Social Network Analysis for Image Origin Classification

Monica Tresa I[a], Asma Begum M[b], Nirmala J[c], Nikita J[d], and Lakshaswaroopa B[e]

[a] Assistant Professor, Department of CSE, K. Ramakrishnan college of Technology
[b]Assistant Professor, Department of CSE, K. Ramakrishnan college of Technology
[c]Assistant Professor, Department of CSE, Mohamed Sathak A J College of Engineering
[d]UG Student, Department of CSE, K. Ramakrishnan college of Technology
[e]UG Student, Department of CSE, K. Ramakrishnan college of Technology

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: The social community websites are new task for private safety, specifically while a person's personal facts is discovered in contents published via means of others, inclusive of pictures with individuals. The fast improvement of numerous online social networks (OSNs) makes it unprecedentedly notable to share pictures online which lead OSNs as a main network to share images online. The unlawful task on the online contents include misusing of those pictures extensively. Because of this situation, finding the initial place and the propagation route of an online photograph are important for lots of forensic applications. In the proposed machine, a easy powerful method to determine the photograph starting place via way of means of exploiting the unique traces left via way of means of the various OSN operations. To this end, it first conducts a complete have a look at at the manipulations that numerous OSNs perform on uploaded images. It develops a machine to support customers collaborative private safety via way of means of permitting multiple customers to together manipulate the get admission to their non-public data.

Keywords: Privacy Protection, Online Social Networks (OSNs), Forensic Applications, Image Origin, and Provenance Identification

1. Introduction

As a vital data carrier, virtual pictures are the foremost additives of community resources. With the ever-growing recognition of non-public cell devices, a large number of virtual pics are generated on online websites including social media daily. Online social networks (OSNs) such as Facebook, Twitter, Wechat allow users to share their pictures online, making them one of the important factors of online pictures. For example, there are nearly 350 million pictures uploaded every day on Facebook [1]. In WeChat, the range gets increasing immensely for about 1 billion [2]. However, these private pictures are no longer well-controlled and protected with the resource of using the present OSN vendors to an extent. Among the resources, many pictures can be browsed, downloaded freely. [3], [4], [5]. In this context, a few irrelevant behaviors concerning the uploaded pictures should get up which includes misappropriation of others' pictures and importing pictures without owners' consent. Consider the subsequent scenario. Alice was photographed and the pictures are shared over a few OSNs without one's permission or she doesn't know that her pictures are photographed. When those pictures get noticed by Alice, she wants to stop the spread of those pictures on the internet further. To terminate it, the initial step that Alice wants to do is, she needs to discover is the starting place of those pictures, in which social media those pictures shared over. For instance, the virtual digital dig cam identity should be achieved with the help of convenient resource of using studying the sensor sample noise [6]. In [7], [8], different techniques had been used to discover the software to detect a virtual photograph. Specifically, for spotting out the initial point of OSNs shared pics, one important technique is to find the metadata contained in the photograph, which incorporates a few data of the related OSN. Unfortunately, we identified that many of the OSN does not offer the metadata contained in the photograph. Even if the metadata information is provided, such data can be modified or erased without difficulty. Besides, [9] the work is proposed to infer the photograph authenticity on Facebook with the resource available on the internet. Later, Caldelli et al. designed a way to discover the OSN systems of provenance with the aid of using resorting to the skilled Bagged Tree Random Forest classifiers [10]. The exclusive functions used of their technique had been extracted from DCT area as it is miles predicted that the uploaded pictures had been compressed the use of the JPEG algorithm with the resource of using OSNs. This technique is viable to distinguish special social community origins; but the overall performance isn't great in particular while the excellent of the uploaded photograph is excessive. Further, all of the experiments on this technique had been handiest based on pictures which are in a type of grayscale. In this work, endorse a photograph starting place identity technique with the aid of using exploiting the precise strains left with using OSN. It is discovered that most of the OSNs practice diverse implementations on the images that are uploaded, e.g., compression and filtering. The abnormal operations that are dependent are inevitably provides strains on the pictures, accomplishing the starting place to achieve. In order to do this, a complete study on the diverse OSNs done on uploaded pictures. Information of those output, characteristic vector is layout and finally educate a multi-magnificence SVM classifier for figuring out where those on line pictures are emerged from. Based on the investigation, experimental outcomes are provided in a large manner, displaying the technique achieves excessive accuracy of photograph starting place identity.

