IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. IV (Jan – Feb. 2015), PP 65-71
www.iosrjournals.org

An Automated Model to Detect Fake Profiles and botnets in Online Social Networks Using Steganography Technique

Ehsan Ahmadizadeh[a], Erfan Aghasian[b,1],Hossein Pour Taheri[c], Roohollah Fallah Nejad[d]

[a]*Independent Researcher,Kuala Lampur, Malaysia*
[b]*Department of Electrical, Computer and Technology Information, Qazvin Branch, Islamic Azad University, Qazvin, Iran*
[c]*Takestan Branch, Islamic Azad University, Takestan, Iran, Lecturer*
[d]*Department of Computer Engineering, Islamic Azad University E-Campus*

Abstract: *At the present time, hundreds of millions of active users all around the world are using online social network, such as Facebook, Twitter, Tumblr and LinkedIn. This service turned out to be one of the most well-liked and accepted services on the Internet. With the quick development of information technology and networking, the users became able to share many things on the web such as pictures, videos, their daily activities, attended events and even their location. Nonetheless, the majorities of social networks have weak user to 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 cloning attack to form fake profile. Currently, Facebook has 955 million active users. Of this whole, approximately 8.7 percent (which is equal to 83 million users) is fake accounts. Fakes can introduce spam, manipulate online rating, or exploit knowledge extracted from the network. This enormous number of fake profiles can cause hazards for privacy and security such as spying, misusing personal information, identity thievery, and compromise privacy of users and their families. This paper will be discussing 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 labor-intensive.*

Keywords: *Fake book, Trust, Privacy, social Network, Steganography, Watermarking, botnets*

I. Introduction

Online social networks, such as Twitter and Facebook, 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 networks 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 [1-2]. Online social networks have already woven into the fabric of our online lifestyle, and this trend is expected to grow in popularity in the years ahead. At the same time there also exists a growing concern about fake users who can easily deceive themselves off as somebody 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 [1, 2]. Various fakes are created to upsurge the conspicuousness of niche content, fan pages and forum posts through manipulating votes or view counts [3, 4]. Moreover, Individuals create fake profiles for social motives. These comprise stalking, friendly pranks, cyberbullying, and concealing an actual identity to bypass real-life limitations. Likewise, many fake accounts are created for social online games [4].

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 networks have been reported [7, 8, 9, 10]. Fake accounts allow breeding scammers and would imposters attribute a serious security problem. Recently CNET report on August 1, 2012 indicated that Facebook has 8.7% fake users and this percentage estimates to 83.09 million accounts. Quoted from his speech in a press conference:

"When a person reports an account for this reason, we run an automated system against the reported account," he explained. "If the system determines that the account is suspicious, we show a notice to the account owner the next time he or she logs in warning the person that impersonating someone is a violation of

[1]Corresponding author. Tel.: +98-912-1827987
Email Address: erfanaghasian@gmail.com , aerfan2@live.utm.my

Facebook's policies and may even be a violation of local law. This notice also asks the person to confirm his or her identity as the true account owner within a specified period of time through one of several methods, including registering and confirming a mobile phone number. If the person can't do this or doesn't respond, the account is automatically disabled."

This security measure, however, relies upon detection and complaints made by users who are being impersonated; this implies to this matter that it may be often too late when the damage is already inflicted. Fundamentally the problem lies in the lack of preventive measure and the fact that the information used in registering a social network account is not verified at all. How we wish we could have an early alarm that alerts us whether a user who tried to add you as a friend on online social network indeed is suspicious or not. In other words, how do we know somebody on online social network who tries to be friend of you, possess a real identity of his or her, or one that is forged from somebody else?

Although most of 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 [11]. 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 by using other's information or picture and use social engineering techniques to steal information.

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 Facebook profile and user have set the 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.

II. Related Works

Three closely related fields are information hiding, watermarking and steganography that encompass a great deal of overlap and allocate several technical approaches. Steganography and Watermarking are renowned and broadly used to hide the original message. Steganography is used to embed message within another object known as a cover work, by properties tweaking. Digital watermarking is a technique for inserting the watermark information into an image that it may be visible or invisible [11]. On the other hand, there are numerous philosophical dissimilarities that have an effects on the necessities, and therefore in the design, and of a technical solution [13, 14]. By using such techniques and methods, confidentiality and authenticity of content would be kept. The figure below shows a steganography technique to protect the content from being detection or removal.

