FAKE PROFILE IDENTIFICATION AND AVOID PROFILE DUPLICATION

Mr. K. Arun Prasad
Associate Professor
Department Of Information Technology, Agni College of Technology, Chennai
arunprasad.it@act.edu.in

Jayashree S
Department Of Information Technology, Agni College of Technology Chennai
jayashreesk95@gmail.com

Ashwini S
Department of Information Technology, Agni College of Technology, Chennai
ashwinisekar1@gmail.com

***Abstract* — Nowadays most of the user using social networks in our daily life. We are using it to keep in touch with our friends and find some new friends. Many of the social networks are providing less authentication method to user. Which is based on some information like display name and posting photo in the social network. These provide weaker authentication make it more effortless to misuse he/she information and they do a cloning attack to form a fake profile. We using data hiding technique to hide information in profile picture or photo to detect fake profile and is associated with digital forms as cryptography, steganography and watermarking. In this project we are using discrete wavelet transform algorithm for data hiding .this would prevent clone attack in social network. Also when the user uploading his/her profile photo it will be watermarked and then only it updated in social network. Java static watermarking algorithm is used for watermarking technique. We can avoid the clone attack in the social networks.**

Keywords— Social Network; watermarking technique; Steganography; discretewavelet

I. Introduction

In our own social network, we will allow users to share and post about their personal information and have a virtual presence in a virtual society that everyone can interact. These social network are rapidly becoming the medium for communities in different parts of the world to keep in contact, share and distribute information about their everyday activities, photos, travels and political upraising. There also exists a growing concern about fake users who can easily deceive themselves off as someday else, by using photos and profiles either snatched from a real person(without him/her knowing) or generated artificially, In our real world, fake accounts are created for moneymaking malicious activities. These activities involve click-fraud, spamming, malware spreading and fraud of identity.

Given the huge amount of individual information that is shared between friends in an online social network, protecting and preventing the privacy of individual user becomes into view as a significant problem. In current years, numerous privacy threats that take advantage of personal data of a user or unintended vulnerabilities of online social network have been reported. Fake accounts allow breeding scammers and would imposters attribute a serious security problem.