2. Detect the Image Processing Mechanism of Various OSNS

Nearly, more of the present OSNs follow diverse methods to upload images [11], [12], [13]. To display the unique photograph, it's miles much critical to understand how the OSN manipulates [18] the pictures that has been uploaded. Consultant OSNs are being focussed: Facebook, Twitter, Wechat Moments. Although a few preceding work (e.g. [12], [13]) investigated this problem, and had given a hard result and one platform is being focused here. Given a scientific research approximately these consultant OSNs, the mechanisms for processing the photographs. OSNs follow the manipulations to the uploaded pictures[16] [18] can be differentiated as resize the images and JPEG compression and filtering. Maximum OSNs carry out resizing while the decision of the add photograph is simply too large. To understand the decision, just add a sequence of pictues of exceptional resolutions and those images with the downloaded versions of images. For Facebook, Twitter, while both duration and width dimensions are less than some specified pixels, the photograph decision stays, or else resizing is conducted. For Wechat Moments, this decision threshold is resized. In Flickr, resizing operation is complex. Peculiar sized photograph is presented to the users; however additionally presents numerous resizing scheme. JPEG Compression for the above mentioned supporting OSNs, all of the pictures [15] that have been uploaded are subject to JPEG compression. The compressions are implemented in YUV shadeation area with the subsampling mode on OSNs. The images are compared with the old ones. This belongings makes to clean are diagnosed from others. To enhance the viewing experiences, maximum OSNs follow some of the extra filtering which is much enhanced on the pictures that are uploaded. This is proved through enforcing precisely the identical JPEG compression because the downloaded image which is ensured of no resize on the unique photograph which is uploaded. While evaluating the regionally manipulated photograph with the downloaded images, the strains of greater processing are evident. Also it is discovered that understanding such filtering in a precise way, as it is implemented regionally and adaptive.

3. Proposed System

In this proposed system, category device is to differentiate amongst images. An interesting subject is that the supply identity mission is ready to differentiate amongst diverse classes of devices (e.g scanned images, pictures, pc generated) extracting a few strong and characterizing features. A approach to become aware of pictures created with the aid of using distinctive reassets with none type of preceding understanding is proposed suggesting a blind clustering of the distinctive supply. The explosion in the use of social community offerings enlarges the range of photo facts and affords new situations and demanding situations within the supply identity and category mission.

