International Journal of Engineering & Technology, 7 (2.24) (2018) 307-310

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Survey of Algorithms Used for the Prevention of Fake Profiles in Social Networks

Manish Dandwani, Vishal Vaibhav, S. Nagadevi

[1,2]*Department of Computer Science and Engineering, SRM University, Kattankulathur, Tamil Nadu, India.*
**Corresponding Author Email: dandwani.manish@gmail.com*

Abstract

A great many dynamic clients all around the globe are utilizing on the web informal community, for example, Facebook, Twitter, Tumbler and LinkedIn. These shortcomings make it easy to abuse client's data and do personality cloning assault to frame counterfeit profile. In this proposed framework, information concealing systems to shroud some data in profile pictures with a specific end goal to identify botnets and counterfeit profiles. This venture introduces an order and examination of discovery instruments of clone attacks on online interpersonal organization, in light of trait similitude, companion arrange closeness, and profile investigation for a period interim and record of Internet Protocol groupings. In this task we have proposed discrete wavelet change calculation for information covering up. In this manner this would keep the clone assaults and giving complete client information protection saving. Likewise when clients transfer the profile pictures they can be watermarked and refreshed. For the watermarking method Java static watermark can be used. Any phony clients refreshing a similar profile picture can be distinguished and their separate IP would be followed and blocked. Likewise for secure picture transmission, we utilized Discrete Wavelet Transform (DWT) for information concealing/steganography and Discrete Cosine Transform (DCT) for picture pressure.

Keywords: *Fake profile, clone attacks, DWT, DCT, watermarking.*

1. Introduction

Social network has become a daily necessity and play really big roles in sharing of personal data and knowledge. Many people share their photos, videos etc. to the different social media to tell about their personal life. Users typically access the social media via any device such as Mobile, Laptop, Tablets. World is gradually increasing it connection to the power of internet. Social media increases the interaction between the human beings and helps them for recreation [1]. It helps people in increasing their contacts and making new ones. This also becomes prone to attacks as unauthorized users try to manipulate and use data like photos text etc of existing users. In recent days many fake accounts have already been created for use of malicious activities. There is a desideratum to reduce fake profiles. [3]

2. Social Network

Social media and network has been evolving since the time cyber technology has been developing. Usenet was one of the first online communities to be formed by Duke university graduates. It was a kind of discussion forum where students could voice their suggestions and opinions. After the invention of www by Tim Berners Lee social media evolution skyrocketed.[4]

There are many advantages of gregarious networks such as it ameliorates the edification of adults and children and have wide influence on learners. It avails in engendering discussion forums class blogs. Gregarious networking is platform where one can discuss conceptions. It avails in marketing of a company, where one can expand its business.

There are many disadvantages withal, recently many cybercrime proposed an incrementing threat to all the users. Cyber bullying is one of the cyber malefaction which includes different branches.

Fig. 1: Social Media

3. Fake Profile

In Online Social Networks there are many fake users who are using the profiles of the innocent human beings and misusing them. This is known as Fake Profile Attack (FPA). In the FPA personal informations is used to create a different account without prior information to the original user.

Along with performing the research for the communities, OSN managers also take interest in detection of fake profiles and identifying the individual behind this malicious practice. For instance, Facebook removes the profiles that have been created with random strings [4]. But still intruders have managed to breach the privacy settings and many attacks have come to surface which is leading to many security problems. Thus many techniques have been formed for thise prevention[3].

4. Related Work

There are many ways in which cloning attacks can be stopped. From the past years there are many techniques which are applied to solve this problem. Some of the techniques and their consequences are described below.

A. Clone Attacks

Many sensor nodes are deployed in the truculent environment which lack physical shielding, the sensor and the social network are vulnerable to many physical attacks including clone attacks. In this attack, the intruder steals data and extract all the credentials like keys ,identities ,stored codes , images , videos and make a replica of the captured information and introduces it in designated place in the network. [4][9]

We have made sure that every individual information on the network should posses a scheme to detect the copyright of the original information so that its replica can’t be mishandled and misused over the networks.