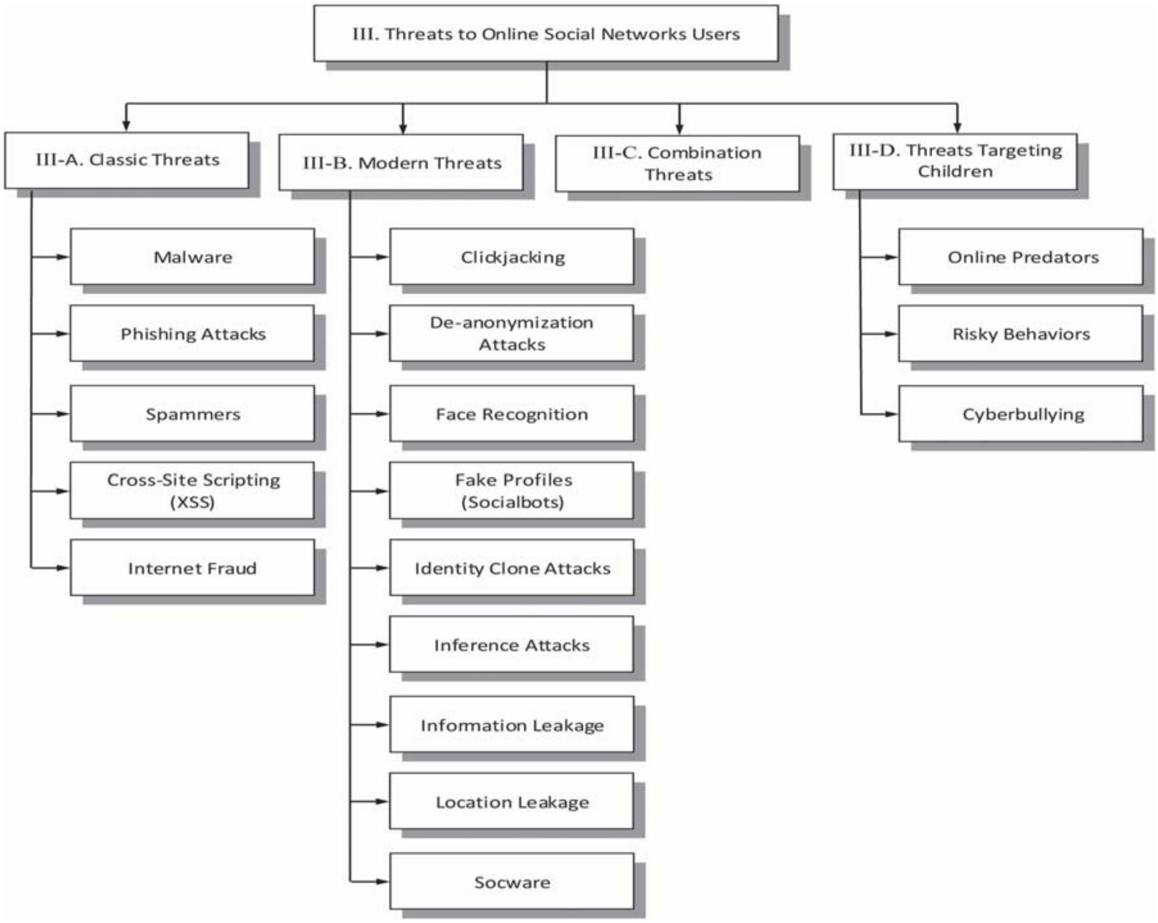

Fig.1.Threats to social network users

II. Problem Statement

Even though most of the social networks have already added privacy setting features for each post, however, still any private information can be leaked. Let's say a post like a picture is on a user profile and user have set the e privacy for the picture to be seen just for one of user's friends and user think it's totally safe. But there is no guarantee that user's friend will not share your picture with anyone else, means that user's friend can easily save picture and upload it somewhere or share it with someone else without any notification to user.

The users don't care much about what they are sharing on social networks and the privacy of their post, it can be quite troublesome for them. On top of all benefits of online social networks, there are many disadvantages identity theft is one of the biggest concerns of online social networks. There are millions of fake profiles, which maliciously manipulate or harm other people and the reason for this matter is that it is very simple and quite fast to create and form a fake profile b using other's information or picture and use social engineering techniques to steal information.

III. Proposed System

Detection and identifying fake profiles and botnets in social networks are restricted to user's report and just subsequent to a number of reports for particular user; the system will check the validation of user.

In the proposed approach, steganography techniques and methods 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 and also date of upload 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 and 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. Also when users upload the profile picture or photos it would be watermarked and updated. For watermarking technique *Java static watermarking* systems and algorithms is been used. Any fake users updating the same profile picture can be detected and their respective IP would be tracked and blocked. Also in our project to provide secure authentication we have invoked certain attributes which can be asked to the users during registration. Thus we can able to avoid clone attacks in social media networks.

IV. Implementation

a. **Social network** - which can be asked to the users during registration. By getting the permission from the original user only, the other user can download his/her profile pictures and shared pictures. Majorities of social networks have weak user authentication method, which is based on some basic information like displayed name, photo. These weaknesses make it effortless to misuse user's information and do identity

b. **Java static marking -** *Watermarking* is the process of hiding digital information in a carrier signal. In this method, anyone tries to download his/her profile picture need to get the permission from the original user. IF Original user allow the other user to download his/her own picture. The watermarking technique will removed and picture will be downloaded automatically.

