Image privacy protection in social networking using data hiding technique

Miss. Vidya B. Solanke
Student:Dept. of Comp. Sci. &Engg.
SGBAU, Amravati
Maharashtra, India

Dr. RanjanaD. Raut
Associate Prof: PGDept. of Applied Electronics
SGBAU,Amravati
Maharashtra, India

Dr. Vilas M. Thakare
HOD: Dept. of Comp. Sci. &Engg.
SGBAU, Amravati
Maharashtra, India

Abstract—*Social networking sites are used for daily communication among users for sharing data such as images and other textual data. Likewise,the digital data related to people connected to social networking sites may face several attacks from the attackers or unauthorized users, Therefore privacy of profiles get crashed and to overcome this problem privacy policy system is developed, In this system data hiding is used to encrypt the image and privacy policy is set for images of user profile to restrict the access to users image, These two technique gives privacy to user profile and prevent it from getting crashed. The proposed method helps to provide the privacy to the users image successfully and the system works effectively.*

Keywords— Data hiding, Privacy inference, Policy setting, Online services.

I. INTRODUCTION

Nowadays, to provide privacy various privacy tools offered by major social websites like Facebook, Gmail, yahoo, LinkedIn, Google plus, Twitter, and others, it is still a challenging task for common users to achieve a desirable level of privacy protection during image sharing. This is because most users do not have sufficient privacy knowledge to configure a proper privacy setting or they simply do not wish to spend time on this. Thus the proposed method helps to provides more security to the secret data in cloud based services. Privacy settings for profile is a common issue where lot of work has been done and a lot more can be done. Explore how to achieve strong content protection, and how to propagate it automatically to sensitive user-uploaded content by using web traveler policy [1]. This paper blurs the ROI region with mosaics function. After that, the users can remedy back the ROI region if they own the mosaic factor [2]. Proposed a framework and with this framework a user can express his/her picture privacy policy in a machine readable format and (to some extent) automatically enforce it [3]. The reversible data hiding method is mainly focused on image privacy protection. Embedding information onto the image for some privacy reasons [4]. iPrivacy which automates the privacy setting process and releases the burden from users. Unlike many previous works which typically recommend privacy settings based on similarity of users' profiles or image tags, authors study the problem in a different angle by looking into the shared images themselves. this idea is to automaticallydetect the privacy-sensitive objects from the images being shared, recognize their classes, and identify their privacy settings [5].

In This paper data hiding is used to encrypt the imageand due to this each users those are visiting to the profile not directly get the image because image is in encrypted form and only those person who has the private key only that can access to the image and to detect privacy sensitive objects a hierarchical deep multi-task learning (HD-MTL) algorithm is used. This system gives efficient and effective results by applying the proposed technique.

II. BACKGROUND

Web-Traveler policies apply to the five basic operations possible for a given object posted on a site i.e view upload, download tag and comment, Explore how to achieve strong content protection, and how to propagate it automatically to sensitive user-uploaded content by using web traveler policy [1].

In mosaic technique, it blurs the ROI region with mosaics function. Then, the users can recover back the ROI region if they own the mosaic factor. With low cost of maintenance, this paper integrates the data hiding technique into a fined-grained access control to mosaic the sensitive information as well as enable to recover the mosaic region if necessary.The proposed scheme details two procedures, namely encoding procedure and decoding procedure. The encoding procedure contains embedding phase and mosaic phase [2].

Proposed a framework and with this framework a user can express his/her picture privacy policy in a machine readable format and (to some extent) automatically enforce it.Personal Picture Policy

Framework (P3F) eliminates the gap in communication from the photographed person to the photographer and/or publisher of the person's picture. It incorporates a simple flag-based system that covers the most important restrictions a person might impose on his/her own picture. It is similar to the Creative Commons system used for copyright restrictions on creative works (e.g., by photographers for their pictures). [3].