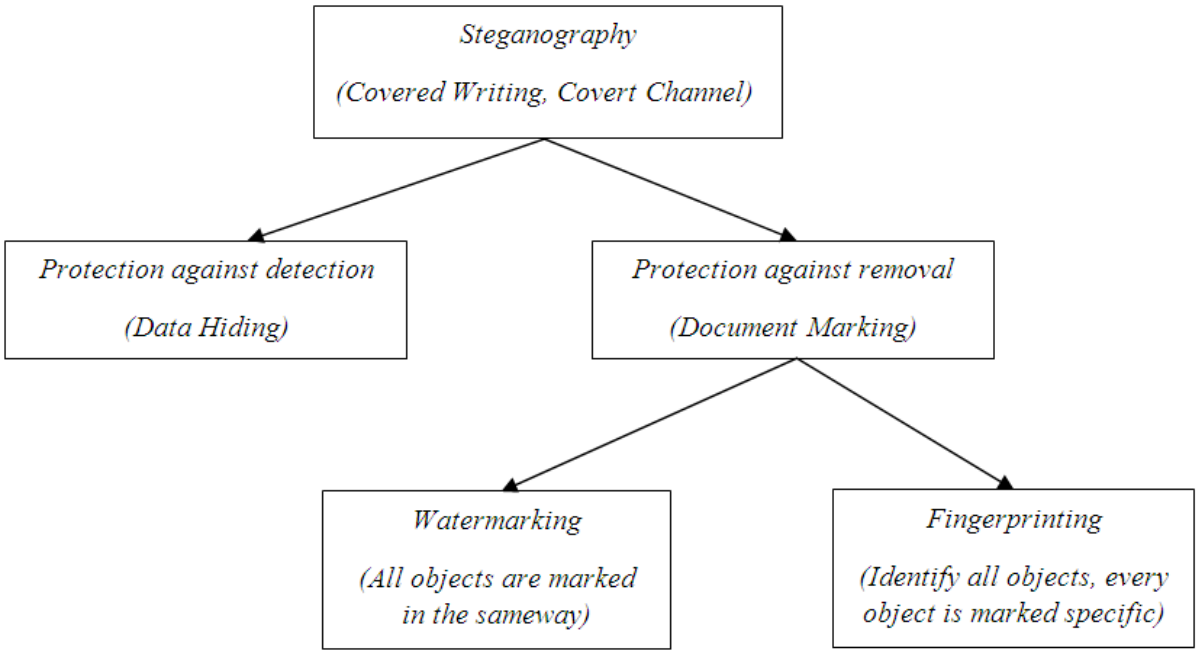

Figure 1: An Analysis of Steganography Techniques [15]

Watermark could be well thought-out to be some sort of information that is embedded into underlying data for localization, traitor tracing purpose, ownership proof and finally tamper detection [16]. On the other

hand, steganography is the science and art of communication in a manner that the existing message cannot be identified [17]. For doing such work, there are several steganography techniques such as technical steganography and Linguistic steganography [18]. Nonetheless, the techniques in steganography and watermarking are quite different but mixing these two techniques could afford an acceptable level of CIA for any user [17].

With the broad distribution of On-line Social Networks, the privacy and confidentiality of the users involved in such services is going to be a key distress. Numerous researchers proposed solutions to lessen the threats on confidentiality and privacy for those group obtaining profiles in online social networks previously (as an instance, count up more than 800 million for Facebook, one of the mainly well-liked online social network). As a case in point of such solutions for privacy-threat mitigation, Conti et.al planned the concept of Virtual Private Social Network (VPSN). VPSN fundamentally is a sign of the concept of Virtual Private Network (identified in computer networks) contained by online social networks: only friends surrounded by the VPSN are capable to observe the valid and actual information of an individual [19]. Other users in the online social network, as well as the online social network manager, do not have permission to access and observe the same information. The majority of the effort in the literature intended at preventing the information of the online social network in lack of awareness for unauthorized users, which mean to be accessed merely by the authorized users in the authorized way. For instance, Mahmood et.al showed how an attacker may obtain right of entry to the information that the victim distributes and shares in the profile, not in favor of the victim's wishes [20].

