International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195344

Img-Shelter : Privacy Protection of Images In Online Social Networks Using Watermarking Scheme

P. Ponvasan[1], M. Muthusangari[2]

[1]M.E, Assistant Professor, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudhur, Karaikudi, Tamil Nadu, India

[2]PG Scholar, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudhur, Karaikudi Tamil Nadu, India

ABSTRACT

Social networking sites are very useful in sharing information, making friends and keeping in touch with old friends. It is an online service, platform, or site that focuses on facilitating the building of social networks and social elation among peoples for sharing interests, activities, backgrounds, or real-life connections. But with the increasing demand of social networking sites (SNS) privacy and security concern have also increased. Protecting personal information privacy has become a controversial issue among online social network providers and users. Most social network providers have developed several techniques to decrease threats and risks to the users' privacy. These risks include the misuse of personal information which may lead to illegal acts such as identity theft. This study aims to measure the awareness of users on protecting their personal information privacy, as well as the suitability of the privacy systems which they use to modify privacy settings. In this paper, 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. Experimental result can be shows that in real time environments using C#.NET as front end and SQL SERVER as back end and comparative study of existing algorithms based on computational time and privacy rate.

Keywords : Online Social Network, Image Privacy, Copyrights, Watermarking Scheme, Information Privacy

I. INTRODUCTION

In modern-day years, on-line Social Networks (OSNs) have attracted many masses of hundreds of clients global. Even even though Social Networks have perpetually been a primary part of everyday lifestyles, now that an increasing number of oldsters are related to the internet, their online counterparts are fun a increasingly important feature. OSNs have additionally grown to be a scorching issue in regions of research starting from sociology to laptop technological knowledge and mathematics. Except for allowing clients to create a community to symbolize their social ties, many OSNs facilitate uploading of multimedia content material cloth, quite a few strategies of communiqué and sharing many elements of ordinary life with friends. Humans can keep in contact with (bodily a long way off) associates, quite in reality percent content material fabric and studies and hold up to the moment within the remedy in their personal home or whilst on the glide. Social network systems provide a clean human computing device interface for net customers, making it easy to share unlimited-form statistics (same to pictures and movies) with friends anyplace and each time. Additionally, clients can revel in real-time and unfastened chats with others, post the ultra-modern reputation updates/verify-ins, and categorical evaluations approximately gift social sizzling spots. On the grounds that social networking's advent, we've great a few massively superb systems emerge (consisting of facebook, Twitter, and Instagram). When surfing on such structures, most customers are blind to the platform's privateness problems; but in reality, users' social network privateness is primary. Some sensitive statistics equal to a non-public alternative, profile, and shared pics could be leaked to others who aren't granted entry rights, if the social media service dealer doesn't take pleasant precautions to guard entry control. It's simple that most people social community structures goal to preserve their consumers' privateness as hundreds as they will be able to. Nevertheless, benefits aside, gain threats to person privateness are greater often than not underestimated. For example, because of most people nature of many OSNs and the internet itself, content material can without problems be disclosed to masses broader visitors than the man or woman supposed. Users extra frequently than now not have drawback revoking or deleting knowledge and statistics a few clients would possibly additionally be published by way of the use of others without their consent. Confinement in OSNs is a complicated remember and isn't always at all times intuitive to clients, particularly whilst you keep in mind that it is in no way times much like how privacy works in actual-existence interactions. Ideally, clients need to be successful to exchange a few confinements for functionality, without their information turning into reachable beyond the scope they intend. For instance, a purchaser of self-assist OSN would really like to fulfill mother and father with the same clinical scenario however does now not need each person to understand approximately his disease. Even in an outstanding deal a good deal less extreme times, the price of confinement is maximum of the time underestimated. In this artwork, we highlight that the essence of the scenario is that gift mechanisms for defining access to pictures in OSNs, can't actually manage times in which the involved events have conflicting settings. First, the image uploaded is regarded the proprietor of the photograph and is granted complete rights, whereas the oldsters showing inside the photograph need to now not seemed co-owners and have to not granted any rights. On high of this famous coarse-grained procedure, OSN businesses positioned into impact extra coverage policies, a number of so that you can significantly complicate troubles. Moreover, any customers which can be tagged have an effect at the visibility of the image, because the image will possibly be viewable by using way of all their contacts (default privateers environment). Therefore, even when the customers tagged inside the photo have limited its visibility, if the uploaded has not constrained access the photograph will in all likelihood be publicly available, something which the remainder users isn't always going to even be conscious of. Generally, those events will also be characterized as cases of conflicts of hobby, the region they need of the content fabric cloth author is going in the direction of the choice of the depicted customers, or the privacy settings of purchaser override those of 1 different. Note that even though the access manipulate mechanisms may additionally want to variety at some point of OSNs, conflicts of hobby are an ordinary impediment, as they rise up from the content cloth material of the pics. The various varieties of social networks are proven in figure 1.