The reversible data hiding method is mainly focused on image privacy protection. Embedding information onto the image for some privacy reasons, Reversible data hiding (RDH) method is to retrieve both embedded data and encrypted image without any distortion.[4].

iPrivacy which automates the privacy setting process and releases the burden from users. Unlike many previous works which typically recommend privacy settings based on similarity o*f users' profiles or image tags, authors study the problem in a different angle by looking into the shared images themselves. this idea is to automatically detect the privacy-sensitive objects from the images being shared, recognize their classes, and identify their privacy settings [5].

This paper presents the brief introduction of privacy settings for users profile in section I. Section II discusses background. Section III discusses previous work. Section IV discusses existing methodologies. Section V discusses analysis and discussion. Section VI describes proposed methodology. Section VII discusses the possible outcomes and result. Finally section VIII concludes this paper.

III. PREVIOUS WORKDONE

In the research literature, Smitha et al. (2011)[1] web-Traveler policies apply to the five basic operations possible for a given object posted on a site i.e view upload, download tag and comment, Explore how to achieve strong content protection, and how to propagate it automatically to sensitive user-uploaded content by using web traveler policy.

Yi-Hui et al. (2013)[2] This paper blurs the ROI region with mosaics function. Then, the users can recover back the ROI region if they have the mosaic factor With low cost of maintenance, this paper integrates the data hiding technique into a fined-grained access control to mosaic the sensitive information as well as enable to recover the mosaic region if necessary. The proposed scheme details two procedures, namely encoding procedure and decoding procedure.

Adrian et al. (2013)[3] Proposed a framework and with thisframework a user can express his/her picture privacypolicy in a machine readable format and (to some extent) automatically enforce it.

Arjun et al. (2016) [4] reversible data hiding method is mainly focused on image privacy protection. Embedding information onto the image for some privacy reasons, Reversible data hiding (RDH) method is to retrieve both embedded data and encrypted image without any distortion.

Jun et al. (2016) [5] iPrivacy which automates the privacy setting process and releases the burden from users. Unlike many previous works which typically recommend privacy settings based on similarity of users' profiles or image tags, authors study the problem in a different angle by looking into the shared images themselves. This idea is to automatically detect the privacy-sensitive objects from the images being shared, recognize their classes, and identify their privacy settings.

IV. EXISTING METHODOLOGY

A. Privacy Through Web-Traveler Policies

In this method, Web-Traveler policies apply to the five basic operations possible for a given object posted on a site i.e view upload, download tag and comment. for example a policy state that Alice's picture Pic1 can be viewed and downloaded by Alice's friends, but that they cannot upload it in their profile. Policies are enforced under the assumption that the user who originally uploaded the content within the SN is in charge of specifying a protection policy for itl. Therefore the privileges for some of the operations are dependent on the others. For example, Alice to download an image Pic, she must be able to view it [1].

B. Fine-Grained Mosaic Technique

In this technique, With low cost of maintenance, this method integrates the data hiding technique into a fined-grained access control to mosaic the sensitive information as well as enable to recover the mosaic region if necessary. The proposed scheme explain two procedures, that are encoding procedure and decoding procedure. The encoding procedure contains embedding phase and mosaic phase. The fine-grained access control model can specify the security rules based on the constraints [2].

$$p'_x = p_x + sign(\lambda) \times ((|\lambda| \bmod 2) - \left\lfloor \frac{|\lambda|}{2} \right\rfloor . \quad (1)$$

$$\lambda = s - (p_x \bmod 3) . \quad (2)$$

C. Framework Based On Image Privacy Policy.

In this methodology, Personal Picture Policy Framework (P3F) eliminates the gap in communication from the photographed person to the photographer and/or publisher of the person's picture. It incorporates a simple flag-based system that covers the most important restrictions a person might impose on his/her own picture. It is similar to the Creative Commons system used for copyright restrictions on

creative works (e.g., by photographers for their pictures).A modular visual coding system is used to convey the policy information across the communication gap described above. The policy is embedded in the visual information of the photograph (e.g., as part of the clothing), making it an inseparable part of the picture so that it is highly likely to survive along the publishing path. Under favorable conditions, this information is hidden in such a way that it is unnoticed by the human eye. Hence, it is called as Privacy Policy Hiding. [3].