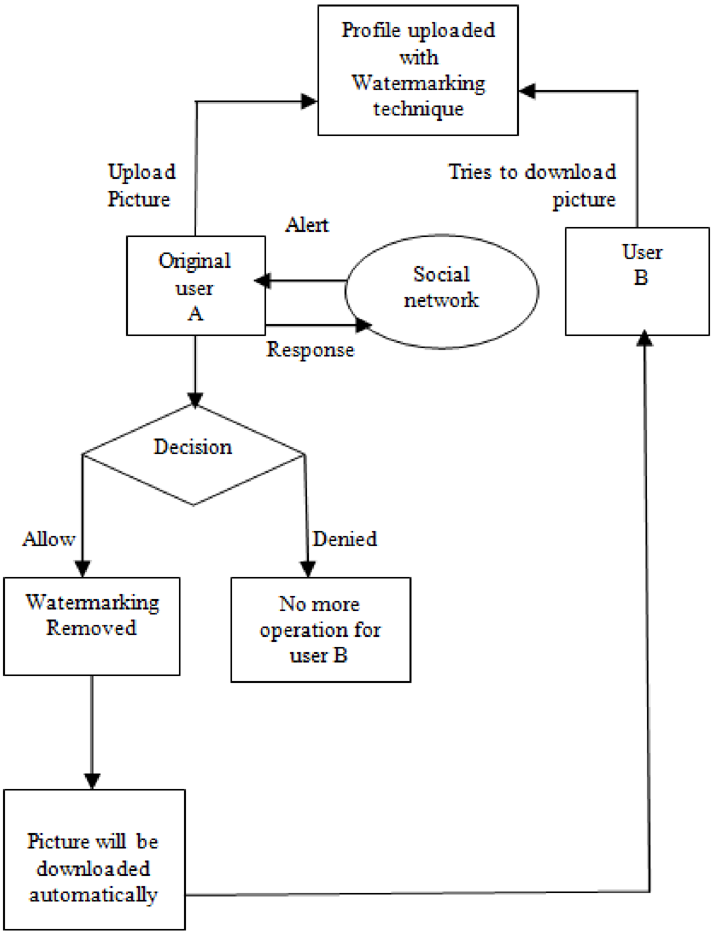

Fig.2. Architecture diagram

A. ***Static watermarking:*** Static software watermarks are stored in the applicaton executable itself.For example this could be stored in the executable or in the string resources.There are two types of static watermarks mamely data and code.

B. ***Java watermarking***:Java programs distributed on the internet are having serious problem with the copyright infringement.Java decompliers such as Mocha can be used to decompose class files into source files.Many of the solution available are either commercial or research-orineted such as SandMark.An example commercial applicaion is Dasho createdd by premptive solution which inserts watermarks into source code.

C. **Image steganography (DWT) -** *Steganography* is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography is a technique of hiding an encrypted message so that no one suspects it exists. The discrete wavelet transform is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. We use *discrete wavelet transform* algorithm for data hiding. Thus this would prevent the clone attacks and providing complete user data privacy preserving. Also when users upload the profile picture or photos it would be watermarked and updated.

The wavelet transform has gained widespread acceptance in signal processing and image compression. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet called mother wavelet by dilations and shifting. The DWT has been introduced as a highly efficient and flexible method for sub band decomposition of signals. The 2DDWT is nowadays established as a key operation in image processing .It is multi-resolution analysis and it decomposes images into wavelet coefficients and scaling function. In Discrete Wavelet Transform, signal energy concentrates to specific wavelet coefficients. This characteristic is useful for compressing images. Wavelets convert the image into a series of wavelets that can be stored more efficiently than pixel blocks. Wavelets have rough edges, they are able to render pictures better by eliminating the blockiness‖. In DWT, a timescale representation of the digital signal is obtained using digital filtering techniques. Image consists of pixels that are arranged in two dimensional matrix, each pixel represents the digital equivalent of image intensity. In spatial domain adjacent pixel values are highly correlated and hence redundant. In order to compress images, these redundancies existing among pixels needs to be eliminated. DWT processor transforms the spatial domain pixels into frequency domain information that are represented in multiple sub-bands, representing different time scale and frequency points. One of the prominent features of JPEG2000 standard, providing it the resolution scalability, is the use of the 2D-DWT to convert the image samples into a more compressible form. The JPEG 2000 standard proposes a wavelet transform stage since it offers better rate/distortion (R/D) performance than the traditional DCT. This essentially divides the array into two vertical halves, with the first half storing the average coefficients, while the second vertical half stores the detail coefficients. This process is repeated again with the columns, resulting in four sub-bands (see Fig. 1) within the array defined by filter output. Fig. 1 shows a three- level 2D DWT decomposition of the image.

