International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

HAMPERING THE CLONING ATTACKS IN ONLINE SOCIAL NETWORKS

S. SWETHA[1], M. VAISHNAVI[2], M. VIDHYA[3]

[1,2,3] *B.Tech, Department of information technology, Valliammai engineering college, Tamilnadu, India.*

Abstract – *The millions of active users all around the world are using online social network such as Facebook, Twitter, Tumbler and LinkedIn. The usage of online social network make it effortless to misuse user's information and to identity cloning attack to form fake profile .Fake users misusing the authorized users information's like text, photos and videos with or without the authorized user's permission. This paper is designed to provide security to the user images in social networks. Hence, in this paper, when users upload the profile picture or photos it would be watermarked and updated. Any fake users uploading the same profile picture can be detected and their respective IP would be tracked and blocked. Thus if any user account is find suspicious, an automated scanning is performed. So when the fake user's login next time, an alert message would be sent to the account owner and the user activities would be closely monitored. If the account owner doesn't respond the alert message the account would be suspended with prior information. And also when users uploading their images to the cloud computing platform, they lose direct control on these data, so users worry that their personal privacy information will be leaked and misused. In order to protect the user's personal privacy, before uploading images to the server, the image needs to be encrypted. The image will be encrypted by DWT image steganography method (hiding one image inside another image). This paper would be useful for preventing the cloning attacks.*

Keywords: cloning attack, watermarking, personal privacy, DWT, steganography

1. INTRODUCTION

Social networks are becoming so essential now a days and plays a bigger role in every day's life for sharing personal information's and knowledge sharing. Also social network is used to see the everyday activities, photos, videos and political activities happening. The millions of active users all around the world are using online social network such as Facebook, Twitter, Tumbler and LinkedIn. Thus the major concern in social network is fake users misusing the authorized user information like text, photos and videos with or without the authorized user permission. Currently many fake profiles have been created for fraudulent activities like money making, malware / virus / Trojan virus distribution to track the user behaviour. Also a research states many fake Profiles have been created for online social games. In existing social network, the individual information's are kept secret and transmitted in a secure manner with user privacy preserving. Thus even intruders have breached the privacy preserving in many scenarios. Thus many privacy attacks have been identified now a days to steal the user personal information for malicious activities. Thus this leads to a huge security problems. CNET report in the year 2013 states Facebook has 8.7% fake users which are approx. 83.09 million users. Thus in existing fake users are been difficult to be tracked. Thus if any user account is find suspicious, an automated scanning is performed. So when the fake user's login next time, an alert message would be sent to the account owner and the user activities would be closely monitored. If the account owner doesn't respond the alert message the account would be suspended with prior information

2. EXISTING SYSTEM

In the existing system, there is no security for profile images and shared images and also existing system defines the encryption mechanism with the help of a trusted party. A social network user might choose to encrypt photos before posting in a platform by employing some encrypted mechanisms such as attribute-based encryption. The existing system use traffic analyzing and graph analyzing method which all are human monitoring method and not automatic.

2.1 DISADVANTAGES

- No security for profile pictures. User profile pictures are misused for creating a fake profile.
- There is no effective secure transmission of images.

3. PROPOSED SYSTEM

In the proposed paper, Watermarking techniques will be used to detect and identify such fake profiles. In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username would be attached to pictures by means of watermarking methods. Accordingly, in future, if somebody else saves that picture and attempts to create a fake profile with stolen data, the system is able to automatically detect this deception as fraud and would prevent and protect the fake user from any additional positive action. Our proposed system invokes discrete wavelet transform algorithm for data hiding. Thus this would prevent the clone attacks and providing complete user data privacy preserving. For watermarking technique Java static watermarking is been used. Any fake users updating the same profile picture can be detected and

their respective IP would be tracked and blocked. Also this system provide secure authentication by invoked certain attributes which can be asked to the users during registration. Thus we can able to avoid clone attacks in social media networks.

3.1 ADVANTAGES

- User identity are secured.
- User can securely transmit the images from the user side to cloud and also share images using DWT based image steganography.
- Clone attack is effectively prevented.

4. SYSTEM MODEL

The Fig-1 explains the user activities such as sharing a image, uploading images to cloud. The admin can perform the actions such as authorization of the user, watermarking the image, verification, upload the steganographic images to the cloud storage.

First the user has to register into the system. At the time of registration it will get all details and it will automatically obtain the IP address of the user. Then the user login in to the application and the admin checks whether the user is an authorized user and then permits the user to move on to the next level. The user will set the profile picture or sharing images to the application. It will automatically watermarked by his/her username in the image and uploaded in the system.

Second step is that if any unknown user downloaded the image and after downloading he/she modify the image and try's to upload in the system, it will validate the image. The validation is done by checking if there is any existence of watermark. If already any watermarking is in the image then an alert will send to the original user. Then the original user will decided whether to allow or not. If the original user will send a block message then the image cannot be uploaded. If the process has been repeated then the user IP will be blocked.

