International Journal of Engineering & Technology, 7 (2.33) (2018) 615-618

International Journal of Engineering & Technology

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

Research paper

Preventing malicious accounts based on mining with steganography in online

Ms. K. Karpaga Priyaa [1] *, Keerthipati Lahari [2], V. Vasundhara [2], C. Saranya [1]

[1] Assistant Professor, Dept. of CSE, Sri Sairam Engineering College
[2] Final Year CSE, Sri Sairam Engineering College
**Corresponding author E-mail: karpagapriyaa.cse@sairam.edu.in*

Abstract

On-line Social Networks (OSNs) are progressively exerting consequences on the way communication takes place among people through sites such as Twitter, Facebook, Google+ and LinkedIn, possessing millions of users. The Online Social Networks' (OSN) users face security-privacy threats such as Profile cloning, privacy breach and malware attacks. By these attacks, the fake user steals the virtual identity of the original user which they use to interact with other online users. To prevent these attacks, the proposed system uses Steganography which is the process of hiding information within other non-secret text or data. Our proposed system utilizes Steganography by implementing Watermarking technique which hides a secret text inside an image invisibly. Moreover the system avoids the leakage of personal information and prevents the creation of fake accounts. Experimental results show that the proposed technique can effectively detect and prevent creating malicious accounts in comparison with the techniques reported previously.

Keywords: *Fake accounts; Secret text; Steganography; Watermarking.*

1. Introduction

The online social networking provides networking for business, pleasure, and all points. Networks themselves have different purposes and their online equivalent work in various ways. Any social networking website permits people to communicate with their friends and acquaintances. The major concern in Online Social Networks (OSNs) is that how sharing and exchanging of private information happens through sites such as Facebook [8], LinkedIn [19] and Twitter [22] having millions of users across the globe. In Twitter, spamming occurs at a higher rate and spammers are detected based on the classification of spammers and non-spammers which is demonstrated in [1] and even URL redirect chains are detected using the results of [8], [18] and [13]. The accounts used by the spammers are identified in Twitter and around 15, 857 spam profiles were deleted [17]. Social networks are employed for personal use which allows the users to post a profile. Social phishing occurs mostly through email in order to capture personal information of users [10], [2]. To be a member of OSN, users should provide information like photo, date of birth, email id which creates a profile for the user. These profiles are basically, a list of information that users wish to share with their connections. Steganography based approach that hides the information within other non-secret text or data. Our proposed system uses steganography by implementing watermarking technique which hides a secret text inside an image invisibly and prevents the creation of fake profiles.

2. Background

The main focus of this paper is on using a simple, effective algorithm for the detection and prevention of the fake profiles. We describe some of the related works for fake profile detection in this section.

2.1. Detecting compromised accounts on social networks

For detecting cloned profiles, the existing system COMPA [6] was designed which used a mechanism to detect compromised accounts on social networks. This approach builds a Behavioral profile based on characteristics like time during which an account is active, message source, languages used for communicating, message, links in messages and proximity. The COMPA system identifies whether the profile of a user is cloned and moreover detects the presence of fake profile for any user.
Some of the drawbacks are:

- No identification of sudden behavior change of original user.
- Incorrect assumption as fake user.

2.2. URL spam filtering service

Thus the term "service", is tagged to the spam URL filtering. Both, Email spam and Twitter spammers have insight their properties in either ways. In addition, the distinguishable features such as generic redirectors' abuse, web hosting, and spam features overlap was explored between Twitter spam and email [24]. It provides smooth decisions that enable the services to remove individual post messages, while operates in a general way to different shapes of web services. The drawback is that the IP address of spam infrastructure achieves much less accuracy.

2.3. Toward worm detection in online social

To inspect the OSN sites, a few users are monitored by a heuristic algorithm obtained using the topological properties of social graphs [25]. The time to propagate from one user to another user's account can be reduced by a special property small average shortest path length. The affected user's account can be detected with greater accuracy by mitigating the noise that occurs in normal user communication. This noise reduction is achieved by the system through the application of a two-level correlation scheme. The disadvantage is that the detection system, adds a decoy friend into a normal user's friends list. Thus, the decoy friend of the infected user (whose account is affected by OSN worm), can inbox a worm evidence.