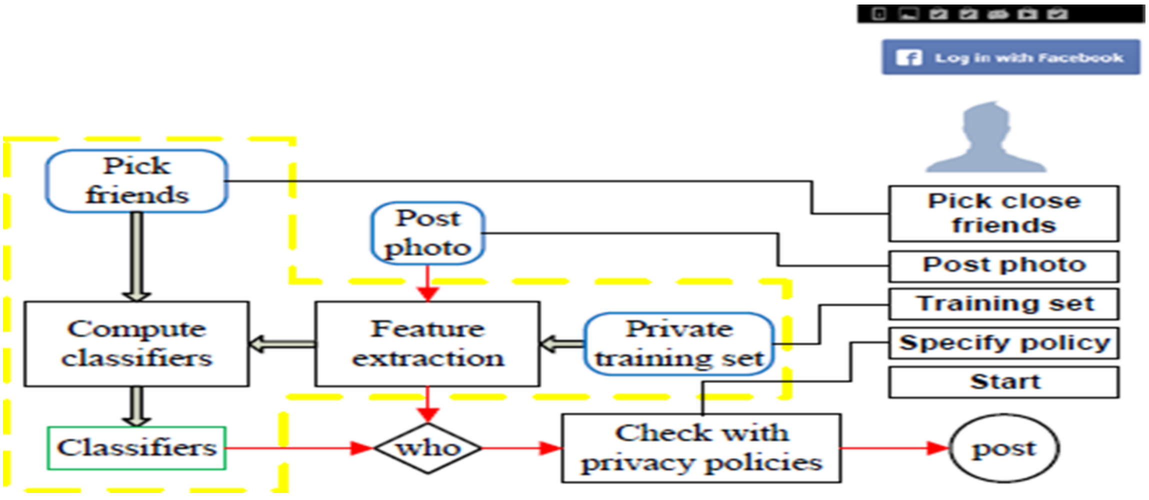


Figure 1.1 Proposed System Architecture

4 .Implementation of Provenance Identification in OSN

1. User verification

User verification is used via social community to make certain that customers offer records this is associated with the identification of a real person.

2. Image duplication

(i). Find similar photos

It appears for similarities in distinctive images and without difficulty reveals duplicates in addition to pictures of the same pixels.

(ii). Find resized and rotated photos

Resize pictures, rotated photos, edited images, cropped and flipped photos taken using different camera settings can be identified by Duplicate picture module.

3. Access post

(i) Update profile information

User's profile information like username can be updated by users. In order to ensure security they are allowed to change password and user can update their profile picture also.

(ii) Post information

Interest of the users can be posted on the wall, where others can be in a position to view the interest of the users and get reviews from them

4. Source find

Thousands of pictures have been routinely published on every platform after which to be downloaded to viably carry out experimental exams for social network provenance identification.

5. Image origin classification

The definition of a approach primarily based on functions which with the aid of using resorting at educated classifiers is capable of picking out the social platform of provenance.

6. Friend search

It is easy way to find their same interest of their friends.

Three social factors, (i).personal interest, (ii) interpersonal interest similarity, and (iii) interpersonal influence.

(i). Location based recommendation

Based on the specific landmarks given by the user friends may be recommended.

Explanation:

Before getting into any of the website , it demands user to give their personal information. The information given by the user will be verified to make sure it is the identification of a original person. After uploading their corresponding documents, then duplication of images has to be identified. It is done by two ways. Finding similar pictures uploaded by the user and modified photos. Duplication of the images can be identified, Similar photo also means that images with the same pixels[17] can be identified. Modified pictures like edited image, cropped image, compressed image, resized image also can be identified. Since these two ways ensure security, it limits the users to have fake profile in social networking sites, thereby avoids illegal activities and unwanted communication which results in a positive and good relationship among the original users. Users are given freedom to update their name in profile and change password which ensures more security[14] since social networking deals with more number of users from different region. The users are given a place to share their interest in a wall so that like minded people may get a chance to view the post and give their opinion and reviews to the post shared by user on the wall. Thousands of images are being rotated on each and every platform so that it can be downloaded viably to perform social network identification. The source from which the images origined or shared are identified by trained classifiers. Friends can be recommended to users based on their interest they shared in profile information and the post they share on wall and reviews they give to another users. And also based upon the location they share while users check-in or through personal information given on profile. Loss of information can be avoided. If data size is large, size of grid view is extended which avoids the loss of information.

5. Implementation

The following pictures explain the detailed implementation of open social network platform is shown in fig 5.1. Open social network home page looks like this in fig 5.1 which gives users two option such that they login or new user can register by giving their personal information.

