



New Technique to Protect the Privacy of Images in Social Network by Using Hash Algorithm & Least Significant Bit

Imad S. W. Khufash, Hebah H. O. Nasereddin

Faculty of Information Technology, Middle East University (MEU),
Amman, Jordan

Abstract— Generally, steganography is used to embed data into multimedia (images, audio or video), one of the used algorithm in steganography is the Least significant bit (LSB) .which sometimes can be detected by robbers, where this will affect privacy of the hidden data, thus, this paper will try to enhance the security of the embedding data by using LSB with secure hash function family (SHA).These two algorithm (SHA) and (LSB) -together- will be used to enhance the privacy of images in online social network (OSN) , The implemented technique includes two stages , hashing and embedding ; in hashing the (SHA) algorithm will encrypt signature of the user to obtain hash value , while embedding will embed the hash value into the image ,that's how the technique will guarantee that no signed images could be re-upload by other users .

Keywords— steganography; Least significant bit; robbers; secure hash algorithm; Online social network

I. INTRODUCTION

Online Social networks (OSNs) such as MySpace, Facebook, Cyworld, and Bebo have attracted a lot of users, many of users who have using these sites into their daily events , that offers various technological and support a wide range fields of interests and activities. [1].

Millions of users worldwide share, everyday, astronomical amounts of their private information through blogs, wikis, (OSNs), therefor, web communities, companies and governments try to provide more secure for the privacy field and adjust these services by taking the advantages of technological evolution in big data storage, cloud computing, semantic web, mobile services, which facilitates the design and development of new social web services. [2].

The technology provide to use the Internet as a best communication tool, user can transfer secret data over the Internet as part of the proper communication, but we cannot ignore the danger of hackers and snipers if the secret data are sent unshielded into the internet. [3].

The problem of authentication of published information and who can see and share it and the risk of the unwanted malicious users represent a real privacy problem for the user, (OSN)s try to manage users' privacy by using "privacy settings" for the services in many cases , but in fact a new violations ranging from identity theft up to personal information exposure are disclosed daily with the ease of re-uploading and re-publishing a user's images, without informing the real owner, this will harm the owner both social and economically. [2].

"The problem of ownership, should not be considered in terms of property or copyright, but it rather refers to the fundamental right to privacy", some users think that by uploading their own photos on (OSN) s, they can allowing access only to the users that they want, in fact the uploaded images are part of their privacy and users should be able to selectively introduce themselves to the others or not. [2].

The information can be have more secure by cryptography or by steganography , "the cryptography is aiming at the secret encoding of the information, while the information presence is obvious ,opposite to it, steganography is aiming at hiding the presence of the information". [4].

II. RELATED WORKS

The researcher suggested automated procedure that guarantees the copy right of Multimedia for users across multiple (OSN). (OSN) will not interact with any solution to protect the copy right of users Multimedia, because it is like any other company, that focus to have a bigger share in the market, rules and constraints will make customers to switch into other company. The idea of redesign all the (OSN) from scratch is bad idea but, all (OSN) should cooperate with each other to avoid the sniping of multimedia and protect the copy right of their users. (OSN) should avoid using external player like governmental rules. The solution is to invent an option for the users that can be used to protect his multimedia that he share on (OSN), that technique used a watermark with encryption algorithm on the multimedia, watermark later will be published on others (OSN) so that no one can Re-upload that content on any (OSN).[2].

The researcher Proposed new secure architecture to find an effective solution to reduce fake pages and possibility of recognizing VIP pages on (OSN) s by the logo method which appears inside the profile photo. It is limited to serve only the VIPs which have an effective website, apply this on Facebook, which are the most famous social-networking sites and also flexible to use a third party. Service on the FaceTrust will reports the number of fans who joined to VIPs pages that use the FaceTrust application. [5].

The researcher here proposed a secure tickets generator; using a secure hash function. Both sides Information Creator and Information Holder validate a ticket. The users with illegible tickets are allowed to access information. The Information Holders and Information Creator on both sides of the ticket validation process were configured to control access to different Information Creators and Information Holders. This prevented information leakage via authorized users [6].

The researcher implemented a privacy-preserving image-centric social discovery system to expand user’s friends with common interests securely, by deploying a system which use cloud as image storage back end. Design a secure and compact index to enable fast and scalable search over millions of user image profile, the evaluation demonstrates that the system is practical and efficient under huge image dataset with 1 million users. [7]

III. USED METHODOLOGY

This paper introduces new technique to protect the privacy of images in social network by using hash algorithm & (LSB). The new technique will use user signature which will be encrypted by hash algorithm, the encrypted signature value will be placed in the image according to its uploading time ,in case he want to apply privacy on his uploaded images.

