IMAGE SECLUSION AND TRESPASSING IN OSN USING WATERMARKING TECHNIQUES

S.Janani[1], G.Kalaivani[2], M.Priyadharshini[3], M.Saranya[4], S.Dhivya[5]
UG Students [1, 2, 3,4], Assistant Professor[5]
Department of Computer Science & Engineering
Kongunadu College of Engineering & Technology, Thottiam
jananiscse@gmail.com[1],kalaivaniguna1@gmail.com[2]

ABSTRACT

A social networking service (also social networking site, SNS or social media) is an online platform that is used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Social networking sites are varied and they incorporate a range of new information and communication tools such as availability on desktop and laptops, mobile devices such as tablet computers and smartphones, digital photo/video/sharing and "web logging" diary entries online (blogging). While Online Social Networks (OSNs) enable users to share photos easily, they also expose users to several privacy threats from both the OSNs and external entities. Image over the social network is transferred or transmitted between servers and multiple users. Privacy of that data is very important as it belongs to personal sensitive information. In existing system, text based encryption can be implemented in social networks. There are many different approached of storing data securely over the social networks, using big data such as end-to-end encrypted data transmission, dynamic credential generation only for text data. In this project, can introduce a novel watermarking scheme with wavelet algorithm named as discrete wavelet transform in real time social network application. In this scheme can use images and stored in server in secure format. And also extend the project, categorize the picture as sensitive or normal. If it is sensitive means, perform copyrights algorithms. Then provide the permission to the receiver end for download the images in secure manner. And also implement protection controls to block mouse operations and print screen options. Then extend the work to implement information filtering approach to be used to give users the ability to automatically monitor the messages written on their own walls, by filtering out unwanted messages and comments about images. This concept can be implemented in real time for sending mobile intimation at the time of user in offline mode about negative comments. So user can easily guard the system from privacy violations.

INTRODUCTION

A social networking service is an online platform that is used by people.In this project, we concentrate to solve the privacy violation problem occurred when images are published on the OSN without the permission.Therefore , the digital watermarking technique based on DWT algorithm.This watermarks are embedded in uploaded images.Watermarked images are shared in user homepage. so images can be difficult to misuse by other persons.

LITERATURE SURVEY

[1] M. Cheung, J. She, and Z. Jie, "Connection discovery using big data of user-shared images in social media," Multimedia, IEEE Transactions on, vol. 17, no. 9, pp. 1417–1428, 2015.

In this paper, there are two types of user pairs: related pairs, which are the pairs of users that are follower/followee, and nonrelated pairs, which are the pairs in which a follower/followee

relationship does not exist between the two users. A practical method, BoFT, is discussed to label user shared images with BoFT labels on over 360,000 user shared images. The characteristics of user shared images are then investigated and modeled as exponential distributions based on the analysis of 3 million follower/followee relationships from two social networks with different origins, Skyrock and 163 Weibo, for which similar observations are found. Based on the observations, a practical follower/followee recommendation system is proposed and formulated with the discovered connections, which are extensively verified with ground truth. It is concluded that follower/followee recommendation using discovered connections by user shared images.

[2] M. Cheung and J. She, "Evaluating the privacy risk of user-shared images," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 12, no. 4s, p. 58, 2016.

This work has investigated 1,598,769 user shared images by 6,036 users on Fotolog, an image-oriented social network. Based on intensive measurements and characterizations of these user shared images, this work has proved the phenomenon that two users with a higher similarity between their shared images are likely to be of the same gender or origin or have an online friendship between them. From this phenomenon, an analytic system using bag-of-features tagging to de-anonymize a user's identity using their shared images is proposed and verified by nearly 1.6 million shared images. It is observed that friendship is the most sensitive information for disclosing user identity. This paper has also presented 2

showcases to demonstrate the effectiveness of using user shared images for gender identification and origin inference. The experiments show that using user shared images is effective to disclose user identity.

[3] M. Cheung, J. She, and X. Li, "Non-user generated annotation on user shared images for connection discovery," in 2015 IEEE International Conference on Data Science and Data Intensive Systems. IEEE, 2015, pp. 204–209.