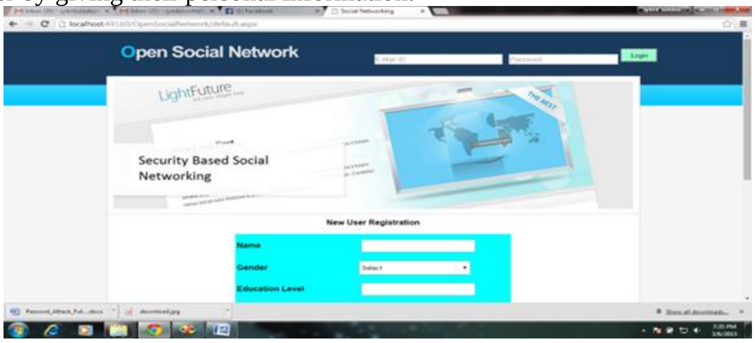
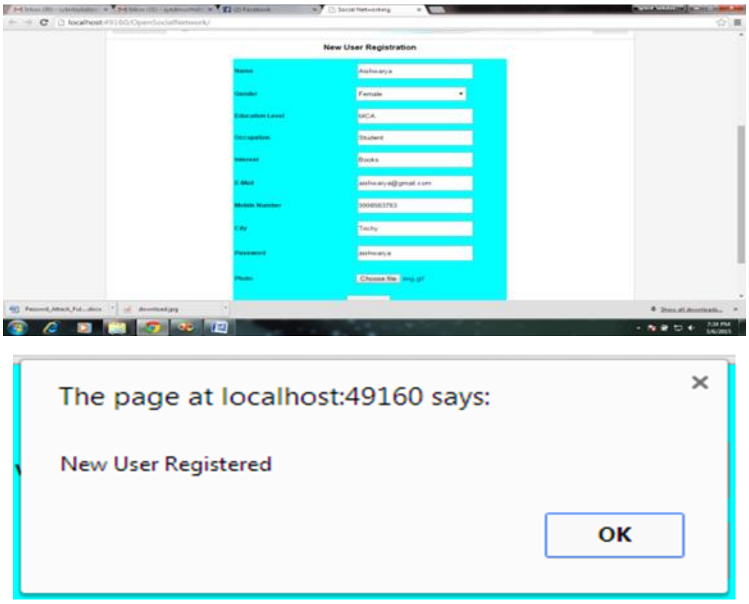


Fig 5.1 OSN Platform

Those who don't own their id, they can register themselves using New user creation is shown in Fig5.2



New User Registration

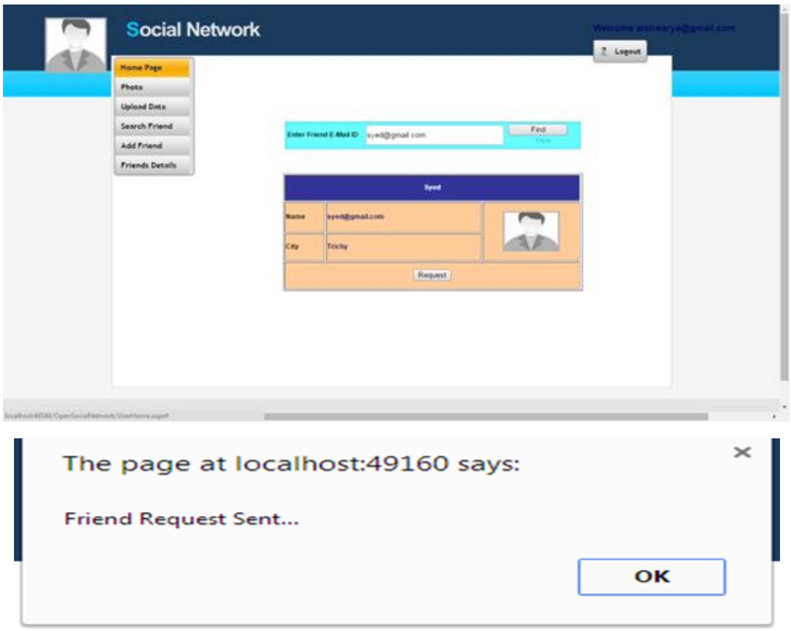
Name	Aishwarya
Gender	Female
Education Level	MCA
Occupation	Student
Interest	Books
E-Mail	aishwarya@gmail.com
Mobile Number	9994583783
City	Trichy
Password	aishwarya
Photo	Choose file img.gif

The page at localhost:49160 says:

New User Registered

Fig 5.2 New user creation

After creating new id, In Fig 5.3, OSN gives us an opportunity to search a friend by their name and gives them a friend request



Enter Friend E-Mail ID: syed@gmail.com

Syed

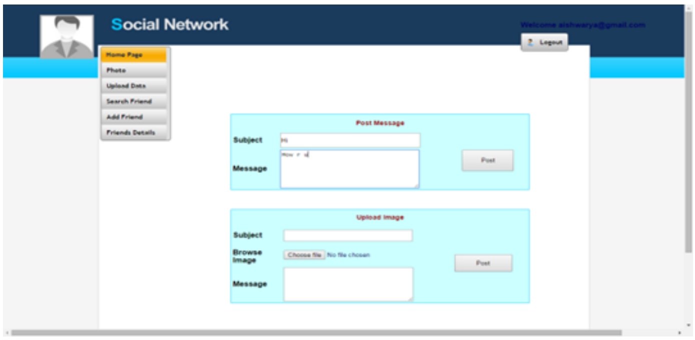
Name	syed@gmail.com
City	Trichy

The page at localhost:49160 says:

Friend Request Sent...

Fig 5.3 Send friend request

In fig 5.4(i), OSN allows to text and in fig 5.4(ii) shows that user can send images to a friend.



Post Message

Subject: Hi

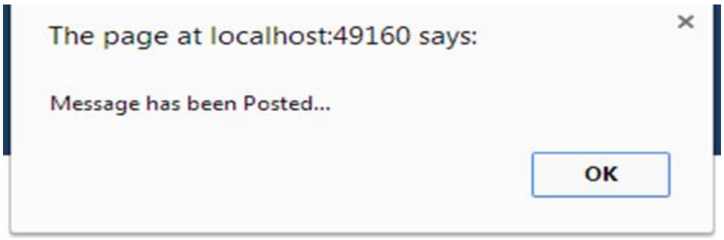
Message: How r u

Upload Image

Subject:

Browse Image: No file chosen

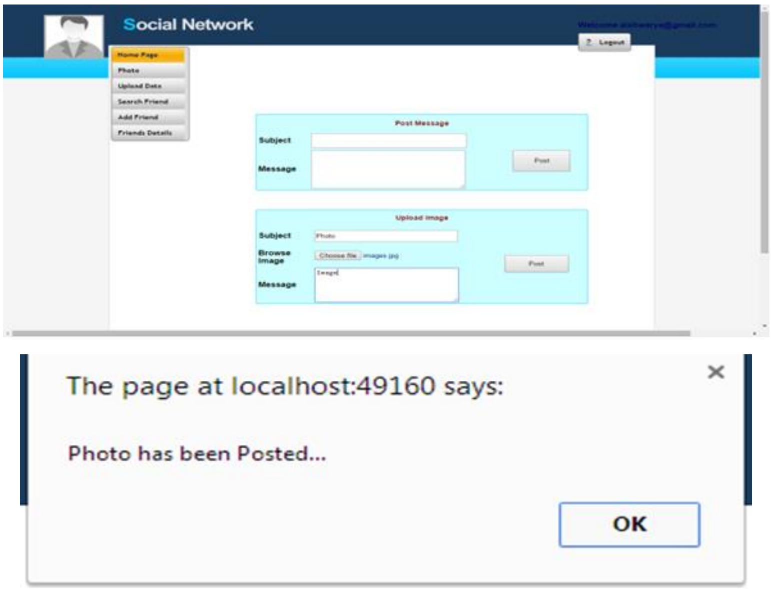
Message:



The page at localhost:49160 says:

Message has been Posted...

Fig 5.4(i) Send message to a friend



Subject: Photo
Browse Image: images.jpg
Message: Image

The page at localhost:49160 says:

Photo has been Posted...