Fig 1 : Social Network

II. RELATED WORK

BiaoWang, et.al,…[1] investigated the trouble of dynamic rumor influence minimization with user experience. First, based totally on present works on information diffusion in social networks, we include the rumor popularity dynamics in the diffusion version. We examine present investigations on topic propagation dynamics and bursty topic patterns. Then we choose Chi-squared distribution to approximate the global rumor popularity Inspired with the aid of the novel energy version proposed by using Han et al., we then analyze the man or woman tendency towards the rumor and gift the opportunity of a hit rumor propagation between a couple of nodes. Finally, inspired through the concept of the use of model, derive the cooperative succeeding chance of rumor propagation that integrates the global rumor recognition with individual tendency. After that, we introduce the idea of user experience software feature and analyze the impact of blocking time of nodes to the rumor propagation manner. We then adopt the survival idea to give an explanation for the chance of nodes getting activated, and endorse both grasping and dynamic algorithms based totally on most chance principle. We propose a rumor propagation model taking into consideration the subsequent three elements: First, the global popularity of the rumor over the whole social network, i.e., the overall topic dynamics. Second, the attraction dynamics of the rumor to a ability spreader, i.e., the individual tendency to forward the rumor to its friends. Third, the acceptance chance of the rumor recipients. In this model, inspired by using the use of model, we combine all three elements collectively to recommend a cooperative rumor propagation opportunity. In our rumor blocking off techniques, we bear in mind the have an effect on of blocking time to user revel in in actual global social networks.

De-Nian Yang, et.al,…[2] creating a grand concept for the social networking provider carriers to support active friending. To help lively friending, the key problem is on the layout of the algorithms that choose the advice applicants. An easy scheme is to offer recommendations with the aid of unveiling the shortest route between the initiator and the target in the social community, i.e., recommending one candidate at each step alongside the direction. As such, the initiator cans steadily method the target by acquainting the individuals at the course. However, this shortest-path advice method may additionally fail as quickly as a middle-character does now not accept the friending invitation (due to the fact only one candidate is blanketed in the advice listing for every step). To cope with this trouble, its miles suitable to suggest more than one candidates at each step because the initiator is much more likely to proportion more common buddies with the goal and thereby more likely to get widely wide-spread via the goal. Especially, by way of broadcasting the friending invites to all associates of the initiator's pals, the possibility to attain the friending target and get well-known can be effectively maximized as huge wide variety of paths is flooded with invitations to approach the goal. Nevertheless, friending invitations are abused right here due to the fact the above unidirectional broadcast is aimless and liable to involve many unnecessary friends. Moreover, the initiator may not want to address a huge variety of tedious invites. In this paper, we examine a brand new optimization hassle, referred to as Acceptance Probability Maximization (APM), for lively friending in on line social networks. The provider providers, who keen to explore new monetary equipment for sales increase, may additionally recall charging the users from lively friending service.

Andrew McCallum, et.al,…[3] provided the Author-Recipient-Topic (ART) version, a directed graphical version of phrases in a message generated given their writer and a hard and fast of recipients. The version is similar to the Author-Topic (AT) version, however with the essential enhancement that it situations the consistent with-message subject matter distribution collectively on each the author and person recipients, as opposed to on character authors. Thus the invention of topics within the ART model is stimulated via the social shape in which messages are dispatched and received. Each topic includes a multinomial distribution over words. Each author-recipient pair has a distribution over topics. We can also easily calculate marginal distributions over subjects conditioned entirely on a creator, or solely on a recipient, which will locate the topics on which all and sundry is maximum probable to ship or acquire. Most importantly, we can also correctly use these man or woman conditioned subject matter distributions to measure similarity among people, and for that reason find out humans' roles with the aid of clustering using this similarity. For example, people who receive messages containing requests for photocopying, travel bookings, and meeting room preparations can all be said to have the role "administrative assistant," and can be found as such due to the fact inside the ART version they will all have these topics with excessive chance of their receiving distribution. Note that we will find out that human beings have comparable roles although within the graph they are connected to very exceptional units of people. Thus, we advocate an Author-Recipient-Topic (ART) model for message statistics. The ART version captures subjects and the directed social community of senders and recipients via conditioning the multinomial distribution over subjects relatively on both the writer and one recipient of a message. Unlike the AT, the ART version takes into consideration both author and recipients highly, similarly to modeling the email content material as a aggregate of subjects. The ART model is a Bayesian network that concurrently models message content, as well as the directed social community in which the messages are dispatched.

