

# A Machine Learning Based Technique for Automating Privacy Settings of Shared Images in Social Site

Shruti Tornalker, Dr. P. Sandhya

**Abstract**— It is well known fact that privacy has being one of the major concerns the photographs that might not want somebody else to see because of our wrong privacy settings might just get into the other peoples timeline. So, in order to avoid this problem of unnecessarily making every photograph as public or publishing the photograph with privacy policy we intend to develop a project which provides content based privacy to the images. Content Based Privacy (content based privacy means that the images is of different types for example

images containing kids so and so) this images can be identified through image content matching algorithm every image is composed of certain combination of pixels. Each pixel represents certain texture, color, shapes. By properly identify the texture, color, shape of an Image we can find out category of image weather. Whenever we initially start accessing a site our behavior is remembered by the system that means which type of photo that we are sharing with friends, which type of the photo that we are sharing with family and which of the type of photo that we are sharing with everyone.

Based on both metadata that is text information as well as image content that is color, texture and shape then as the user publishes new photograph every photograph will be matched with his previous image content. For example, if we give a new image then it will extract features and matches with the previous one it automatically predicts the policy. Then even if you forget to change the privacy setting of the images this photograph should be easily able to tag this means changing the privacy setting of the image such that only family members or other groups which we want will be able to see without setting each time.

**Index Terms**— Content Based Privacy, Metadata, Content matching algorithm.

## I. INTRODUCTION

Current time we share a lot of photos specifically in the social networking sites like “face book” and “flicker”. Now privacy is one of the major concerns with our photos there are few hobby photos that we take which we want everybody to see for instance, we go out some places we see some sceneries and we post that in “face book”, in “twitter”, “flicker”. Which we make want all our friends to see whenever there is a new born baby in the family we generally mitigate that photo through “whatsapp” such that our family members are able to see how about the facility is available in almost all social

networking. So for example the kids photograph we want to see we want only our family members to see similarly there were few photographs which we want only our college group to see. For example, a group photo taken in the class room, for example we share a study group and we take some photographs of certain notes. We want certain groups to be seen those photographs. In the groups also we might have various interest groups for example, we might be having a group which is say for example, archeological science group which shares and which uses the photo trap of various archeological science now whenever we post a photograph by default it goes to the default privacy setting for different user for different photos user has to select various privacy settings more often or not we tend to forget to set such privacy settings because it is quite a tedious process. We need to select a group, we need to tag a particular group and so and so far content based privacy is used to develop a project.

We can find out the category of the image from the text that we put with the image. for example, somebody posting his new born kids photo will invariably write something like our baby born on so and so date or we are lucky an up to have a baby. So immediately we can understand that the photo is associated with the category called baby or its content is that of the baby of that person. Now as the person keeps on sharing his photographs with some privacy setting at the beginning for example baby’s photo for only family members, for example his classmates photographs only for classmate members for example sports photograph only for group associated with sports for example the photographs of various building with archeological survey group. So once the user starts seeking with privacy at the beginning the project remembers his privacy setting and tries to find out both textual content that means the content that we enter while publishing the photograph as well as the image content in the sense the value of pixel color, the texture value, the shape value so and so. For example, the text contents an image that we associate with an image known as a metadata. Metadata is do not really the data the data is image here metadata is the description of the images. So whenever we initially start accessing a site our behavior is remembered by the system that means which type of photo that we are sharing with friends, which type of the photo that we are sharing with family and which of the type of photo that we are sharing with everyone so as per the image content and data every new image content will be matched. So for example if you try to give a new photograph of a baby from your past data it should be able to automatically tell that this is the photograph of a baby. If you forget to make a setting on each image it automatically predicts the policy each time there is no need to change a setting of privacy large amount of data

**Shruti Tornalker**, Master of Computer Applications, Visvesvaraya Technological University, Postgraduate Centre ,Kalaburagi, Karnataka,India.

**Dr. P. Sandhya**, Associate Prof & Course Co-ordinator, Department of Computer Applications, Visvesvaraya Technological University, Postgraduate Centre ,Kalaburagi, Karnataka,India

can be uploaded at a time this is the overall project.