D. Reversible Data Hiding method

In this technique, user try to upload an image, the frontend software embed some privacy information into the image using Reversible Data Hiding (RDH) method using and also save encrypted image into database. To show this image on friend's wall, the frontend software check the image's embed privacy information match with friend's privacy information. If both privacy information are same, then only the image is visible to the friends. Otherwise, the user is not a friend so the image is not visible. Here, first method is embedding and second one is to keep the encrypted image into database. [4]

E. Identifying Sensitive Objects via Deep Multi-Task Learning

In this method, (a) massive social images and their privacy settings are leveraged to learn the object-privacy relatedness effectively and identify a set of privacy-sensitive object classes automatically; (b) a hierarchical deep multi-task learning algorithm is developed to jointly learn more representative deep CNNs (convolution neural networks) and more discriminative tree classifier over a visual tree, so that authors can achieve fast and accurate detection of large numbers of privacy-sensitive object classes; (c) automatic recommendation of privacy settings for image sharing can be achieved by detecting the underlying privacy-sensitive objects from the images being shared, recognize their classes, and identifying their privacy settings; and (d) one simple solution for image privacy protection is provided by blurring the privacy-sensitive objects automatically.[5]

$$\kappa_I(X_i, X_j) = \sum_{l=1}^{1000} \delta(X_i^l, X_j^l) \quad (1)$$

where X_i and X_j are the bags of object classes in these two social images, $\delta(X_i^l, X_j^l)$ is defined as:

$$\delta(X_i^l, X_j^l) = \begin{cases} 1, & if \quad X_i^l = X_j^l = 1; \\ 0, & otherwise \end{cases} \quad (2)$$

V. ANALYSIS AND DISCUSSION

Image is the important factor in social media, But maintaining Privacy of this images and setting privacy policy is major problem. The content shared by users are misused by other user which are connected to their account and likewise the privacy get crash. it is easy for other users to collect rich aggregated information about the owner of the uploaded content and the subjects in the this content. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

For recovering privacy problem various methods are developed.

The method includesWeb-traveler policies can seamlessly travel with the content, as they were attached to it. Policy propagation means applying these policies to unprotected content. Propagation is achieved by analyzing personal annotations, i.e., tags, and by considering content similarity. By deploying such extended content protection, we show how our approach can help prevent underage viewers from accessing adult content, and tracking misused copyright-free data.[1]

Fine grained mosaic method developed a low cost model with fine-grained access control for digital images. This paper blurs the ROI region with mosaics function.[2]

Framework for privacy policy is used for privacy settings, With this framework a user can express his/her picture privacy policy in a machine readable format and (to some extent) automatically enforce it. An easily understandable flag system is used to define restrictions on picture usage and linkability.[3]

Reversible data hiding is a technique where image privacy information is embedded into the image and only based on this privacy information the users can view image.[4]

Deep multi-task learning is a method for image privacy used for blurring the privacy sensitive objects automatically.[5]

TABLE 1:COMPARISON BETWEEN EXISTING METHODOLOGIES.

Techniques	Advantages	Disadvantages
Privacy throughWeb traveler policy	This is the first method to provide back-end data privacy protection.	This method does not while controlling unwanted download operations.
Fine–Grained Mosaic technique	This method needs low cost maintenance	Quality of mosaic image is very bad such that users cannot realize what the original contents are.
Framework based on privacy policy of image processing	An easily understandable flag system is used to restrict usage and linkability.	None of the techniques examined for building patterns around barcodes.
Reversible data hiding technique	This method achieve double protection from attackers and unauthorized users.	Cost of maintenance is high.
Deep multi-task learning	Automatically blurring the privacy sensitive objects inimages is the main advantage of this method.	This method does not avoid privacy inference through analyzing the inter class or object background co-occurrence contexts.