Luoyi Fu, et.al,..[4] bridge the theoretical analysis of essential scaling laws of wi-fi networks with the insights already won through practical protocol development. By doing so, we provide a theoretical foundation to the design of shrewd scheduling and routing schemes that exploit social family members, analytically demonstrating the benefits of such schemes in phrases of throughput ability. In precise, to address the aforementioned predominant functions of such big scale networks, we install the rank based totally model, in which the opportunity of befriending a selected node is inversely proportional to α^{th} strength of the number of closer nodes. We pick the rank-based model over the gap-based totally one because the latter one underestimates the friendship probability of the distant nodes within the low-density place, whilst the geographical distribution of users is inhomogeneous in common occurrence. In contrast, the rank-based model states that the friendship probability relies upon on each the geographic distance and node density. It is well worth noting that each the rank-based totally model and the strength law node levels are heavy-tailed distributions. Heavy-tailed distributions are beneficial modeling tools in realistic settings, however are often difficult for analysis because they imply a brilliant degree of versions inside the machine, i.e., some of the supply-vacation spot pairs are close acquaintances at the same time as some may be very a ways away. In addition, a few nodes have extremely large quantity of fans (together with celebrities) even as a few others can also handiest have a few. However, our results show that in spite of the excellent heterogeneities in the network, a uniform most beneficial performance can be guaranteed. Comparing with traditional unicast networks, the site visitors sample in our version is appreciably specific because the destinations are decided on according to the rank-based model, so that you can result in a positive diploma of visitor's locality. Intuitively, as parameter α will increase, sources will be much more likely to befriend a node located in nearer proximity, and therefore less distance or hops are had to be included in the packet delivery manner. This amount to a smaller interference per site visitors float, and in phrases implies a bigger degree of transmission concurrency may be achieved. As a result, the unicast capability is extended. However, the non-uniformity of the site visitors sample will cause considerable problem in analysis.

Andrea Montanari, et.al,…[5] represented the social network by using a graph wherein each node represents an agent inside the gadget. Each agent or player has to make a preference between two alternatives. The payoff of each of the two alternatives for the agent increases with the variety of friends who are adopting the same preference. The above version captures situations in which there is an incentive for individuals to make the same picks as their immediately buddies or friends. This might also appear while making a decision among two opportunity operating systems (e.g., Windows versus Linux), selecting mobile telephone carriers (AT&T versus Verizon), or maybe political events (Republican versus Democratic). We use a totally easy dynamics for the evolution of play. Agents revise their strategies asynchronously. Each time they pick out, with probability near 1, the approach with the first-rate payoff, given the current conduct in their pals. Such noisy satisfactory-reaction dynamics were studied notably as a easy version for the emergence of technologies and social norms. The essential bring about this line of labor can be summarized as follows: The aggregate of random experimentation (noise) and the myopic attempts of gamers to boom their application (first-class response) drives the system toward a specific equilibrium in which all gamers take the identical action. The analysis additionally gives a easy circumstance (referred to as threat dominance) that determines whether or not an innovation delivered inside the community will ultimately come to be significant. The gift paper characterizes the fee of convergence for such dynamics in phrases of specific graph-theoretic portions. Suppose a superior (hazard-dominant) generation is brought as a brand new opportunity. Our characterization is expressed in terms of quantities that we name tilted reduce width and tilted reduce of the graph. We refer the reader to the following sections for specific definition of these portions. Roughly speak me, the 2 quantities are duals of every other: The former characterization is derived via calculating the maximum in all likelihood course to the equilibrium and implies an higher bound on the convergence time; the latter corresponds to a bottleneck within the space of configurations and provides a lower certain.

