. Automatic image annotation phase makes use of a manually annotated training set taken to generate an annotated image database. Annotation based image retrieval phase gets a user query, and then finds similar terms for the query with the help of WordNet. Also discover the similarity between the query and images in annotated image database. Then find the similarity between matching images. The system carries two major tasks.

- Automatic image annotation
- Annotation based image retrieval

Automatic image annotation phase makes use of a manually annotated training set taken to generate an annotated image database. Annotation based image

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

retrieval phase gets a user query, then find similar terms for the query with the help of Word Net. Also discover the similarity between the query and images in annotated image database.

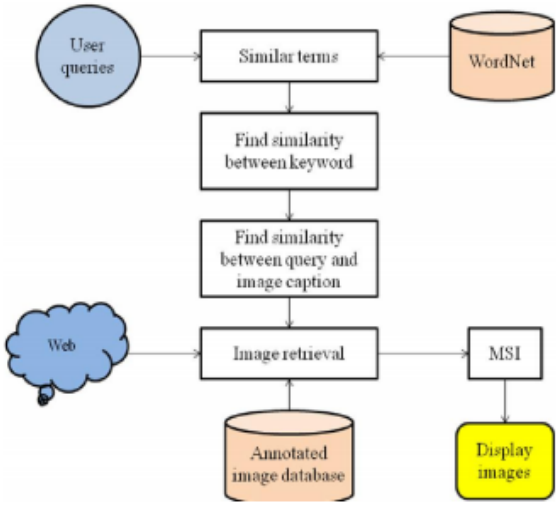


Figure 3 System Architecture

4.1. Color Histogram Feature

Color histogram is simplest and most frequently used to represent color. The color histogram serves as an effective representation of the content. Color is one of the most important features of images. Color features are defined subject to a particular color space or model. 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 or regions. An important color features namely color histogram is extracted. Color histograms are frequently used to compare images. In this gray level variations are used to compute the histogram of any image. For this purpose the color image is first converted in to gray level image. Then the histogram values are computed for gray level variations. According to histogram values, images are extracted from the database.

4.2. Textures Feature Extraction

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

4.3. SIFT Descriptors

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

4.4. Database updation with HMM annotated images

Hidden Markov Model, provides [8] Estimating the parameters of the model from annotated image+ caption pairs. Aligning image-regions with caption-words in an image+ caption pair, and Computing the likelihood of a caption-word being present in an image Let a collection of image+ caption pairs be provided and consider the problem of developing a stochastic generative model that jointly describes each pair.

IV. MODELING SOCIAL CONTEXT

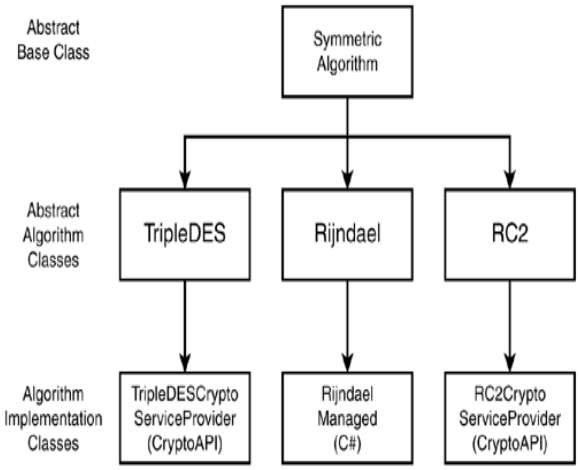
We observe that users with similar background tend to have similar privacy concerns, as seen in previous research studies and also confirmed by our collected data. This observation inspires us to develop a social context modeling algorithm that can capture the common social elements of users and identify communities formed by the users with similar privacy concerns. 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. 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. These social context attributes are extracted from users' profiles. Besides basic elements in users' profiles, many social sites also allow users to group their contacts based on relationships

V. RIJNDAEL'S ALGORITHM

Rijndael (pronounced rain-dahl) is the algorithm that has been 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 applications. The algorithm was 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, an earlier collaboration between the two cryptologists. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. The blocks can be interpreted as unidimensional arrays of 4-byte vectors.



A. Collective Privacy Decisions

The most intuitive approach to aggregate users' decisions is to let co-owners iteratively disclose their preferred settings and explicitly agree on the set of possible viewers each owner proposes to include. Owners could update their preferences as they view other owners' preferred settings and try to reach a common decision on a single policy after a few rounds of revision of their internal settings.

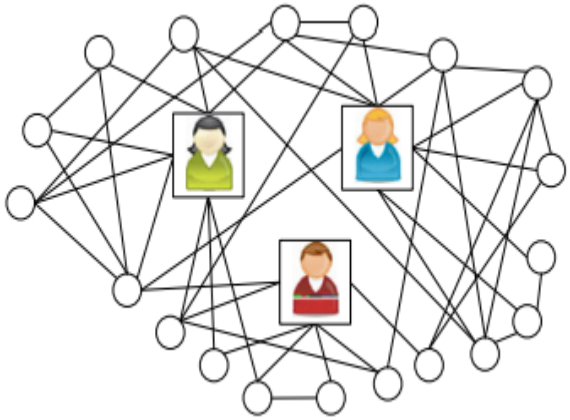


Fig. 5 Example of combined co-owner graph

This approach, however, is hardly applicable in that it requires all the owners to agree on a single set of privacy policies, which may sometimes be an endless task. Since SN users typically access the network independently, it is also hard to force synchronization, without introducing unacceptably long decision processes. A more conservative solution is to construct a privacy policy that allows viewers' rights only to the set of users who satisfy each of the owners' preferences, avoiding the need of the owners' explicit consent on the final set of viewers. However, this approach is pretty simplistic and fails to leverage the individuals' preferences within the co-owners' group. In addition to the identified drawbacks, majority and ranking based approaches, such as the ones described above, have proved to be unfair, in that astute individuals may manipulate outcomes to their advantage [20].