2.4. The underground on 140 characters or less

In order to view a friends message on twitter web page, it contains the enter details of who has sent and what they have sent etc., like the friends name, their icon, the tweet message, posting time, geolocation data and the application which they have used to post the tweet [9]. If a link is posted, these are the only available information with which they make decisions to click the link or not. The disadvantage is with only few spam URLs posted, the URLs might have unintentionally tweeted by account's owner as they are unaware about the URLs were spams.

2.5. Steganography algorithm to hide secret message inside an image

The drawback in present algorithms is that only simple access controls like password and login are being used. But once the person has logged into the system, he has the rights to use all the information that was hidden in an image with a secret key [24]. He will gain the access to use the secret key also once he login in to the system. So in order to overcome this, our novel stenography algorithm proposed many semantics that is, according to our algorithm, the entire information will be embedded inside an image and a secret key to access the information is also embedded inside the image. So, unless the person knows the secret key he cannot be able to access the information hidden inside the image [22]. This can ensure confidentiality and integrity of the message. Therefore the stenography algorithm shows the method of hiding these information and key inside the image.

3. Existing system

Most of the OSN users face privacy, security threats such as such as Profile cloning [25], and breach of privacy [13] Small number of users is monitored under surveillance using two level correlation schemes [19] which does not suit real world entities. As a user of an OSN, one should be aware that their profile has not been cloned by any unauthorized person. For identifying the cloned profiles, the existing system COMPA [6] was designed which used a mechanism to detect compromised accounts on social networks. This approach builds a Behavioral profile based on characteristics like time during which an account is active, message source, languages used for communicating, message, links in messages and proximity. The COMPA system identifies whether the profile of a user is cloned and moreover detects the presence of fake profile for any user. It is necessary to find the rare information by analyzing user's profile, to construct a behavioral profile. User activities on social networks are analyzed based on the study of social network based applications [15] with an instance of Facebook. This data will be specific to a user. The user details like their name, display picture, educational information, and work details are used in identifying the user. Each social network has the user profile with it which has similarity to legitimate profile.so two steps are involved here. Initially, comparison of original with searched profile record using honeypots [12]. Then a similarity index [24] will be calculated. Based on the similarity index, this system detects the presence of fake profile. But this detection might not identify the sudden behavior changes of the user. To overcome this issue, detection can be based on high level attributes like images instead of detecting based on user's characteristic which adds more security to personal information of users.

4. Proposed system

The COMPA system identifies the presence of fake profiles after its creation which leads to duplication of user's information. In the proposed system, a mechanism is used in which the user's information is not duplicated by preventing the creation of fake accounts and user's information is retained secured.
The proposed system uses a technique, Steganography [23] in which we add a secret text to the profile photos and posted pictures while uploading images. The uploaded image with the secret text and email id of the user gets recorded in a repository [3]. When another user downloads the original user's image, and tries to upload it in their profile, the notification alert is sent to the original user.

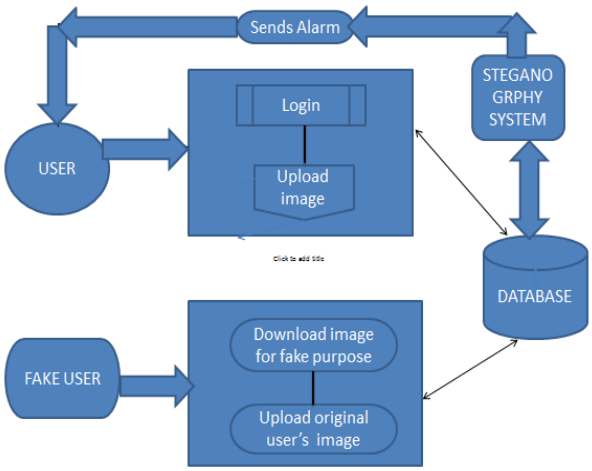

Fig. 1: Proposed System.

Here the block diagram encompasses the consecutives. First the user is validated before logging in. Then steganography algorithm is used to hide the secret text in images invisibly and checks whether the uploaded image has any secret text hidden inside, which implies the entry criteria. If this criterion fails, an alert message is sent to the original user.