III. EXISTING METHODOLOGIES

Information and communication technology (ICT) plays a significant role in today's networked society. It has affected the online interaction between users, who are aware of security applications and their implications on personal privacy. There is a need to develop more security mechanisms for different communication technologies, particularly online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to allow or deny others access to personal information details. The increased use of information and communication technologies has had a significant impact on the interactions between users. This is particularly true for people who use mobile devices to communicate with one another or to access the Internet. Web users have difficulty knowing where and how their information is stored and who is authorized to use it. Therefore, protecting mobile web users' data and increasing their confidence in data privacy has become a real challenge.

3.1 SEARCHABLE ENCRYPTION IN IMAGE PRIVACY

Encrypting the images before uploading to the cloud services alleviates the privacy concerns as the service providers would only have access to the cipher text. However, a downside of such a solution is that it undercuts the convenience provided by such services. Users can no longer browse, organize, and manage their images on the cloud side because they would be unable to distinguish between the images in cipher text form. This system transforms the feature vector of an image into a simhash. Similarity is defined by having Hamming distance from the query smaller than a given threshold. To allow seamless integration with any inverted-index-based SSE scheme, we design a sub-simhash data structure. It divides each simhash into several parts, where each is populated to different indices. In more details, for each part, the images that share the same sub-simhash are linked together as a linked list (which can be replaced by other data structure). Similarity searches are done by probing different sub-simhashes of the query image. In other words, image retrieval probes the inverted index for possible matches, starting with the first sub-simhash of the query image, and repeats the probing for its subsequent sub-simhashes. This will cover a large portion of similar images.

3.2 PRIVACY POLICY IN SOCIAL NETWORK

Suppose user want to share any images and video so user may or may not want to share this data to all level, user must want to provide some assurance where user will place data and provide some type of security on traveling data. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.

IV. PROPOSED METHODOLOGY

Photo sharing refers to the transfer or publishing of user's digital photos online and the website which provides such acquaintances offer services such as hosting, uploading, sharing and managing of photos through online system. This function provides the upload and display of images through both websites and applications. The photo sharing term can be set up and managed by individual users for the usage of online photo galleries including photo blogs. It means that other users can view but not essentially download the photos, users being able to select different copyright options for their photos. Unfortunately, it may reveal users privacy if they are permitted to post, comment, and tag a photo liberally. The crimes in the social networking sites are increasing day by day. One of the main crimes is misusing the image by morphing and using it for blackmailing. Users can view the image and edit the image. On social networking sites, users post their own pictures and these pictures can be viewed by anyone. Anyone can access the image, whether the users are authorized or unauthorized. There is no centralized privacy. This paper deals with how to protect the image's privacy using copy right techniques. 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. Online photo sharing applications have become popular as it provides users various new and innovative alternatives to share photos with a range of people. The photo sharing feature is incorporated in many social networking sites which allow users to post photo for their loving ones, families and friends. The integrity and authenticity is the compelling question as, among other fields, these images are also being used as evidence in the courts of law. It is very critical to verify the integrity of these images and is often desirable to identify if an image has been manipulated from the time of recording. To understand, how things go in the background of a jpeg image, we will implement watermarking approach to hide default pattern into image. Water mark bits are embedded into image. So unauthorized users only get watermark data only. Based in inverse DWT, we will get the seen water mark that can be restored into customary image. In the interface aspect, we will exchange the color of textual content pixels into color of photograph pixels. So photo may also be considered as undeniable content. Person can set privateness settings to dam the pictures to down load by way of third parties. So unauthorized users most effective get watermark information handiest. Then utilizing disable options of screenshots in interface system.

4.1 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 .NET page.

4.2 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.

4.3 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 is used to protect the images. The output of the embedding process, the watermarked image, is then transmitted to the OSN home page.

4.4 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.

4.5 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. Based on this setting, unauthorized user only views the image and can’t be used. If he downloads means, only get water mark values. Finally provide hardware control system such as screenshot controls. Then disable the screenshot options. Device controls values are extracted and to provide coding implementation to disable the coding at the time protection. We can implement this concept in all browsers. The proposed block diagram is shown in fig 2.