Despite the fact that the difficulty of protecting the privacy of the information has been well thought-out before now, authors believe that very modest consideration has been place in preventing the confidentiality of the user that may not make use of a specific online social network at all yet. Actually, an attacker or an adversary is eager to acquire confidential information of a victim and may run a "social engineering" sort of attack. As a paradigm, an attacker may form the profile of the victim, and after that attempt to find private information of the victim, whereas interacting with victim's actual friends linked to the fake profile. Authors would submit to this malicious action and behavior as a Fake Profile Attack.

Bilge et.al Mentioned and illustrate the possibility of mounting threat attacks on identity on online social network with two alternatives: single-site online social network and cross-sites online social networks. In the former case, the victim encompass a profile in the online social network where the attacker would form the profile which is clone [21]. In cross-site online social networks, the victim does not include a profile in the similar online social network where the attack is run; however, the profile of the victim is present in other online social networks. Jin et.al Showed a detection framework based on resemblances of the profiles: attribute and friends network likeness. They also mentioned that Facebook is well thought-out to be the online social network where the challenger runs the attack [22]. A like approach was used in Kontaxis et.al wherever they considered Twitter as the goal online social network [23].

In this research, authors highlighted and emphasized that the existing solutions for detecting and identifying Confidentiality, Integrity and Availability (CIA) for leveraging the assumption is that a profile of the victim is accessible in various online social network, which may not constantly be the case. Additionally, if the online social network in which the attack is run and it regard as a reference for resemblance which are not of the identical sort, authors expect the performances of the detection and identifying solutions to be lower, put side by side to the case when taking into account, for instance, the reference profile being in the same online social network as the cloned one. Jin et.al previously mentioned that their approach (measuring resemblances and similarities) is extremely definite to the existence of a unique and original profile where the victim has an existence in before now. Beyond doubt, while there is not any pre-existing profile, the comparison measurements and other method, techniques and routines for the exposure of CIA planned so far cannot be practical to FPA [22].

Lately, an additional issue and subject have been introduced; it concerns several identities in online social networks [24]. This issue is proposing a framework for grouping similar identities, which refer to the individual.

In this paper authors are going to focus on steganography methods and techniques and also watermarking techniques to bring more security and privacy for users in a new way.

III. Analysis and Proposed Solution

No matter what privacy and confidentiality selections the user has been set for his/her content or photos, still, there are hence numerous ways that specified information can be misused. At this time, 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. This indicates that anybody is capable of creating reports in opposition to someone else, still, numerous fake users report valid users. Only for the reason that so many users report him/her and also deficient in enough supports for the users, it can lead to termination of a real and legitimate user, and it is extremely hard and troublesome to get account back. In

case of social networks mostly bonnets are fake profile generators who produce spam and consume server's resources. As a case in point, recently, Facebook discovered botnet network called Lecpetexbotnet .this spam generator as most of the botnets distributed by social engineering methods. Facebook and most of social engineering websites discovered such a botnets by traffic analyzing and graph analyzing method which all are human monitoring method and not automatic [25]. This paper describes a watermarking based solution for detecting fake profile and botnet on social networks.

Profile picture are regularly the major representative factor for every user on social network websites and it can be misused in different ways similar to creating a fake profile devoid of any permission and acquire information by using it. 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.

As it has been shown in figure 2, when user A is uploading a picture to a social network similar to Facebook, it will be resized and alter to some standard extent. At the same time, steganography method can be utilize to conceal information attached to the picture, therefore, when user B saves that photo and strive to upload it under some other names; the system will automatically check the right and privilege of the user and ownership of uploaded file. Consequently, subsequent 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 B from re-uploading.

