Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

FAKE USER PROFILE DETECTION ON ONLINE SOCIAL NETWORKING.

Ideantificaiton of profile using Image Stegenography.

Chetan Bhagat, Prasanna Bhalerao, Avinash Godge, Harshwardhan Mane
Under guidance of Mrs. S.A.Ubale.

Computer Engineering, ZCOER, Narhe, Pune-411041.

Abstract —*Online Social Networking (OSN) service is a platform for all the users to share their information worldwide. The information can be in a form of images, audio, video, etc. User can share their personal data onto the social media. Many web sites provide a platform to connect the people through OSN media. OSN became extremely large and increasing day by day. Few websites allow user to create profile on their site and they can communicate with any random person. As user increases the security becomes a major constraint. Every user became aware about security issue as user shares his personal information on social media. A lot of fake users may capture this information and use it for the wrong purpose. There are thousands of fake profiles over social networks. Very little research has been done in detecting fake users over the social media. The research focuses on different components to detect the fake users. The components like login time-logout time, session, location, information uploading pattern etc.*

By getting the references from the above components we are developing the site which is able to detect the fake users.

Keywords*-social network, privacy, fake profile, Steganography and the Blowfish algorithm.*

INTRODUCTION

Social medial is a platform for all users to communication or share their personal information. Users can share their images, videos or any document over his profile. Online social network provides platform to easily interact with each other as the social network can increase widely, there are number of issues occurred related to security, privacy. As the user can share the images is may be or may not be confidential. With the increasing volume of images user shares through thousands of social sites, so there should be challenge to maintain the privacy and security of the image. For that we can have some tools or techniques to solve the problem. The image may be shared, upload, browsing through the large database of the image. Most of the common techniques are the metadata of the image such as captioning image. There are many concepts like image processing and Steganography etc. we use Steganography technique to identify the fake user profiles over the social network. In Steganography technique it can hide the secret message in the particular image means it can cover the data onto the image. So it can be unseen to user. The message in plain text can be converted to the cipher text and in invisible manner. In other words the Steganography can create image which can hide the secret message in the particular image.

EXISTING SYSTEM

Most of the data sharing web sites allow user to set their privacy preferences. But recent studies show that the user struggles to set up and maintain the privacy settings. The main reason behind the providing security is the secure the data or information transaction. There may have some essay way that must provide user to handle as well as learn though privacy setting. Sharing the images of online social networking sites, there may lead to privacy information. The online media can provide other users to share other user’s data. This shared data can be results from of unexpected exposure of one’s social environment and lead to abuse of one’s personal information.

PRAPOSED SYSTEM

We specially used the most effective algorithm blowfish to encrypt the message and dynamic LSB for hiding the message into cover image. Blowfish is a symmetric encryption algorithm, meaning is that it use the same secrete key to both encrypt and decrypt the messages. Blowfish is also block cipher ,means that it can divide the message into fixed length of blocks as well as it divides the image according to their size . and fill the n number of pixels according to the need. The block length of blowfish is also 64 bits. The blowfish algorithm has many advantages. It is suitable for hardware implementation and no license is required for it this algorithm is compact and it required less memory.

In this paper we propose the use of Steganography system which aims to provides the hassle free privacy settings experience by automatically generating personalized policies. The social context of the users, such as their profile information and relationships with the others may provide useful information regarding to user’s privacy preferences. For example, the user may share the its own images to any other user or upload his photo but can be seen by only his related persons. The Steganography techniques can be comparing the two images. And each image can contain some specific information .this information can be in hidden formats.

SYSTEM ARCHITCTURE

The main aim of Steganography are to hiding data onto particular image. It can work on some algorithms like DSS .the work of this technique is like first one user which can have their original image which can he uploads on online networking site using Steganography .In this technique the some pixels in the image can get some particular word on it. and this can in hidden formats so no one can see this particular message so each image can get some uniqueness. At the same time another user can download the same image for uploading on social networking site at that time when he can upload the same image his image can get some steganogryphic information which is also in the hidden form .By observing above both user image it can be essay to understand which is the original user and who is the fake, so the this technique is helpful for the detecting the fake user on an social networking site.

In our implementation we first encrypt the message using blowfish algorithm and convert it into cipher text. On the basis of this cipher text we calculate length and divides it into appropriate number of modules. These individual cipher modules then hide into the individual covers image using dynamic LSB method. For dynamic LSB method each covers image is passed over canny edge detection for smooth and edge portions separation.

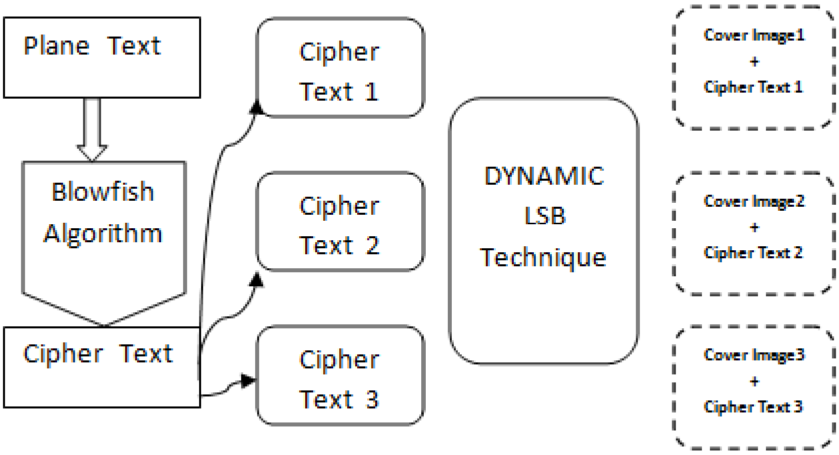

Figure3: Embedding Text into Cover Image

REFERANCES

[1] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[2] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee, “A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3-2008), Noida, India, August 7-9, 2008, pp. 105-114.

[3] Robert Krenn, “Steganography and steganalysis”, An Article, January 2004.

[4] Nedeljko Cvejic, Tapio Seppben “Increasing the capacity of LSB-based audio Steganography ” FIN- 90014 University of Oulu, Finland ,2002.

[5] Sajad Shirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speech steganography” ICASSP 2008

[6] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacks and Countermeasures”,Kluwer Academic Publishers, 2001