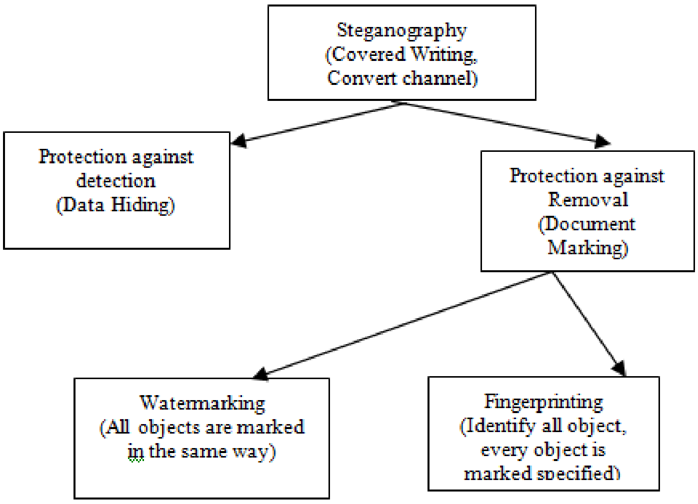

Fig.3. An analysis of Steganography techniques

D. Intrusion detection system - An intrusion detection system (IDS) is a software application that monitors a network or systems for malicious activity or policy violations. IF any violation occurs it will be reported to the administrator using a security information and event management (SIEM). SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms. System will automatically check the right and privilege of the user and ownership of uploaded file.

E. Alert and block - Once original user gives the reply as deny to other user, after that he/she try to download and the IP address will be tracked and there account will be made blocked for the respective original user.

V. Summary

In this proposed system, data hiding techniques to hide some information in profile pictures in order to detect botnets and fake profiles and finally will propose an automated model to detect fake profiles and botnets instead of current manual method which is costly and labour-intensive. This project presents a classification and analysis of detection mechanisms of clone attacks on online social network, based on attribute similarity, friend network similarity, profile analysis for a time interval and record of Internet Protocol sequences.

VI. Conclusion

Social networks have become some of the most popular websites and services on the internet, and usage is growing among of all ages. More and more interactions, both personal and business, are done on social networks, security and privacy of social network website is a noteworthy issue since they are getting more popular each day and lack of security and privacy can result on our daily lives. Classifying fake users on online social network has always been a challenging computational task and the current ones show to be improper. In this paper watermarking and steganography was proposed to detect identity cloning.

VII. Reference

[1] Nielsen, Social Networks and Blogs, 4th Most Popular Online Activity, Nielsen Online Report, 2009.
[2] Stolen Facebook Accounts for fake profile detection.
[3] Personal communication with the Manager of User Support and the Product Manager of the Core and Community Management teams in Tuenti, 2011.
[4] Fake Accounts in Facebook - How to Counter it, http://tinyurl.com/5w6un9u, 2010.
[5] Why the Number of People Creating Fake Accounts and Using Second Identity on Facebook are Increasing, http://tinyurl.com/3uwq75x, 2010. Nielsen, Social Networks and Blogs, 4th Most Popular Online Activity, Nielsen Online Report, 2009.
[6] Boyd, D and Ellison, NB, Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, 13, 2 (2007).
[7] Stolen Facebook Accounts for Sale, http://tinyurl.com/25cngas,2010.
[8] Personal communication with the Manager of User Support and the Product Manager of the Core and Community Management teams in Tuenti, 2011.
[9] Fake Accounts in Facebook - How to Counter it, http://tinyurl.com/5w6un9u, 2010.
[10] Why the Number of People Creating Fake Accounts and Using Second Identity on Facebook are Increasing, http://tinyurl.com/3uwq75x, 2010.
[11] Guardian, Twitter Hoaxer Comes Clean And Says: I Did It To Expose Weak Media, Guardian, 2012.
[12] Post, W, Twitter Hoaxer Tommaso De Benedetti Comes Clean, Washington Post, 2012.
[13] Salon, the Fake Facebook Profile I Could Not Get Removed, Salon.com, 2012.
[14] Roberts, S, Fake Facebook Friends - People Behaving Badly, Youtube, 2012.
[15] Desai, V.H, Steganography, Cryptography, Watermarking: A Comparative Study, Journal of Global Research in Computer Science, Vol.3, No.12, Dec 2012. An Automated Model to Detect Fake Profiles and botnets in Online Social Networks …. DOI: 10.9790/0661-17146571 ww.iosrjournals.org
[16] Center, ITR, Facebook Social Media Survey 2012.
[17] Cox, I, Miller, M, Bloom, J, Fridrich, J and Kalker, T, Digital Watermarking and Steganography, 2nd Edition, Morgan Kaufmann, 2007.
[18] Cox, I,, Miller, M,, Bloom, J, and Miller, M, Digital Watermarking, Morgan Kaufmann, 2002.
[19] Popa, R, an Analysis of Steganographic Techniques, The "Politechnica" University of Timisoara, 1998.