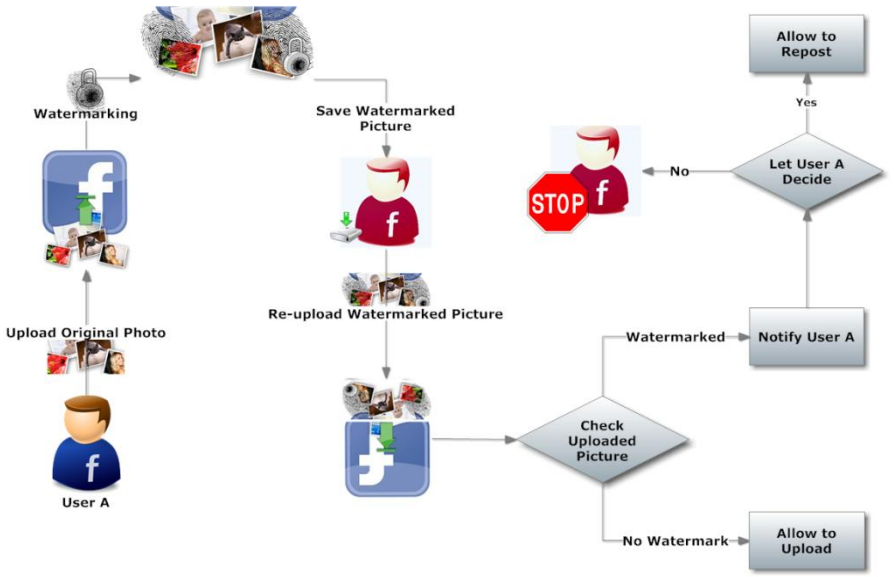

Figure 2. Proposed Model

However, it may not work if user B edits the picture and creates some changes after saving the watermarked image. As a case, if user B saves the watermarked picture of User A and crops some part of it, this method might not be able to detect the existence of watermarking anymore, means that user B is still able to re-upload and misuse it. In order to solve this matter, authors proposed a secondary solution besides watermarking procedures to detect and identify such users. Image search features such "Google search by image" is a practical method to discover precise or comparable images accessible on the internet which can assist to become aware of suspicious or fake users on social networks. This feature makes it feasible to look for giving images from side to side of billions of images uploaded to the Internet. Figure 3 shows a single picture has been used to generate several profiles. As highlighted in figure 3, each picture has dissimilar size which makes it unworkable to detect infringement by using watermarking method only.