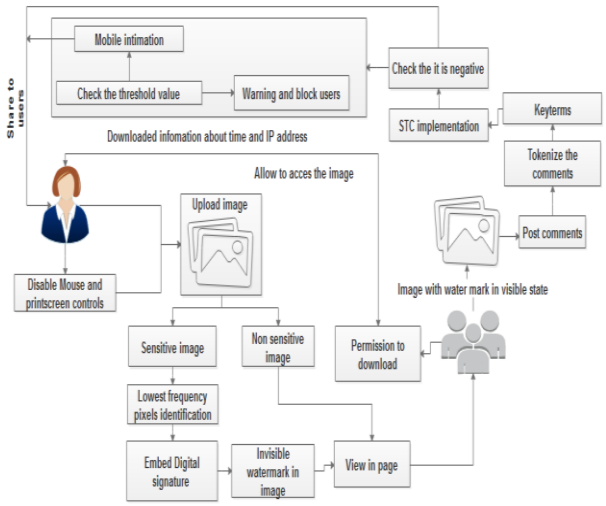
This paper evaluates non-user generated annotation to discover user connections for follower/followee recommendation. Instead of using scale-invariant feature transform (SIFT), we examine the use of non-user generated labels with different color-based and feature-based methods. The approach is evaluated using a dataset of 542 users and 201006 images, as well as the actual relationship among users. The results prove the effectiveness of non-user generated annotation. We evaluate a novel approach to non-user generated annotation, with the actual relationships of the scraped data with over 200k images; 2) we prove that non-user generated annotation can discover connections for recommendation, regardless of the visual method used to represent images; and 3) we confirm that the feature-based approach is 95% and 65% better than the color-based and tag-based methods, repectively. To the best of our knowledge, this is the first paper to prove that non-user generated annotation is not limited by the method used and that feature-based approaches are better for connection discovery. The GIST descriptor was initially proposed and it has shown good results for scene categorization and image search.

[4] M. Douze, H. J´egou, H. Sandhawalia, L. Amsaleg, and C. Schmid, "Evaluation of gist descriptors for web-scale image search," in Proceedings of the ACM International Conference on Image and Video Retrieval. ACM, 2009, p. 19.

In this paper, we compare the global GIST descriptor with the BOF image representations in different application scenarios. To our knowledge, these descriptions have not been compared in a similar setup. Clearly, one would not expect a global descriptor to outperform BOF representations. One of the problems of GIST description being the fixed spatial layout, we evaluate the impact on the accuracy resulting from this fixed spatial image partitioning. Finally, we propose an indexing strategy for GIST that improves the efficiency without significantly penalizing search accuracy. The advantage over the binary codes proposed is that only a small fraction of the database has to be visited. The idea is to first apply the

Hamming Embedding technique proposed to the GIST descriptor. This selects most of the potentially correct images. Then we apply filtering and re-ranking steps to further improve the quality of the ranking.

WORKING



EXECUTION STEP

Social Network Creation

Social network refers to interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. In this module, we can have three types of users such as image owner, image users and image server. Image owner can be upload the image into system and image server stores the images in database. Image users use images which are shared by image owner. We can social network application as android application for image owner. Server page can be designed as PHP page.

Upload Image

The first stage of any sharing system is the image acquisition stage. In this module, we can upload various images such as natural images, face images and other images. Uploaded images can by any type and any size. In this module, specify the image as sensitive or non-sensitive image. Sensitive image is referred as personal image. Non-sensitive image can be referred as forwarded image.

Embed The Watermark

In this module, we can embed the watermark text into images. Watermarking ensures authenticating ownership, protecting hidden information, prevents unauthorized copying and distribution of images over the internet and ensures that a digital picture has not been altered. We can implement Discrete Wavelet Transform (DWT) domain image watermarking system for real time image. In the embedding process, the watermark may be encoded into the cover image using a specific location. This location values are used to protect the images. The output of the embedding process, the watermarked image, is then transmitted to the OSN home page.

Privacy Settings

Each user images are first categorized into privacy policy. Then privacy policies of each images can be categorized and analyzed for predict the policy. So we adopting two stages approach for policy recommendation than applying the common one-stage data mining approaches

to mine both image features and policies together. The two-stage approach allows the system to employ the first stage to classify the policy as with privacy or without privacy. In the second stage, we can set without privacy means, prefer the user list details.

Protection System

In this module, we can set the protection or blocking system to avoid third party aces without knowledge of image owners. This module is used to set the image with privacy. If user set with privacy settings means, all users are considered as third parties.

STC Implementation

In this module, we designan automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. The architecture in support of OSN services is a three-tier structure. The first layer commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management). Additionally, some OSNs provide an additional layer allowing the support of external Social Network Applications (SNA). Finally, the supported SNA may require an additional layer for their needed graphical user interfaces (GUIs). The major efforts in building a robust short text classifier (STC) are concentrated in the extraction and selection of a set of characterizing and discriminant features. In order to specify and enforce these constraints, we make use of the text classification. From STC point of view, we approach the task by defining a hierarchical two-level strategy assuming that it is better to identify and eliminate "neutral" sentences, then classify "non-neutral" sentences by the class of interest instead of doing everything in one step.