B. Improving Privacy Tools

As our final point of analysis, we examine the potential for assisting users in managing their privacy. Specifically, we focus on friend lists, a mechanism for users to group their friends that is similar to the Circles feature of Google+. We explore whether the friend lists could be automatically populated using community detection algorithms [16] over the social network. To do so, we examine the friend lists of our 200 surveyed users using the Face book API. The cumulative distribution of the sizes of the 233 friend lists More than 50% of friend lists have more than 10 members, while 20% of the lists have more than 30 members, which indicates the potential difficulties with manually generating and maintaining such large lists of friends. To verify the extent to which 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.

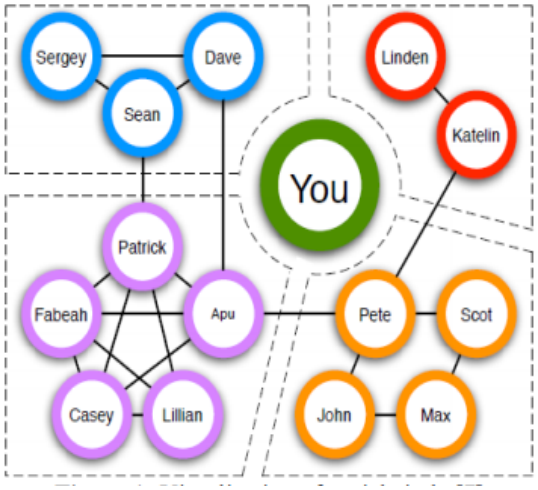


Figure 6: Visualization of social circle [7]

C. Social-graph visualization

Visualize the social circles of users. It would help users make better informed and hence better

decisions about their privacy settings. This will help the user associate privacy settings with how their information is presented to different people group instead of the lists of privacy menus. This interface is a series of tabbed pages, where each page presents a separate audience view of a profile, along with controls for showing or hiding information to that group. Authors are currently iteratively prototyping their proposed interface. In first iteration, the audience view is created and examined without any mechanism for modifying settings, similar to Orkut's interface. This allows 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

VI. EXPERIMENTAL RESULTS

The diverse between existing and the proposed system (see figure 3.0). In the proposed system the access of the pages were limited when compared to existing system. Access control is by provided that access rights in a SN are limited to few basic constitutional rights, such as read, write and play for media content. This based type of approach which 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 can select a suitable partiality and access the information. Photo tags can be categorized as directorial or forthcoming based on the user needs

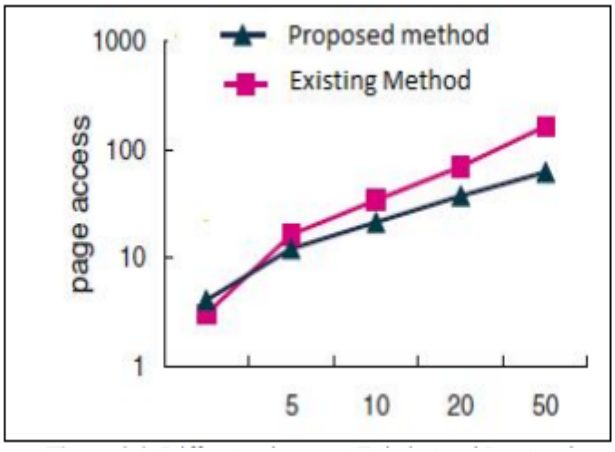


Figure 7: Difference between Existing and Proposed

VII. CONCLUSION

Social network is an upgrading media for information sharing through internet. It provides a content sharing like text, image, audio, video, With this emerging E-service for content sharing in social sites privacy is an important issue. We have studied and approached towards adaptive privacy policy prediction users for maintaining the privacy of their uploaded images by automatically recommending privacy policies. This system provides a framework which deduces privacy preference based on the history of the users proclivity. This help user to set hassle free and flexible policy. The present work proposes Semantic annotated Markova Semantic Indexing (SMSI) a semantic image retrieval is done and its performance improved by incorporating an automatic annotation system. Automatic annotation of images in database has been done by using a proposed Hidden Markov model which uses the extracted features (color and texture) where all states represent the concepts. Semantic similarity based 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 provides better result for proposed system rather than existing retrieval system of framework.

VIII. FURTHER WORK

We plan to extend our analysis concerning the systems manipulation by elaborating on colluding users. our approach should be able to reflect this if necessary. Currently, users can choose to undo the auction and update the privacy preferences. In this paper, different methods are studied which make privacy setting easier for user. User's social environment and characteristics, and image's content and its metadata are useful to predict privacy policy for user. Using all this content and above methods privacy recommendation can be 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. Sourlas, 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.

Thalakola Syam Sundara Rao born in Phirangi Puram, Guntur Dist., Andhrapradesh He received M.Sc (Information systems) in Computer science from SS&N (Sri Subbaraya & Narayana) college, Narasaraopet, Guntur, AP, Nagarjuna University in the year2003. Presently I am pursuing M.TECH in CSE from Paladugu Nagaiah Chawdary & VIJAY, Repudi, Guntur, Andhrapradesh, India. I attended various national level technical symposiums.

O.SRINIVAS is an assistant professor department of CSE at P.N.C & VIJAI Institute of engineering and technology, Guntur. He received M.Tech in computer science and engineering from JNTUK. He gained 3 years of experience in teaching. He is a good researcher in programming.