In case of any re-uploading by others, the technique will stop and prevent the operation of re-uploading, the main steps of the new technique are demonstrated below:

1: registration and signature creation

1.1-User will fill-up his signature while registering, as shown in figure 1

The registration interface includes the following fields and instructions:

- Full Name:** Input field with instruction "Enter your first and last name" and a note "Your full name will appear on your public profile".
- Sex:** Radio buttons for "Female" (selected) and "Male".
- signature:** Input field with instruction "Pick a unique signature".
- Password:** Input field.
- Mobile Number (Optional):** Input field with a "+91" prefix and instruction "Ok".
- Email:** Input field with instruction "Enter your Email Address".

At the bottom, there is a checkbox for "I accept. Create my account." and a link to "Terms of Service". A note states: "By clicking on 'I accept' below you are agreeing to the Terms of Service".

Fig (1): registration interface

1.2- After registration, the user signature will be encrypted using SHA-2 (256 bit) algorithm, a fixed-length of 64 hexadecimal letters will be created.

Example: encrypt user signature where the signature is user1

0a041b9462caa4a31bac3567e0b6e6fd9100787db2ab433d96f6d178cabfce90

1.3- Both (original signature) and (fixed-length encrypted signature) will be store in the database. The flowchart below represent registration and signature creation step

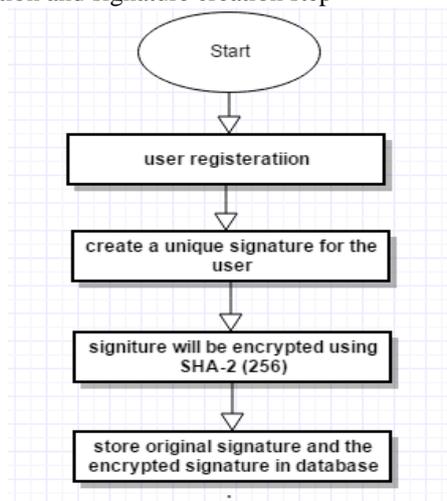


Fig (2): registration and signature creation step

2. Image uploading

Like any (OSN), the user can upload any image on his profile.

Date, time and encrypted signature are important inputs for image uploading, which will be discussed below.

While uploading; the image will be split into series of pixels (x columns and y rows), and the (date, time and encrypted signature) will be embedded into the image.

The flowchart below represent image uploading.

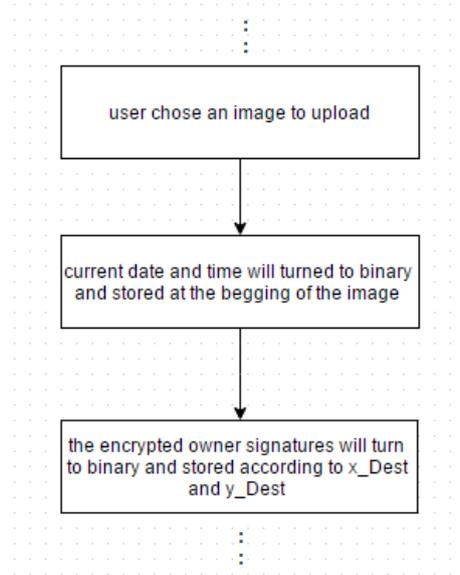


Fig (3): image uploading

2.1 -Date and time embedding:

The uploading date and time (of the image) will be transferred into binary formula.

Example: if the user uploads the image at 15/10/24; 23:17:03, the date and time will be transferred as follows
 15/10/24; 23:17:03=> 00001111 00001010 00011000 00010111 00010001 00000011

The technique will reserve the first 2-rows of the image to store the uploading time and date (of the image) using (LSB) which will be discuss later in details in 3.1 and 3.2.

2.2- Encrypted signature embedding:

Technique will embed the (fixed-length encrypted signature) which consist of 64 hexadecimal value, each value will be stored in separated line according to (x_Dest and y_Dest).

(x_Dest) determine the first used pixel in storing hash value as shown in figure 4.

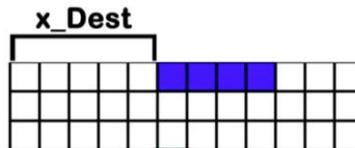


Fig (4): using x_Dest to determine the destination in x-axis.

While (y_Dest) determine the number of the unused rows between each 2 used rows (unused rows have no embedding values). As shown in figure 5.