II. LITERATURE SURVEY:

Due to the using of social sites a huge data is being shared on this which is violating the privacy so for this a survey has been done here and to prevent security a semantic annotated hidden Markova model is used to measure the annotated photos similarity in the database [1].To keep security protection in community, images need to be protected through different settings Here a protection of innovation prompt is used to share a data by the user this will fulfill the users end level goal [2].As the leaking of personal data within the friends or some group it is not satisfied to the user so to handle this type of problem a survey has been taken place through which a review is given of different privacy settings for the user to satisfy their level [3].To provide security to the image and shared data Images which are to be published System automatically annotates the image using hidden Markova mode and features are extracted [4]. Uploading a photos in the content sharing sites may leads to a violating the privacy to avoid this they solved it by providing a review through survey mainly to enhance the secure the personal information [5].To completely survey for a security and sharing image privately by the outline of new projection saving method for labeling image on long range informal destination for the communication has been advised here [6].The answer will be known that how the similar policies obtained by automatically generation of the policy on each uploaded photo so there is also a restricted to access on shared data and also how the effects on effectiveness is approached on tagging system [7].

III. SYSTEM DESIGN

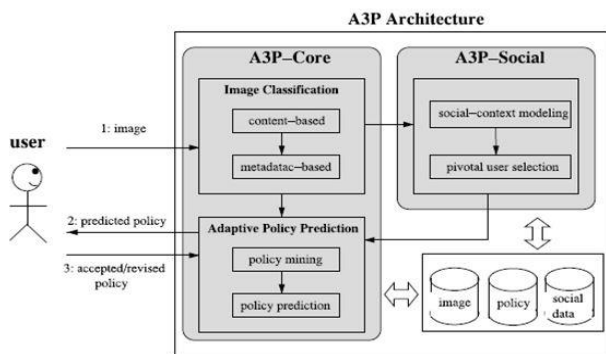


Figure: 1 Architectural Design

User will input an image if already user had earlier put some image into flicker or something. Current images features will be extracted features means color features will be extracted. They will be compared with the previous images will get a metadata. Metadata means what were the tags of previous images, what were the security of previous images this policy will be extracted from by comparing the image policy which is already stored by the user once this is been done whenever this image is published this image will be published with the predicted policy.

Tools and Technologies used

**Flicker API** It is a social site where we can upload, share, tag, and view the image. Here we can upload huge amount of

data the photos can be shared with friends or everyone and also we can make a setting within it where some groups can be formed.

A Forge

A Forge is a real time computer vision library for .Net so the statistics class is going to return three statistics red, green and blue because every image pixel comprises of red, green and blue these three statistics we are going to add in three series of the chart one is the red value one is the green value and one is the blue value. Once it is shown in the chart

**Machine Learning** It is a simple learning which is similar to mining a data any data artificially can be learned in this.

**K-Nearest neighbor classifier** Here as its name indicates it collects the nearest value that is only the nearest neighbor will be classified. It is also known as machine learning algorithm.

So how do we find out the nearest number what we need to do to find out the smallest number is.

First we take

$$\text{Small} = \text{inf}$$

Suppose we have values 121719

Now compare whether 12 be smaller than infinity.

1. Small=inf  
121719

If yes then now small will become 12 and index is 0.

small=12,0  
121719

Then compare whether 1 is smaller with 12 or not yes it is so small value become 1 index will become 1.

3. Then compare  
12 and 1 i.e  
small=1,0  
121719


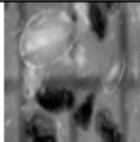



Then compare whether 7 is smaller than 1 or not 7<1, No. and

19<1, No

So at the end of the loop we will get which index has got the smallest value





IV. METHODOLOGY:

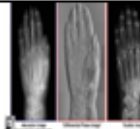




User should create a flicker account he should create an appropriate group. He must invite other friends to different groups. The friends must join the group then he needs to run the application. In the application user should browse specific category of image put all the necessary metadata use the privacy setting and upload the image. When user uploads an image the image features that is texture, color, shape will be extracted and the metadata will be extracted it will be saved in a data base. Every time user uploads a new image that will be compared with the previously uploaded images. If any of the previously uploaded images is closure to the new image automatically the privacy setting will be changed to the privacy setting used for previously uploaded image. If the new image is completely a new image and does not have any relationship with previously uploaded image then user will be prompted for new privacy settings which will also be saved in the data base. Once the user shared the image this image should be available across the internet in the same site so other user should be able to view this image as per the privacy for example we will login to this system with one of our friends account which is already accepted our group request in flicker who is part of the news group we need to show that that user is able to see all the news related photographs and not the other photographs, for example another group which has got our friends who are part of sports group we need to log in through their account to the flicker and then you should show that they are able to see only the sports related photographs that is been shared by us.