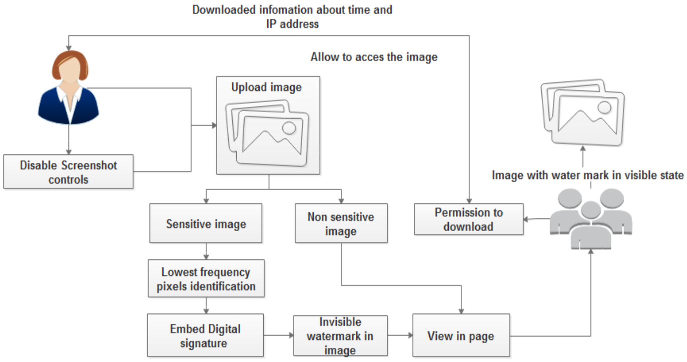

Downloaded infomation about time and IP address
Allow to acces the image
Upload image
Disable Screenshot controls
Image with water mark in visible state
Sensitive image
Non sensitive image
Permission to download
Lowest frequency pixels identification
Embed Digital signature
Invisible watermark in image
View in page

Fig 2: Block Diagram

4.6 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.

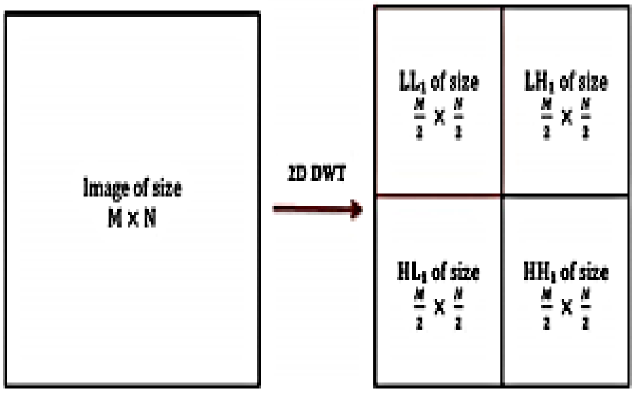


Fig 3 : DWT Process

The figure 3 shows 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.

4.7 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. During the embedding process the size of the watermark should be smaller than the cover image but the frame size of both the images should be made equal. The watermark embedded in this paper is perceptible or visible in nature, so we embedded it in the low frequency approximation component of the cover image.

4.8 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.

R′ ← WatermarkEmb(R,w, kemb1, kemb2, kemb3)

1. For each image c ∈ R

1) Divide c into s × s sized nonoverlapping blocks. Choose the low frequency blocks using DWT. The watermark is a sequence of binary bits denoted as w = w1,w2, ...,wNw. A set of blocks {BKi}Nw i=1 are chosen by a pseudorandom function as kemb1. Each block will carry one bit of the watermark.

2) For each watermark bit wi, i ∈ [1, ...,Nw],

a) The pixels in block BKi are divided into two sets S0 and S1 according to a pseudorandom function with the water mark text kemb2;

b) If wi = 0, flip the bits of pixels in S0. Otherwise, flip the pixel bits in S1. In order to preserve the image quality, we make less flipping on higher bit-planes. We denote the ratios of flipped bits on 8 bit-planes as ϵ =[ϵ1, ϵ2, ..., ϵ8]. That is to say, for the i-th bit-plane, there are Nw × s2 × ϵi/2 bits will be flipped randomly. The flipped positions are determined by kemb3 using Inverse DWT. Flip the water mark text color into image color.

2. Output the watermarked image set R′.

wt ← WatermarkExtra(mt,mo, kemb1, kemb2, kemb3)

1. Divide mt into nonoverlapping blocks with the size s × s using DWT.

2. Locate the set of blocks {BKi}Nw i=1 that carries the watermark
bits w = w1,w2, ...,wNw according to the secret key kemb1.