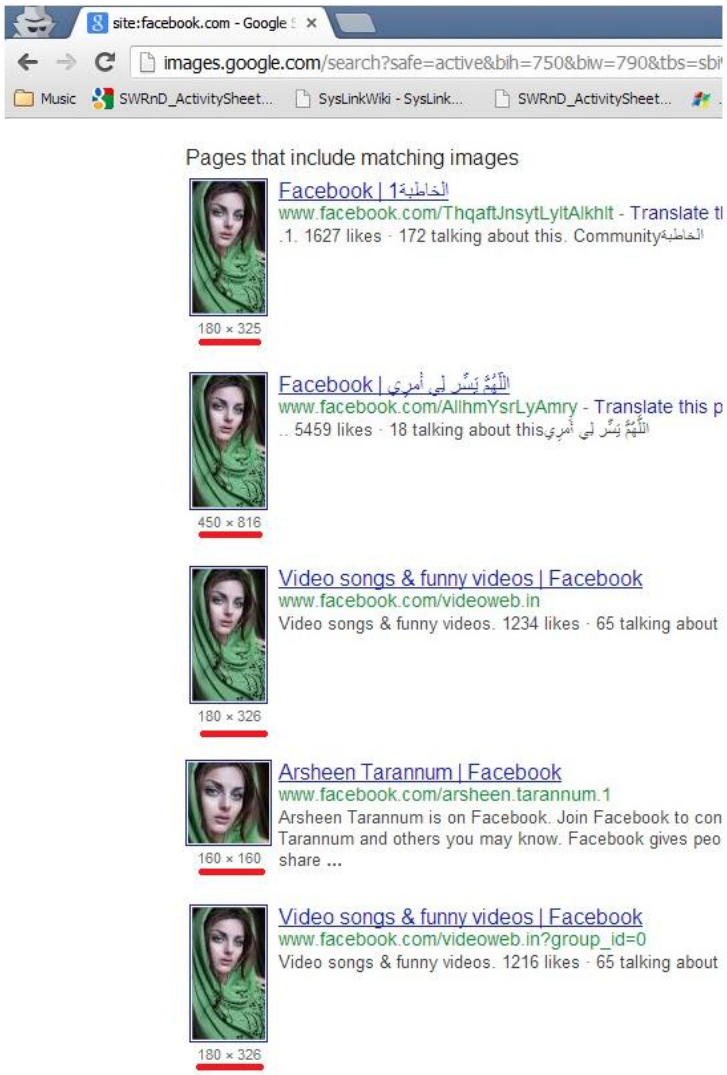

Figure 3. Several result returned from Google

As a result, authors can develop the proposed model in figure 2 by extending it. As figure 4 shows, the system is not only checking for existence of watermarking in uploaded file, however, furthermore, it will check the similarity match through billions of photo which is accessible on the internet. Thus, in case of finding several matches, User B will be asked to prove ownership rights for uploaded content and if he can't prove it, a warning message will be sent to keep away from future infringement, even it can lead to account termination of a repeat infringer.

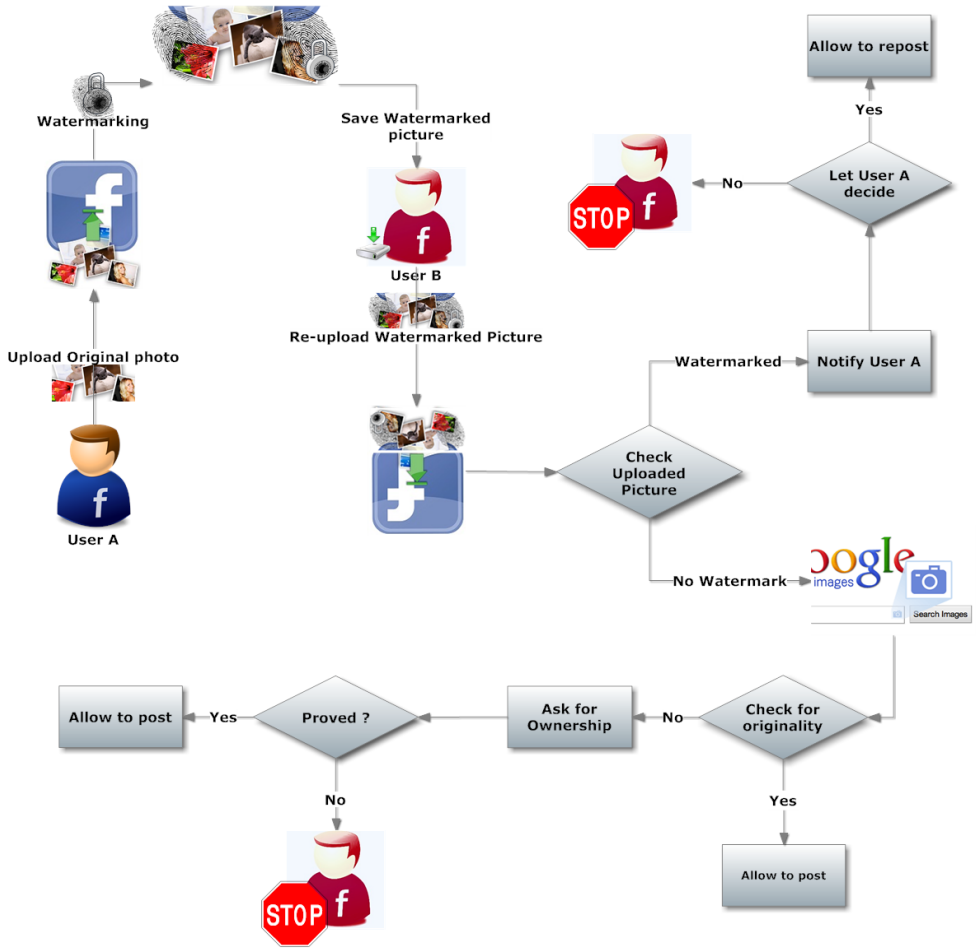

Figure 4. Proposed Model

IV. Conclusion

Nowadays, online social networks have become some of the most popular websites and services on the Internet, and usage is growing among users 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. By applying steganography techniques and watermarking to social networks, we can make them more secure and reliable. Moreover there is no requirement of redesigning the current social networks to implement this solution, so it would be easy to adopt.