VI. PROPOSED METHODOLOGY

In this method, main aim is to improve the image privacy in social networking sites. Proposed method deals with how to protect the image's privacy using data hiding. In this technique, the image privacy information is embedded into the image, and only based on this privacy information the users on the social networking sites are able to view the image. By this method we make sure that only authorized users have access to the image. And also image is encrypted and only those user can access who has the system provided private key, after entering this private key user can view or download the image.hierarchical deep multi-task learning (HD-MTL) algorithm is used for fast and accurate detection of privacy-sensitive objects classes and recommend the best-matching privacy settings for newly uploaded image.

Algorithm:

Step1: Start
Step2: user can upload the image in their profile
Step3: apply data hiding method to encrypt the image.
Step4: attach privacy policy to image.
Step5: system provide private key for accessingimage of other users .
Step6: authorized user enters the key and get theaccess.
Step7: Stop.

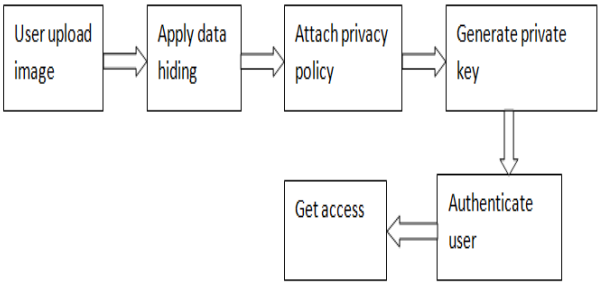

Fig 1: Flow Diagram of Proposed Framework

VII. POSSIBLE OUTCOMES AND RESULT

In the proposed system for getting the output set of images are taken , this images are necessary to encrypt if it is not then privacy is not maintain. For the encryption data hiding is used and then for each image privacy should attach. Other user get the access only if he/she is authorized, and this authorization is given by assigning private key by the system. Result of this proposed system is analyze accurate and efficient.

VIII. CONCLUSION

In this paper, privacy of the image is achieved successfully, the advantage of this system is it uses data hiding method due to this only authorized user get the access to the other users profile and this authorization is done by giving each user its private key.Thus the proposed method helps to provides more privacy to the images in social networking sites also overcomes the drawback studied earlier in existing methodology.

IX. FUTURE SCOPE

The proposed system is working for limited application so in future thus system is ready to work with all types of application.

Acknowledgment

I, vidyasolanke thankful of my supervisors professor Dr.R.D.Raut and Dr.V.M.Thakarefor helping to complete this research paper.

References

[1] Smitha Sundareswaran and Anna C Squicciarini, " Feature Point Detection in Image morphing",IEEE International Conference on Collaborative Computing: Networking Applications and Worksharing, 978-1-936968-36-7,2012.

[2] Yi-Hui Chen, Eric Jui-Lin Lu, Chu-Fan Wang, "Privacy Image Protection Using Fine-Grained Mosaic Technique", IEEE conference on signal and information processing,2013.

[3] Adrian Dabrowski, Edgar R. Weippl, Isao Echizen, "Framework based on Privacy Policy Hiding for Preventing Unauthorized face image processing ",IEEE International Conference on Systems, Man, and Cybernetics, 978-1-4799-0652-9/2013.

[4] Arjun K P , Aswathy Achuthshankar, Aswin Achuthshankar, Soumya M K, Sreenarayanan N M , Priya V V, Faby K A, "PROvacy : Protecting Image Privacy in Social Networking Sites Using reversible data hiding",Intelligent Systems and Control (ISCO),Jan 2016.

[5] Jun Yu, Baopeng Zhang, Zhenzhong Kuang, Dan Lin, Jianping Fan "iPrivacy: Image Privacy Protection by Identifying Sensitive Objects via Deep Multi-Task Learning",IEEE Transactions On Information Forensics And Security, 2016.