4.1. Description of steganography algorithm

In order to enhance the security and confidentiality of data, watermarking technique is implemented. As a division of Watermarking techniques, Text watermarking is used with additional care since embedding of extra information into images should not affect its quality. Steganography and watermarking plays a major role in information hiding.
Algorithm for Watermarking:

1) Open Image:

This step will open the file and save header in a file and save the palette value of body in another file.

2) Split the body of the image file:

This step will split the body image in equal blocks to use these blocks in hide text.

3) Conversion:

- Text to ASCII code conversion
- ASCII code to binary code conversion

4) Encoding text into pixels:

Divided the stream binary code to parts every part 24 bit represent three character of text watermarking, and compare with pixels in palette of image.
The watermarking method is one of the copyright protection techniques for multimedia contents. Since multimedia has several

types of data like text, video, audio, image and graphics object each have a different technique/characteristics to hide the data inside them confidentially.so different watermarking techniques that are suitable for each type has to be designed and developed.
The algorithm defines that the secret text generated by the proposed system is transferred into text file and it is compressed into a zip file. The zipped file is then converted into binary codes. From the series, the final two consecutive codes are encoded as image pixel by using data hiding method. This process occurs until all binary codes are encoded. Once the text hiding into the image is done, the image is called steganography image. The hidden text can also be extracted again.
The Proposed System comprises of a list of modules in which each module is discussed later with its functionality regarding the prevention of creating fake profiles.

4.2. Login module

The Login Form module comprises of username and password text fields. In order to get access to the features in the site, the user must provide a correct username-password pair. The user will be logged out automatically if he/she is idle on the current page for certain time period.

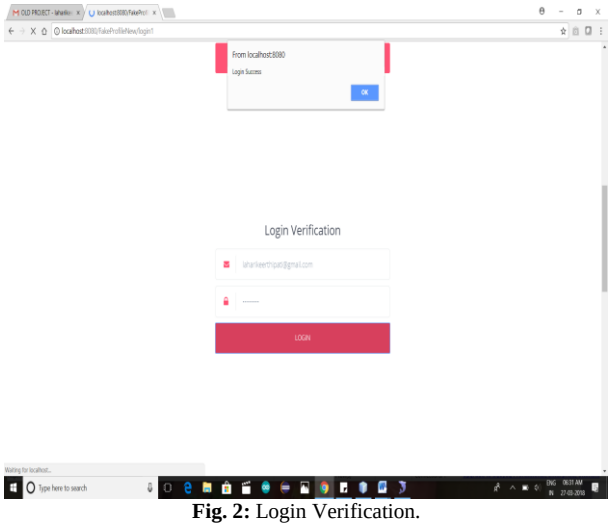

Fig. 2: Login Verification.

4.3. Hide data

In this module, it consists of a new steganography algorithm for hiding data in images. Here we have also used a Steganography algorithm. Hence this new steganography approach is robust and very efficient for hiding data in images.

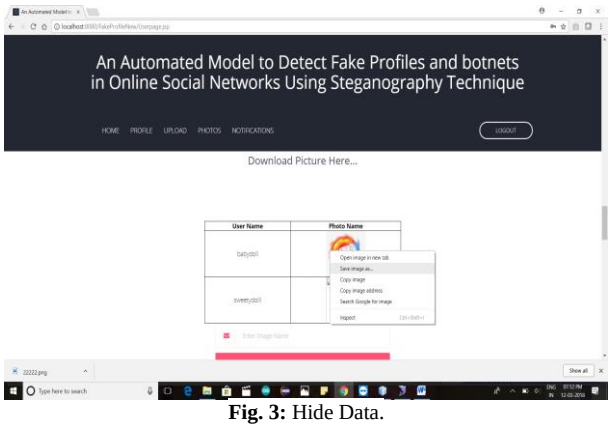

Fig. 3: Hide Data.

4.4. Profile matching

In Profile Matching module, if an another user downloads and upload the image, then internal entry criteria matching system checks for a primary match based on hard-coded whether some secret text is hided inside or not [12].