The issue of replica detection has become a major concern in the field of security. In this paper we have see the different methods that subsist the clone attacks.

B. DWT(Discrete Wavelet Transform)

In the functional and the numerical analysis , a DWT is the wavelet transform in which wavelets are made to be sampled discretely. The DWT is better as compared to the Fourier Transforms as it takes into consideration the temporal resolution and it can capture the location and frequency information at the same time [2].

The pristine image is then high-pass filtered, which yields the three astronomically immense images, in which each describe the local transmutations in effulgence (details) in the pristine picture. It is then made to pass through a low pass filter as well as it is downscaled to yield an approximation image which is then high passed to give three more diminutive detail images, and low-pass filtered to engender the final approximated image in the upper-left.

Wavelet transform decomposes the image into four components, which are designated as low resolution(LL), and the rest corresponds to vertical (LH) and diagonal (HH) ,horizontal (HL), the low resolution may be further decomposed into high frequency and low frequency components.

Wavelet decomposition may be applicable to compression of image and detail enhancement of the image.

C. Hybrid Watermark

This is an amalgamation of robust and fragile framework. The fragile watermark is beneficial as it has good properties of security and localisation. The hybrid watermark works in the way that it can be used to differentiate between malicious or simpler operations [5].

The authentication procedure can be done by not accessing the information about the actual image . Also there is a more effective HDW scheme that makes the use of direct sequence spread method which works in the way that when a watermark image is found it's made to compare with original image and in that way the watermark image is detected .it's a modification of the method that combines the logo method and key. We make the use of a binary image as a watermark image to compare it with original and calculate the invisibility .[5]

D. Steganography (Data Hiding)

Steganography is the method of communicating information like text, images,etc in a manner that the original information is hidden and maybe encrypted. It provides great security to the information stored in the networks.

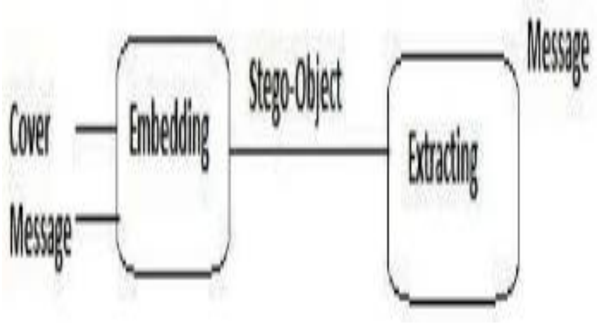

Fig. 2: Steganography

Steganography can be in both textual forms and on images. In the simple textual form, a particular set if texts are steganographed with other cover texts to convert it into an stego object.

In the proposed system we have tried to steganograph an image with another cover image and stored it over the network. It has many advantages as it makes the original image safe from any kind of surveillance and making it safe from the radar of any intruder in the network who may mishandle the information. We have used various techniques for Steganography which have been discussed in the survey.

E. Wavelet Based Watermarking

In this method we first work by inserting the watermark in the middle of the range of frequency. The filter banks could be preserved for watermark embedding. A coefficient is chosen for replacement of image [6]

The advantages of this approach

- With the help of this we can achieve frequency localisation as well as spatial.
- As well as with robustness it has perceptual invisibility for compression
- It has robustness to various factors like noise geometric transform etc
- Frequency and spatial domains can both have watermark embedding [6]