Filtered Rules Implementation

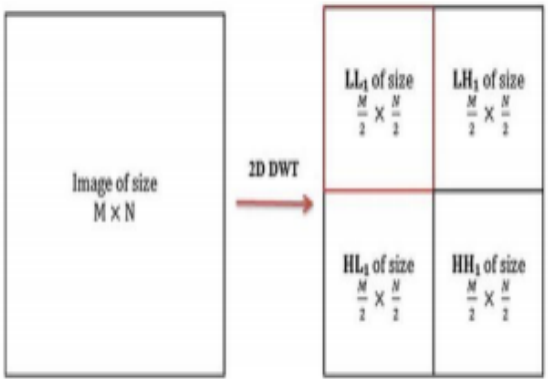
The filtering rules should allow users to state constraints on message creators. Thus, creators on which a filtering rule applies should be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on user profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators, to creators with a given religious/ political view, or to creators that we believe are not expert in a given field (e.g. by posing constraints on the work attribute of user profile). This means filtering rules identifying messages according to constraints on their contents. And block the users who are post the negative comments more than five times and also send mobile intimation to users at the time offline.

ALGORITHM AND IMPLEMENTATION

Discrete Wavelet Transform

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchical decomposition of an image. The

transformation is based on decomposing a signal into wavelets or small waves, having varying frequency and limited duration. The properties of wavelet decompose an original signal into wavelet transform coefficients which contains the position information. The original signal can be reconstructed completely by performing Inverse Wavelet Transformation on these coefficients. DWT decomposes an image into sub images or sub bands, three details and one approximation. The bands are LL, LH, HL and HH.



IMPLEMENTATION OF DWT

This diagram shows that the sub bands in DWT. LL contains low frequencies both in horizontal and vertical direction. HH contains high frequencies both in horizontal and vertical direction. HL contains high frequencies in horizontal direction and low frequencies in vertical direction. LH contains low frequencies in horizontal direction and high frequencies in vertical direction. The low frequency part comprises of the coarse information of the signal while high frequency part comprises of the information related to the edge components. The LL band is the most significant band as it contains most of the image energy and represents the approximations of the image. Watermarks can be embedded in the high frequency detail bands (LH, HL and HH) as these regions are less sensitive to human vision. Embedding into these bands increases the robustness of the watermark without having additional impact on the quality of the image. At each level of decomposition, first DWT is performed in the vertical direction, followed by the DWT in the horizontal direction. The first level of decomposition yields four subbands: LL1, LH1, HL1, and HH1. The LL sub band of the previous level is used as the input for every successive level of decomposition. This LL sub-band is further decomposed into four multi resolution sub-bands to acquire next coarser wavelet coefficients. This process is repeated several times based on the application for which it is used. DWT has excellent spatio-frequency localization property that has been extensively utilized to identify the image areas where a disturbance can be more easily hidden. Also this technique does not require the original image for watermark detection. Digital image watermarking consists of two processes first embedding

the watermark with the information and second extraction.

Watermark Embedding

In this process 2D DWT is performed on the cover image that decomposes the image into four sub-bands: low frequency approximation, high frequency diagonal, low frequency horizontal and low frequency vertical sub- bands. Similarly 2D DWT is performed on the watermark image that has to be embedded into the cover image. Here we have used Haar wavelet. The technique used for inserting watermark is alpha blending. The decomposed components of cover image and watermark are further multiplied by a particular scaling factor and are added.

Watermark Extraction

In this process the steps applied in the embedding process are applied in the reverse manner. First discrete wavelet transform is applied to both cover image and the watermarked image. After this the watermark is recovered from the watermarked image by using inverse discrete wavelet transform.

CONCLUSION

The appearance of well-known online social networking has triggered within the compromise of conventional notions of privateness, certainly in visual media. With a view to facilitate useful and principled protection of picture privateness online, we have got supplied the design, implementation, and evaluation of photo shield gadget that successfully and successfully protects client's photo privateness across famous OSNs. The digital watermarking approach based fully on DWT coefficients modification for social networking offerings has been presented on this paper. In the embedding manner, the coefficients in LL sub-band had been used to embed watermark. Within the extraction process, normal coefficient prediction based on imply clear out is used to boom the accuracy of the extracted watermark.

REFERENCES

[1] J.-D. Zhang and C.-Y. Chow, "igslr: personalized geo-social location recommendation: a kernel density estimation approach," in Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. ACM, 2013, pp. 334–343.

[2] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. ACM, 2007, pp. 29–42.