	Public	Public	True
	Public	Private	False
	Public	Public	True
	Private	Private	True
	Public	Public	True






V. RESULT ANALYSIS

Image Table







Given Image	Detected	Actual	True/ False
	Public	Public	True
	Public	Public	True
	Private	Private	True
	Private	Private	True
	Private	Public	False

	Public	Private	False
	Private	Public	False
	Public	Public	True
	Public	Public	True
	Public	Public	True

	Private	Private	True
	Public	Public	True
	Private	Public	False
	Public	Public	True
	Private	Private	True

	Public	Public	True
	Public	Public	True
	Private	Private	True
	Private	Private	True
	Public	Public	True

	Public	Public	True
	Public	Private	False
	Public	Public	True
	Public	Public	True
	Private	Private	True
	Private	Private	True

	Public	Public	True
	Public	Private	False
	Private	Public	False
	Public	Public	True
	Private	Private	True
	Public	Public	True

VI. CONCLUSION AND FUTURE SCOPE

With the popularity of the social networking sites every day millions of photographs have been shared in the social networking site. This increase the risk of misuse of the photographs been shared many a time user forgets to set appropriate security and privacy setting for the images that have been shared across the social site. In this world we have proposed novel mechanism to guide the user to automate the process of ensuring privacy setting for the images. The proposed technique first learns from already shared images by the user about the pattern and then classifies any new image that user intends to share in social site of flicker as either private or public result shows that the proposed system can predict the privacy setting of the images with an accuracy of over 80% therefore this can be used in a large variety of application and domain including “face book”, “twitter”, “Google plus” and so

This work can be further improved by replacing the K-Nearest neighbor classifier which is a primitive classifier with more advanced classifiers like neural networks further more security settings like sharable within the group sharable within the family or others could be incorporated as a future work to extend the domain of privacy settings of the images.

REFERENCES

- [1] K.Mayuri, V.DivyaVani, Y.SubbaRayudu, (2015) “Enhanced Privacy Access Inference for user uploaded images for Images Sharing sites in web”, International Journal of Computer Science, October. IEEE, ISSN Number 4142 3453.
- [2] K.Ramya Krishna, Smitha Rani Sahu,(2016) “The /security method provocation for user assigned images on content sharing website”, International Journal of Computer Science and Technology, IJCST VOL 7, Issue 1, Jan-March 2016.
- [3] Sangeetha.J, (2015) “A Survey on the Privacy Settings of User Data and Images on Content Sharing Sites”, International Journal of Innovative Research in Computer and Communication Engineering, March. Volume 3, Issue 3, March 2015. IEEE.
- [4] Sangeetha. J, Kavitha. R, (2015) “An improved privacy policy inference over the socially shared images with automated annotation process”, et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Volume.6 (3), 2015, 3166-3169.
- [5] Ashita, (2015) “A review of various privacy policy approaches to improve security in social networking communities”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 12, December 2015.
- [6] Thumpilli Buthcinaida, Ch. K. Reepes Kumar,(2015) “Security approach induction of client transferred picture on content sharing websites”, International Journal of Research in Computer and Communication Technology, Volume 4, Issue 12, Dec- 2015.
- [7] Ms. K.Soniya lakshmi, Mrs. V.subhatra, Ms. D.Gowdhami,(2015) “Privacy policy inference model using enhanced parent control algorithm”, Scientific journal impact Factor (SJIF): 1.711, International Journal of Modern Trends in Engineering and Research Volume 02, Issue 11, [November 2015], ISSN (Online):2349-9745; ISSN (Print):2393-8161.

	Private	Private	True
	Public	Public	True
	Private	Private	True
	Public	Public	True
	Private	Private	True
	Public	Public	True
	Public	Public	True
	Public	Public	True
	Public	Public	True
	Private	Private	True
	Public	Public	True
	Private	Private	True
	Public	Public	True
	Public	Public	True
	Private	Private	True

The accuracy is 42/50 which is 84%