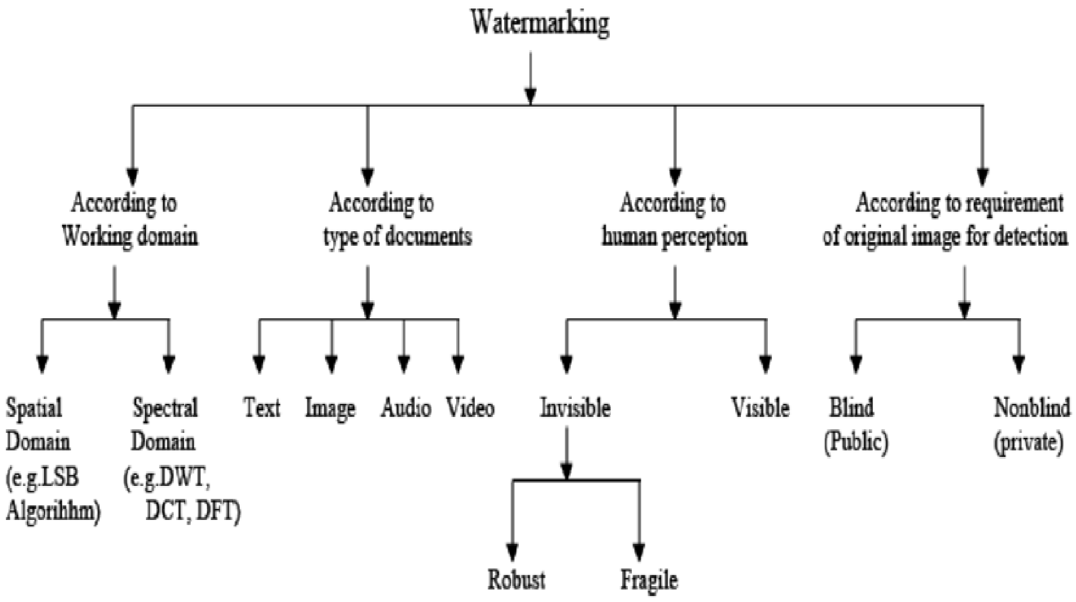
Watermarking
According to Working domain
According to type of documents
According to human perception
According to requirement of original image for detection
Spatial Domain (e.g.LSB Algorihhm)
Spectral Domain (e.g.DWT, DCT, DFT)
Text
Image
Audio
Video
Invisible
Visible
Blind (Public)
Nonblind (private)
Robust
Fragile

Fig. 3: Types of Watermarking

F. Clone attacks in WIS(Wireless Sensor Networks)

Various detection techniques are form in this paper like high level as radio and network based schemas. There are different type of techniques such as centralized detection techniques and distribution detection techniques.[7]

There are many proposed method which rely on centralized authority such as

- Set Operations
- Cluster Based Approach
- Detecting replicated keys
- Fingerprint Verification

In distributed detection detective methods are performed by watcher nodes which have been selected by network nodes and it's not based on central authority

- Node-to-Network Broadcasting
- Randomized multicast
- Line Selected Multicast
- Random Walk based approach [7]

G . Image Watermarking based on DWT

Many researches that have already been conducted on watermarking systems have found that substance of the pictures can come handy for enhancing the vigour and imperceptibility. In the following method we make watermark from the host picture and the dwt is used for the insertion of watermark because of its feature of time recurrence strategy in which adjustment can be made for extracting the data of the image

In some fundings a key wavelet change is embraced. In some researches a watermarking method based on wavelet tree is used for taking into consideration aspects like upside of limitation and multi determination . It works as host image is transformed in wavelet coefficients using DTWT in which the watermarks are then collected into super trees by the use of two super trees watermark bits are formed. Since the watermark bits are scattered in groups and the data of the watermark bit is spread all through extensive spatial districts, along these lines the watermarking method is powerful to assaults in both recurrence and time spaces. This procedure is helpful for evacuation of high-pass points of interest in JPEG pressure and hearty to time space assaults, for example, pixel moving and turn. Notwithstanding copyright security, the proposed watermarking plan can likewise be connected to information covering up or picture confirmation. Some researches produce a method for utilising watermarking along with encryption to find duplicates etc. The LL and hh groups are made to implement watermarks for bringing down the frequency and help gather assaults for example obscuring, revolution, honing, trimming etc.