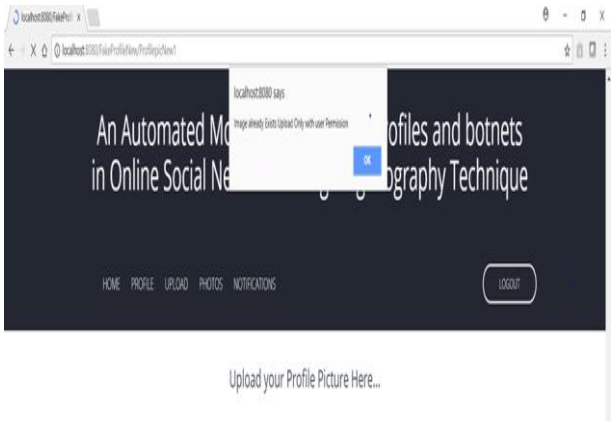

Fig. 4: Profile Matching.

4.5. Alerted profile

This module allows the user either to have multiple accounts for multiple purposes or to prevent the third users creating fake accounts.

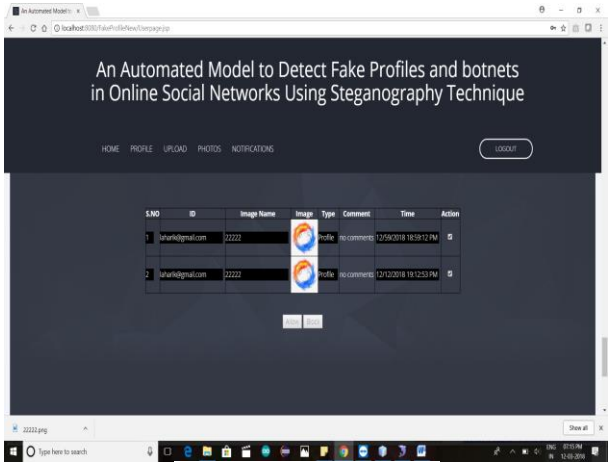

Fig. 5: Allow or Block Action.

The alert message comprises of two choices for the original user to decide upon. One is to allow which provides access to have more than one account to users. The other one is to block which avoids the third users in a way of not creating fake profiles.

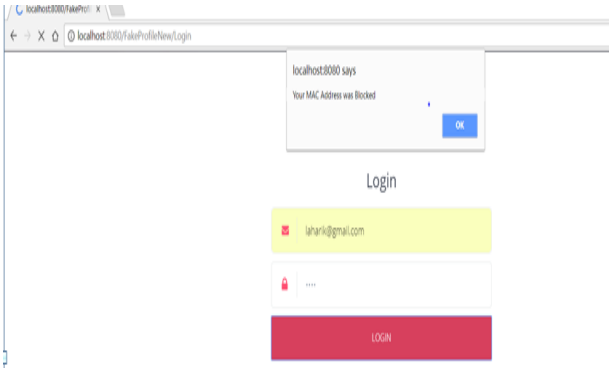

Fig. 5: Pop Up Blocking Fake User.

5. Conclusion

The system solves sudden behavioral changes occurred in use of behavioral profile in COMPA system. In this way, new images upload in our profile only after comparing images with the existing user profile and notification alert is sent in case of inception of

profile. In the end, we discussed the correlation between the number of registered profiles and the correctness of the user data and its impacts on the Face book business model. In this work, we also proposed a training method to increase user awareness as a valid countermeasure. In the future work, the system might work top-notch if user's details like date of birth, location, and more are simulated into an account irrespective of user's image leading to existence of fake profiles.

References

[1] Benevenuto, Fabricio, Gabriel Magno, Tiago Rodrigues, and Virgilio Almeida. "*Detecting spammers on twitter*." In *Collaboration, electronic messaging, anti-abuse and spam conference (CEAS)*, vol. 6, no. 2010, p. 12. 2010.

[2] Cormack, Gordon V. "Email spam filtering: A systematic review." *Foundations and Trends® in Information Retrieval* 1, no. 4 (2008): 335-455.

[3] Crandall, David J., Lars Backstrom, Daniel Huttenlocher, and Jon Kleinberg. "Mapping the world's photos." In *Proceedings of the 18th international conference on World Wide Web*, pp. 761-770. ACM, 2009.

[4] Dalvi, Nilesh, Pedro Domingos, Sumit Sanghai, and Deepak Verma. "Adversarial classification." In *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 99-108. ACM, 2004.