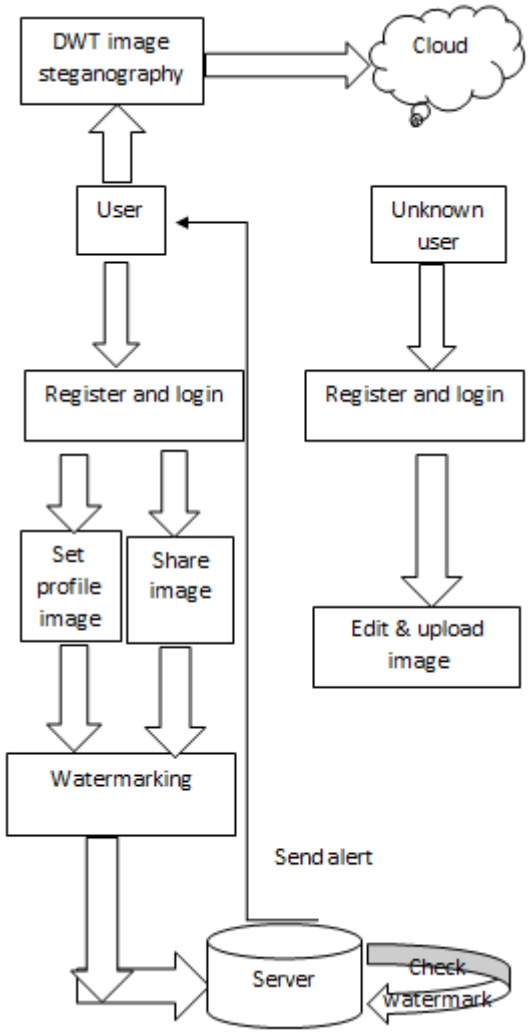

Fig -1: ARCHITECTURE DIAGRAM

When the user upload the images in the cloud, first the images will be secured by DWT steganography method that means hiding the original image inside the cover image and uploaded to the cloud.

5. MODULE DESCRIPTION

5.1 USER REGISTRATION

The User wants to create an account and then only they are allowed to access the Application. Once the User creates an account, they can login to their account. All the user details will be stored in the database. During registration of the user, credentials like username, password, phone number and Email ID are obtained and also it will get the IP address. An application is designed for User Interface, Frame to Communicate with the Database through JDBC Coding using the programming Languages like Java.

5.2 SHARING IMAGES

The user can shared images or set profile pictures. The images will be watermarked and uploaded. A Static Watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal. In this method, at any time a user uploads his/her pictures, some exclusive and useful information such as email or username would be attached to pictures by means of watermarking methods.

5.3 ALERT AND BLOCK

In this alert and block, system will automatically check the right and privilege of the user and ownership of uploaded file. Subsequently to checking the uploaded file, if the system finds the existence of watermark, it will send an announcement and a notification to the owner of original content and prevent user from re-uploading. Fake users updating the same profile picture can be detected and their respective IP would be tracked and blocked

5.4 DWT IMAGE STEGANOGRAPHY

Image Steganography is the process of hiding an original image within the cover image and the extraction of it at its destination. Steganography is a technique of hiding an encrypted message so that no one suspects it exists. Dwt is a linear transformation operates on a data vector that separates data in to different frequency components. The wavelet transform separates the high frequency and low frequency information on a pixel. In this we were using Haar wavelet in this the low frequency wavelet coefficients will be obtained by averaging the two pixel values and the high frequency coefficients will be obtained by taking half of the difference of the two pixels. The obtained bands are Approximate band (LL), Vertical band(LH), Horizontal band(HL), Diagonal band(HH).

5.5 UPLOADING TO CLOUD

The user can upload the images to the cloud in a secure manner.

6. CONCLUSION

In this paper, cloning attack problem is studied. The proposed system provides result for providing security to the user profile images or shared images. An efficient watermarking algorithm is to provide security to the user images and to identify the fake users. Also, the fake profiles would be blocked in this system. The steganography is also used to provide security to the user images. The cloning attack across different social network can be prevented in future.

ACKNOWLEDGEMENT

We would like to thank our project guide Prof.Thenmozhi (Assistant Professor, Department of Information and Technology, Valliammai Engineering College), for their guidance throughout this project. We also like to thank our members of the department for their kind assistance and cooperation during the development of the project.

7. REFERENCES

[1] Georges A.Kamhoua, Niki Pissinou, S.S.Iyengar, Jonathan Beltran, Charles Kamhoua, Brandon L Hernandez "Preventing Colluding Identity Clone Attacks in Online Social Networks", IEEE 37th International conference on Distributed computing systems workshops, PP:187-192, 2017

[2] Mouro Conti, Radha Poovendran, Marco Secchiero "Fakebook: Detecting fake profiles in on-line social networks" IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, PP:1071-1078, 2012

[3] Po-Yueh Chen, Hung-Ju Lin "A DWT Based Approach For Image Steganography", International Journal of Applied Science and Engineering, Volume:4 no: 3, 2006

[4]] Chunyan Zhang, Jingbing Li, Shuangshuang Wang, Zhaohui Wang, "An encrypted medical image retrieval algorithm based on DWT-DCT frequency domain", IEEE 15th international conference on software engineering research, management and applications(SERA),PP 135-141,ISBN 978-1-5090-5756-6, 2017

[5] S.Priyanga, V.M.Priyadharshini, N.Hariharan "Prevention of Fake Profile Proliferatiion in Online Social Networks", International Journal of Innovative Research in Science, Engineering and Technology, volume: 4, 2015.