Luo et al. presented a whole number watermarking methods which was wavelet based to ensure copyright system to upgrade the security. This system is helpful for computerized watermarking in DEM (advanced rise mode) information, which successfully ensures the copyright of DEM information and stays away from the unapproved client. As lifting based plan is added to build the minimally bolstered wavelets whose coefficients are made out of a free factor in this way, it utilizes just basic option and move which is quick and effortlessly acknowledged by means of equipment. As set of wavelength coefficient is install watermark data, consequently the bit is embedded in the high movement surface locales with the greatest quality of Just Noticeable Distortion (JND) resistance of Human Visual System (HVS) that makes the advanced watermark strong.

H. Digital Watermarking using LSB

A robust and simple watermarking algorithm which uses the fourth and third significant digits method. It is better than the previous LSB technique for the hiding of data[8].

The data and the original image is fed into the machine then the image is hidden using the watermarking algorithm after that data is retrieved from the watermarked image.

The LSB method is used for operations that are simple and embed image in cover picture . A secret message is received that helps in changing cover picture pixels in LSB though it's a 8 byte Grid atleast 1-4 bits need to be changed therefore accordingly only like half of the bits will be required to hide the message in cover picture. [8]

4. Conclusion

As we have seen that there is a need for privacy of the user's personal information as anyone can misuse the data of anyone that's why several techniques are evolved since the long time. We have seen several statergies like Watermarking and algorithms like DWT etc. These help in reducing the clone attacks or fake profile attacks and give the privacy to the users of social media.

References

[1] Mauro Conti, Radha Poovendran, Marco Secchiero "FakeBook: Detecting Fake Profiles in On-line Social Networks" IEEE 2012

[2] Chunyan Zhang, JingBing Li "An encrypted medical ,mage retrieval algorithm based on DWT-DCT) frequency domain" IEEE 2017

[3] Aditi Gupta and Rishabh Kaushal "Towards Detecting Fake User Accounts in Facebook"

[4] Deepti Dave, Nishchol Mishra and Sanjeev Sharma "Detection Techniques of Clone Attack on Online Social Networks: Survey and Analysis", Elsevier

[5] Jiri Fridrich SUNY Binghamton and Mission Research Corporation , "A HYBRID WATERMARK FOR TAMPER DETECTION IN DIGITAL IMAGES", Fifth International Symposium on Signal Processing and its Applications, ISSPA ‘99, Brisbane, Australia, 22-25 August, 1999 Organised by the Signal Processing Research Centre, QUT, Brisbane, Australia

[6] Yiwei Wang,, John F. Doherty, and Robert E. Van Dyck "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE 2002

[7] Rubal Grewal, Jasleen Kaur, "A Survey on Proficient Techniques to Mitigate Clone Attack in Wireless Sensor Networks" IEEE 2015

[8] Abdullah Bamatraf , Rosziati Ibrahim "Digital Watermarking Algorithm Using LSB" 2010 International Conference on Computer Applications and Industrial Electronics (ICCAIE 2010), December 5-7, 2010, Kuala Lumpur, Malaysia, IEEE 2010

[9] Georges A. Kamhoua1, Niki Pissinou1, S.S. Iyengar1, Jonathan Beltran "Preventing Colluding Identity Clone Attacks in Online Social Networks" , IEEE 2017

[10] Ehsan Ahmadizadeha, Erfan Aghasianb,1,Hossein Pour Taheric, Roohollah Fallah Nejadd "An Automated Model to Detect Fake Profiles and botnets in Online Social Networks Using Steganography Technique.", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. IV (Jan–Feb.2015),PP65-71

[11] S.V.Manikanthan and V.Rama“Optimal Performance of Key Predistribution Protocol In Wireless Sensor Networks” International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special –March 2017.

[12] T. Padmapriya and V. Saminadan, “Priority based fair resource allocation and Admission Control Technique for Multi-user Multi-class downlink Traffic in LTE-Advanced Networks”, International Journal of Advanced Research, vol.5, no.1, pp.1633-1641, January 2017.