Reference

[1]. Nielsen, Social Networks and Blogs, 4th Most Popular Online Activity, Nielsen Online Report, 2009.
[2]. Boyd, D and Ellison, NB, Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, 13, 2 (2007).
[3]. Stolen Facebook Accounts for Sale, http://tinyurl.com/25cngas,2010.
[4]. Personal communication with the Manager of User Support and the Product Manager of the Core and Community Management teams in Tuenti, 2011.
[5]. Fake Accounts in Facebook - How to Counter it, http://tinyurl.com/5w6un9u, 2010.
[6]. Why the Number of People Creating Fake Accounts and Using Second Identity on Facebook are Increasing, http://tinyurl.com/3uwq75x, 2010.
[7]. Guardian, Twitter Hoaxer Comes Clean And Says: I Did It To Expose Weak Media, Guardian, 2012.
[8]. Post, W, Twitter Hoaxer Tommaso De Benedetti Comes Clean, Washington Post, 2012.
[9]. Salon, the Fake Facebook Profile I Could Not Get Removed, Salon.com, 2012.
[10]. Roberts, S, Fake Facebook Friends - People Behaving Badly, Youtube, 2012.
[11]. Desai, V.H, Steganography, Cryptography, Watermarking: A Comparative Study, Journal of Global Research in Computer Science, Vol.3, No.12, Dec 2012.

[12]. Center, ITR, Facebook Social Media Survey 2012.
[13]. Cox, I, Miller, M, Bloom, J, Fridrich, J and Kalker, T, Digital Watermarking and Steganography, 2nd Edition, Morgan Kaufmann, 2007.
[14]. Cox, I,, Miller, M,, Bloom, J, and Miller, M, Digital Watermarking, Morgan Kaufmann, 2002.
[15]. Popa, R, an Analysis of Steganographic Techniques, The "Politechnica" University of Timisoara, 1998.
[16]. Agrawal, R,, Haas, PJ, and Kiernan, J, Watermarking Relational Data: Framework, Algorithms And Analysis, The VLDB Journal(2003), 13.
[17]. Kaur, G, and Kaur, K, Digital Watermarking and Other Data Hiding Techniques, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2, 5 (2013), 3.
[18]. Cummins, J, Diskin, P, Lau, S and Par-lett, R, Steganography and Digital Watermarking, The University of Birmingham, 2004.
[19]. Conti, M, Hasani, A and Crispo, B, Virtual Private Social Networks, Proceedings of the First ACM CODASPY (2011).
[20]. Mahmood, S, and Desmedt, Y, Your Facebook Deactivated Friend or A Cloaked Spy, In Proceedings of the Proceedings of the 4th IEEE International Workshop on SESOC (2012).
[21]. Bilge, L, Strufe, T, Balzarotti, D, Kirda, E, and Antipolis, S, All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks, In Proceedings of the International World Wide Web Conference Committee (IW3C2) (Madrid, 2009), IW3C2.
[22]. Jin, L, Takabi, H, and Joshi, JBD, Towards Active Detection Of Identity Clone Attacks On Online Social Networks, Proceedings of the first ACM CODASPY (2011), 10.
[23]. Kontaxis, G, Polakis, I, Ioannidis, S, and Markatos, EP, Detecting Social Network Profile Cloning, Proceedings of PerCom Workshop (2011), 6.
[24]. Gani, K, Hacid, H, and Skraba, R, Towards Multiple Identity Detection in Social Networks, In Proceedings of the Proceedings of the 21st international conference companion on World Wide Web (2012).
[25]. Faloutsos, M. Detecting Malware with Graph-Based Methods: Traffic Classification, Botnets, And Facebook Scams, WWW '13 Companion Proceedings of the 22nd international conference on World Wide Web companion, Pages 495-496 (2012)