ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.11

# Capturing Social Networking Privacy Preferences Via Image Contents

Pawar Vishal Dattatray[1], Shinde Amol Ashok[2], Kadam Shubham Bajirao[3], Karhale Sandip Bhausaheb[4], Phulari s. V[5]
B.E Student[1, 2, 3, 4], Associate Professor[5]
Department of Computer Engineering
Pune District Education Association's College of Engineering, Pune, India

**Abstract:**
Now-a-days, the increasing volume of images users share through social networking sites, maintaining privacy has become a problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. The need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We propose a two-level framework which according to the user's available history on the sites determines the best available privacy policy for the user's images being uploaded. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.

**Keywords:** Image processing, NLP, online information services, text mining, web-based services.

## 1. INTRODUCTION

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 apparent. Towards addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We propose 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.

### 1.1 Goals and objectives

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

### 1.2 Scope of Statement

• The product scope of designed project is efficient handling of information, communication, and interoperability for request and receives information.

• To enhance the experience of mobile application.

• This application Location and can be used by any Android mobile user and any Smartphone User. WI-FI is must for some services in this application.

• Users can use the sensors which are built in sensors of smartphones and by using these sensors user can use this application.

## 2. SOFTWARE CONTEXT

The system will be using the image content, detect the unwanted image and providing security to all users. Following are the context of our product:

- The Product will be useful for security.
- The system can be access from Anyone, Anywhere, Anytime.
- Check the Image content and detect the unwanted image.
- High secured user authenticate
- NLP algorithm uses on the Image Content.
- Image Classification into group

## 3. METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY ISSUES

We propose a user profile model which aims to provide users privacy setting experience by providing policies. Also to provide more security to images uploaded by user compare to other system. In general, similar images often incur similar privacy preferences, especially when people appear in the images. Using User profile model, Photo sharing/ content sharing websites allow or maintain privacy for the User Profile instead for only contents which leads more security. That means when user uploads an image, it will sent to our System. The System classifies the images based on their content like size, texture and metadata like tags, comments. Here for the extraction of the features of images we are using Single hierarchical algorithm.

## 4. MODULES OF THE PROJECTS

**4.1 Profile based user model:** In this stage, after generation of user profiles, system generates user notification

wall for each user who socially connected to each other. In this first step is to load user profiles from database. The actions (tag, comment, view download and upload) determine user profile, so for each action profile list is generated like uploaded Profile, view Profile, download Profile etc. contents and metadata the user profile is generated on the basis of user actions i.e. tag, comment, download and view. Classifier generates the classes using cosine similarity. On the basis of classification images and metadata system generates the user profiles having similar policies of images which are uploaded by user. Using this Data, profile based model is created.

### 4.2 Privacy Policy model:

The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user. Thus, we present an approach to choose the best candidate policy that follows the user's privacy tendency.

## 5 MATHEMATICAL FORMULATION

### 5.1 Module 1

User account Validation and Forgot Password
Let S1 be a set of parameters for Proper user validation
S1= User Validation, Image Select
If user want to create the Account
then user proper validation and selected image completely then
Login to user account
If already account is created then only checks the user name and password
If user forgot the password then user wants to select the image,
Then system sends the OTP and get changed password.

### 5.2 Module 2

Image Processing
Let's S2 be a set of user data
S2=Image File
Where,
Image File = user upload image
The image contents check using the NLP, Image Processing Algorithm
If image verify
Then image upload in that particular group
If image content in warning content
Then block the image if user uploads this file then system sends the OTP

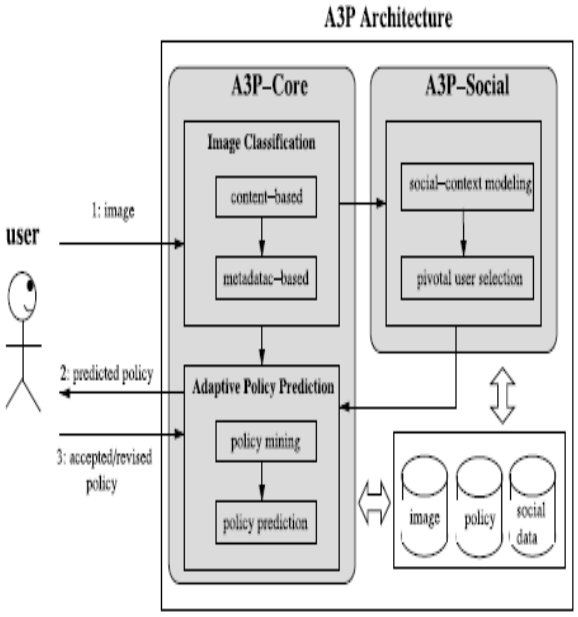
## 6 PROPOSED METHODOLOGY ARCHITECTURE

### 6.1 The role of image's content and metadata

In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos. He may upload some other photos of landscapes which he took as a hobby and for these photos, he may set privacy preference allowing anyone to view and comment the photos. Analyzing the visual content may not be sufficient to capture users' privacy preferences. Tags and other metadata are indicative of the social context of the image, including where it was taken and why and also provide a synthetic description of images, complementing the information obtained from visual content analysis.

### 6.2 Algorithm in A3P-core

Algorithm in A3P-core (that is now parameterized based on user groups and also factors in possible outliers), and a new A3P-social module that develops the notion of social context to refine and extend the prediction power of our system. We also conduct additional experiments with a new data set collecting over 1,400 images and corresponding policies, and we extend our analysis of the empirical results to unveil more insights of our systems performance.




## 7. APPLICATIONS

- **To detect the unwanted image:**

Example, user an upload the image which is image contents doubtful to uploading image so detect the image and cannot upload the image.

- This also can be used for image security

## 8. CONCLUSION

This proposed system that helps to users automate the privacy policy settings on their uploaded images on social networking sites using an Adaptive Privacy Policy Prediction (A3P). This system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. This study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

## 9. REFERENCES

[1]. R. da Silva Torres and A. Falc~ao, "Content-based image retrieval: Theory and applications," Revista de Inform_ aticaTe_ orica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.

[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].SergejZerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova, I Know What You Did Last Summer!: Privacy-Aware Image Classification and Search , Proceedings of the 35th

international ACM SIGIR conference on Research and development in information retrieval, 2012.

[4].Kambiz Ghazinour, Stan Matwin and Marina Sokolova, "Your privacy protector: A Recommender System For Privacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management ( IJSPTM) Vol 2, No 4, August 2013.

[5]. Mehmet Erkan Yüksel and Asım Sinan Yüksel, "An Application for Protecting Personal Information on Social Networking Websites", the Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2010