3. For each i ∈ [1,Nw],

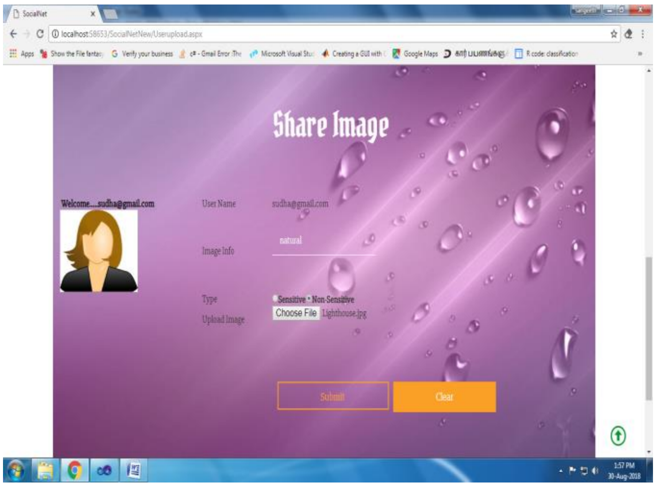
1) Divide the pixels in BKi into two sets S0 and S1 according to locations kemb2;

2) Flip the pixels in S0 and S1 respectively according to [ϵi]8 i=1 and kemb3 to get two blocks BK0i and BK1i. Construct the corresponding block BKi from the original image with the secret key kemb1. Calculate δ0 =Σpj ∈BKi;p0j ∈BK0i (p0j pj)2 and δ1 = Σpj ∈BKi;p1j ∈BK1i (p1j − pj)2. If δ0 < δ1, the watermark bit is extracted as '0'. Else, the watermark bit is extracted as '1'.

4. Output the extracted watermark wt.

V. EXPERIMENTAL RESULTS

The proposed work can be implemented in C#.NET as front end and SQL SERVER as Back end. The image based details can be shown in following figures.



Welcome....sudha@gmail.com

User Name sudha@gmail.com

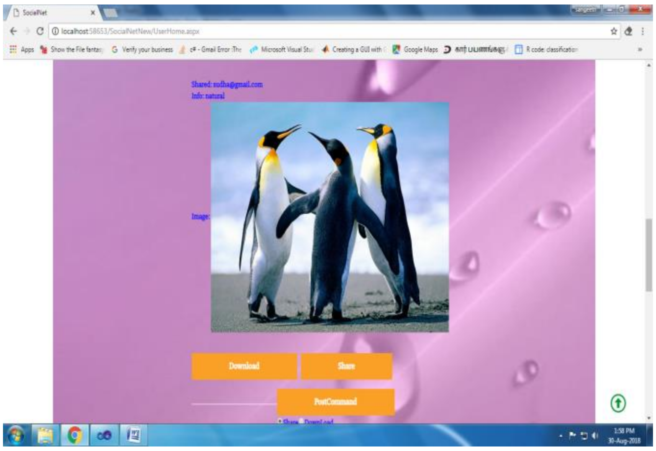
Image Info natural

Type ○ Sensitive ● Non-Sensitive

Upload Image Choose File Lighthouse.jpg

Fig 4 : Image sharing in social network

Then provide the permission to access the social network and shown in fig 5.



Shared: sudha@gmail.com
Info: natural
Image:

Fig 5: Permission to download

Then without permission, user only get watermark only can be shown in fig 6.

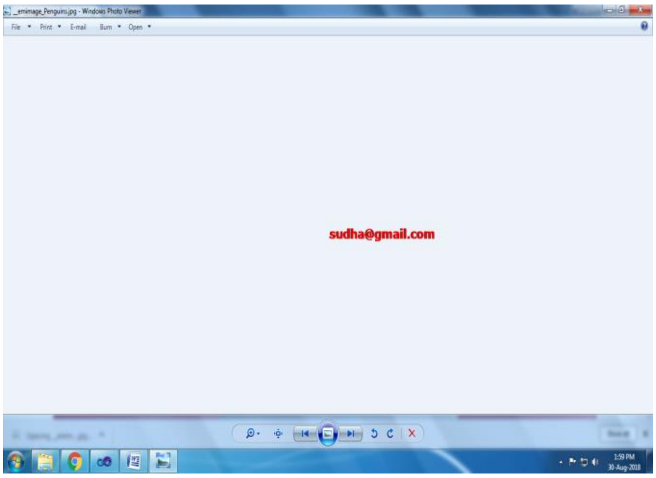
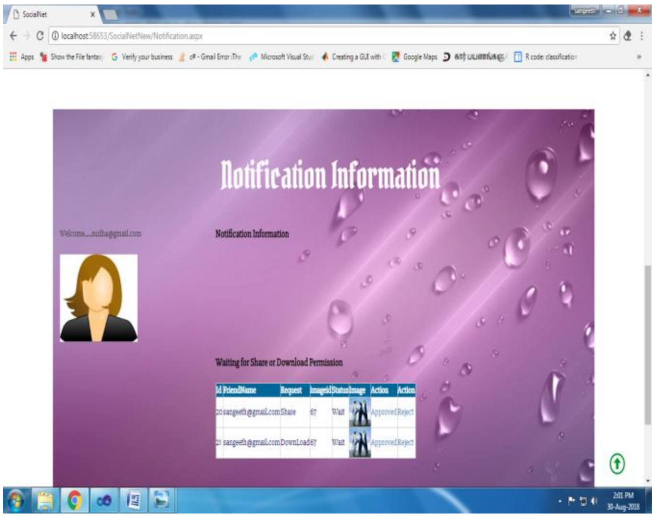