Fig 5.4(ii) Send images to a friend

6. Conclusion

From various social networking sites the images in it are categorized by using novel method. When user uploads multiple images on a specific social network, the method proposed is used to distinguish the images. SVM classifier can be designed to determine the image origin by conducting study on many OSNs. The technique based on such features which by resorting at trained classifiers which is able to identify the provenance of social platform and also to detect the quality factor before uploading. Future work can be focused on more of the social networking sites such as instagram and google+

References

1. K. Choi, H. Byun, and K.-A. Toh, “A collaborative face recognition framework on a social network platform,” in Proc. 8th Int. Conf. Automatic Face and Gesture Recognit. (FG), 2008, pp. 1–6.
2. Z. Stone, T. Zickler, and T. Darrell, “Toward large-scale face recognition using social network context,” Proc. IEEE, vol. 98, no. 8, pp. 1408–1415, 2010.
3. “Autotagging face ook: Social network context improves photo annotation,” in Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), 2008, pp. 1–8.
4. J. Lukas, J. Fridrich, and M. Goljan, “Digital camera identification from sensor pattern noise,”
5. IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 205–214, 2006.
6. N. Khanna, G. T.-C. Chiu, J. P. Allebach, and
7. J. Delp, “Forensic techniques for classifying scanner, computer generated and digital camera images,” in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process.(ICASSP), 2008, pp. 1653–1656.
8. C. McKay, A. Swaminathan, H. Gou, and M. Wu, “Image acquisition forensics: Forensic analysis to identify imaging source,” in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process.(ICASSP), 2008, pp. 1657–1660.

9. M. Moltisanti, A. Paratore, S. Battiato, and L. Saravo, “Image manipulation on face ook for forensics evidence,” in Proc. Int. Conf. Image Anal. Process.(ICIAP), 2015, pp. 506–517.
10. R. Caldelli, R. Becarelli, and I. Amerini, “Image origin classification based on social network provenance,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 6, pp. 1299–1308, 2017.
11. M.-R. Ra, R. Govindan, and A. Ortega, “P3: Toward privacy-preserving photo sharing.” in Proc. 10th USENIX Symp. Netw. Syst. Design Implem. (NSDI), 2013, pp. 515–528.
12. J. Ning, I. Singh, H. V. Madhyastha, S. V. Krishnamurthy, G. Cao, and P. Mohapatra, “Secret message sharing using online social media,” in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), 2014, pp. 319–327.
13. W. Sun, J. Zhou, R. Lyu, and S. Zhu, “Processing-aware privacypreserving photo sharing over online social networks,” in Proc. ACM Multim. Conf.(ACMMM), 2016, pp. 581–585.
14. G. K. Wallace, “The jpeg still picture compression standard,” IEEE Trans. Consum. Electron., vol. 38, no. 1, pp. xviii–xxxiv, 1992.
15. Vetriselvi T, G.RajendraKannammal,” Efficient Post Classification Change Detection of land cover images using Multi-ScaleSegmentation and Self Organizing Feature Map: Results International Journal of Scientific Research in Computing”, 2019.
16. T. Avudaiappan, R. Balasubramanian, S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, K. Shankar,” Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm: Results Journal of Medical Systems”, 2019.
17. M.Sivakumar, Dr.U.Srinivasulu Reddy,” Aspect Based Sentiment Analysis of Students Opinion using Machine Learning Techniques: Results International Conference on Inventive Computing and Informatics”, 2018.
18. Aarthi, M. and Bhuvaneshwaran, A., 2021. Iot Based Drainage and Waste Management Monitoring and Alert System for Smart City. Annals of the Romanian Society for Cell Biology, pp.6641-6651.
19. Pavithra, M., Sindhana, A.M., Subajanaki, T. and Mahalakshmi, S., 2021. Effective Heart Disease Prediction Systems Using Data Mining Techniques. Annals of the Romanian Society for Cell Biology, pp.6566-6571.
20. Tresa, M., Francina, S., Jerlin Oviya, V. and Lavanya, K., 2021. A Study on Internet of Things: Overview, Automation, Wireless Technology, Robotics. Annals of the Romanian Society for Cell Biology, pp.6546-6555.