[5] David Ediger Karl Jiang, Courtney Corley Rob Farber, and William N. Reynolds. "Massive Social Network Analysis: Mining Twitter for Social Good" *in 39th International Conference on Parallel Processing*, 2010.

[6] Egele, Manuel, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. "Compa: Detecting compromised accounts on social networks." In *NDSS*. 2013.

[7] Felt, Adrienne, and David Evans. "Privacy protection for social networking APIs." *2008 Web 2.0 Security and Privacy (W2SP'08)* (2008).

[8] Facebook Statistics: http: //www.facebook.com/press/info.php?statistics.

[9] Grier, Chris, Kurt Thomas, Vern Paxson, and Michael Zhang. *"@ spam: the underground on 140 characters or less*." In *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 27-37. ACM, 2010.

[10] GAO, Hongyu, Yan Chen, Kathy Lee, Diana Palsetia, and Alok N. Choudhary. "Towards Online Spam Filtering in Social Networks." In *NDSS*, vol. 12, pp. 1-16. 2012.

[11] Georgios Kontaxis, Iasonas Polakis and Sotiris Ioannidis. "Detecting social network profile cloning" in *IEEE International Conference*, 2011.

[12] Heymann, Paul, Georgia Koutrika, and Hector Garcia-Molina. "Fighting spam on social web sites: A survey of approaches and future challenges." *IEEE Internet Computing* 11, no. 6 (2007).

[13] Huseyin Cavusoglu Ph.D, Huseyin Cavusoglu Ph.D, Srinivasan Raghunathan Ph.D. "*The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers"* in International Journal of Electronic Commerce, 2004.

[14] Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. "Social phishing." *Communications of the ACM* 50, no. 10 (2007): 94-100.

[15] Kreibich, Christian, and Jon Crowcroft. "Honeycomb: creating intrusion detection signatures using honeypots." *ACM SIGCOMM computer communication review* 34, no. 1 (2004): 51-56.

[16] Lee, Kyumin, James Caverlee, and Steve Webb. "Uncovering social spammers: social honeypots+ machine learning." In *Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval*, pp. 435-442. ACM, 2010.

[17] Lee, Sangho, and Jong Kim. "WarningBird: Detecting Suspicious URLs in Twitter Stream." In *NDSS*, vol. 12, pp. 1-13. 2012.

[18] [18]Lin, Yu-Ru, Hari Sundaram, Yun Chi, Junichi Tatemura, and Belle L. Tseng. "Splog detection using self-similarity analysis on blog temporal dynamics." In *Proceedings of the 3rd international workshop on Adversarial information retrieval on the web*, pp. 1-8. ACM, 2007.

[19] Linkedin: About us http://press.linkedin.com/about.

[20] Nazir, Atif, Saqib Raza, and Chen-Nee Chuah. "Unveiling facebook: a measurement study of social network based applications." In *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, pp. 43-56. ACM, 2008.

[21] Prince, Matthew B., Benjamin M. Dahl, Lee Holloway, Arthur M. Keller, and Eric Langheinrich. "Understanding How Spammers Steal Your E-Mail Address: An Analysis of the First Six Months of Data from Project Honey Pot." In *CEAS*. 2005.

[22] Stringhini, Gianluca, Christopher Kruegel, and Giovanni Vigna. "*Detecting spammers on social networks*." In *Proceedings of the 26th annual computer security applications conference*, pp. 1-9. ACM, 2010.

[23] Sumathi C.P , Santanam Tand Umamaheswari G. "A Study of Various Steganographic Techniques Used for Information Hiding" in *International Journal of Computer Science & Engineering Survey (IJCSES)*, December 2013.

[24] Thomas, Kurt, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song. "*Design and evaluation of a real-time url spam filtering service*." In *Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 447-462. IEEE, 2011.

[25] Xu, Wei, Fangfang Zhang, and Sencun Zhu. "*Toward worm detection in online social networks*." In *Proceedings of the 26th Annual Computer Security Applications Conference*, pp. 11-20. ACM, 2010.

[26] Yung-Shen Lin, Jung-Yi Jiang, and Shie-Jue Lee. "A Similarity Measure for Text Classification and Clustering" in *IEEE Transactions on Knowledge and Data Engineering*, July 2014.