Fig 6: Without Permission



Welcome....sudha@gmail.com

Notification Information

Waiting for Share or Download Permission

Id	FriendName	Request	imageid	Status	Image	Action	Action
20	sangeeth@gmail.com	Share	67	Wait		Approved	Reject
21	sangeeth@gmail.com	DownLoad	67	Wait		Approved	Reject

Fig 7: Notification details

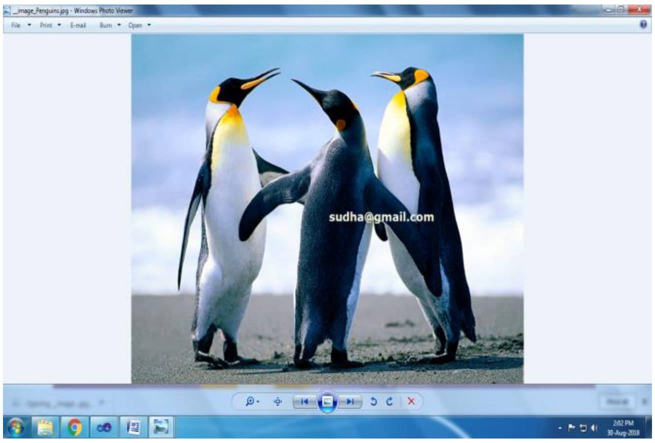


Fig 8: With privacy download

From the above figures, we can provide privacy to images, comments and tags. We can also implement in groups.

VI. 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. On extending the Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content. Then exploiting a flexible language to specify Filtering Rules (FRs), by which users can state what contents, should not be displayed on their walls. FRs can support a variety of different filtering criteria that can be combined and customized according to the user needs.

VII. REFERENCES

[1]. B. Wang, G. Chen, L. Fu, L. Song, and X. Wang, “Drimux: Dynamic rumor influence minimization with user experience in social networks,” in Proc. 30th AAAI Int. Conf. Artif. Intell., Feb. 2016.

[2]. D. N. Yang, H. J. Hung, W. C. Lee, and W. Chen, “Maximizing acceptance probability for active friending in online social networks,” in Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2013, pp. 713–721.

[3]. A. McCallum, A. Corrada-Emmanuel, and X. Wang, “Topic and role discovery in social networks,” in Proc. 19th Int. Joint Conf. Artif. Intell., 2005, pp. 786–791.

[4]. L. Fu, W. Huang, X. Gan, F. Yang, and X. Wang, “Capacity of wireless networks with social characteristics,” IEEE Trans. Wireless Commun., vol. 15, pp. 1505–1516, Feb. 2016.

[5]. A. Montanari and A. Saberi, “The spread of innovations in social networks,” in Proc. National Academy of Sciences of the United States of America PNAS, Aug. 2010, pp. 20 196–202

[6]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology-Eurocrypt. Springer, 2004, pp. 506–522.

[7]. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. of IEEE Symposium on Security and Privacy. IEEE, 2000, pp. 44–55.

[8]. E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[9]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proc. of 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[10]. J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, “A novel routing protocol providing good transmission reliability in underwater sensor networks,” Journal of Internet Technology, vol. 16, no. 1, pp. 171–178, 2015.

Cite this article as :

P. Ponvasan, M. Muthusangari, "Img-Shelter : Privacy Protection of Images In Online Social Networks Using Watermarking Scheme", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 110-120, May-June 2019. Available at doi : https://doi.org/10.32628/CSEIT195344
Journal URL : http://ijsrcseit.com/CSEIT195344