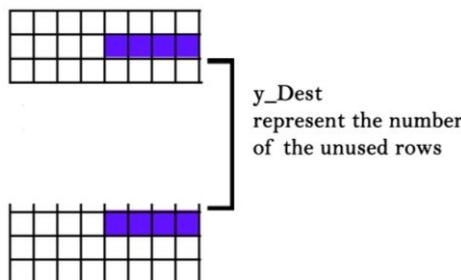


Fig (5): using y_Dest to determine the unused rows between each 2-used rows.

Both (x_Dest and y_Dest) will be stored in the database.

Section??? Will describe the generation of (x_Dest and y_Dest) in detail.

3. Other technique's for more secure:

3.1 Embedding into pixels

For both (date and time embedding) and (encrypted signature embedding), the technique will use only 1-bit from (red) channel for each chosen pixel, according to the following:

- If the sum of (location x and location y) of the pixel, is odd, the third (LSB) will be used.
- If the sum of (location x and location y) of the pixel, is even, the second (LSB) will be used.

Figure 6 show an example of the used technique

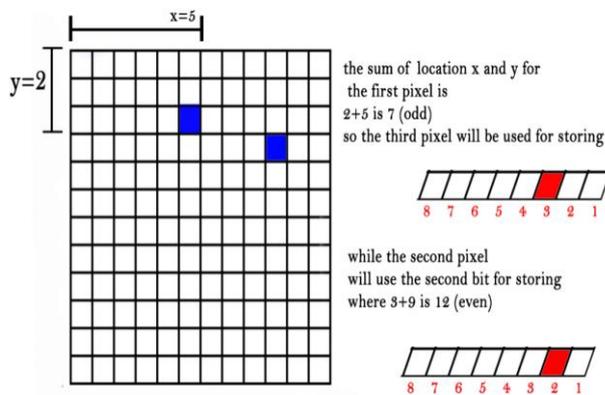


Fig (6) pixel embedding technique

3.2 (x_Dest and y_Dest) random generation

Every fixed amount of time (the technique used 3-hours interval, to reduce the load on server, this period could be minimized or maximized according to the server storage and performance) a new random (x_Dest) and (y_Dest) values will be generated , x_Dest , y_Dest and generation time will be store in database as shown in table 1

Table 1: x_Dest , y_Dest and generation time will be stored in database

| genTime | x_Dest | y_Dest |
|--------------------|--------|--------|
| 2015/9/28 15:25:00 | 54 | 5 |
| 2015/9/28 18:25:00 | 23 | 2 |
| 2015/9/28 21:25:00 | 276 | 7 |

While uploading, the technique will use the latest generated (x_Dest and y_Dest) values, these values will determine the destination of x and y for embedding data as described in section 2.2.

3.3 Reduce noise technique

This technique will try to reduce the possible noise of embedding dealt by steganography. Tables below show the reduction of noise after using “reduce noise technique”.

In case of placing 0 with 1 as shown in table 2 and 3

Table 2: cases of placing 0 with 1

| Original | After placing (Without modifying) | Noise degree | After placing (modifying) | Noise degree (modified) |
|----------|-----------------------------------|--------------|---------------------------|-------------------------|
| 000 | 100 | 4 | 100 | 4 |
| 001 | 101 | 4 | 100 | 3 |
| 010 | 110 | 4 | 100 | 2 |
| 011 | 111 | 4 | 100 | 1 |

Table 3: cases of placing 1 with 0

| Original | After placing (Without modifying) | Noise degree | After placing (modifying) | Noise degree (modified) |
|----------|-----------------------------------|--------------|---------------------------|-------------------------|
| 100 | 000 | 4 | 011 | 1 |
| 101 | 001 | 4 | 011 | 2 |
| 110 | 010 | 4 | 011 | 3 |
| 111 | 011 | 4 | 011 | 4 |

4. in case of re-uploading the embedding image (protected image)

If others try to re-upload the protected image, the new technique will do the following: While re-uploading , the technique will retrieve the first 64 pixels in the image, which represent the uploading date and time , a date format will be retrieved as follows (year / month / day , hour: minute: second) to use it to check the retrieved date and time from the database as show in Table 4 .

Table 4: retrieve x_Dest , y_Dest according to generation time from the database .

| genTime | x_Dest | y_Dest |
|--------------------|--------|--------|
| 2015/9/28 15:25:00 | 54 | 5 |
| 2015/9/28 18:25:00 | 23 | 2 |
| 2015/9/28 21:25:00 | 276 | 7 |

If the retrieved date and time are exist within any existing stored period, then (x_Dest and y_Dest) will be retrieved. By retrieving x_Dest and y_Dest, the map destination of the stored (encrypted signature) will be retrieved to create the hashed signature. If the retrieved encrypted signature exist in the database, the upload will fails, unless the signature is belong to the owner.



Fig (7): the technique will display a (privacy-warning) window in case of property violation

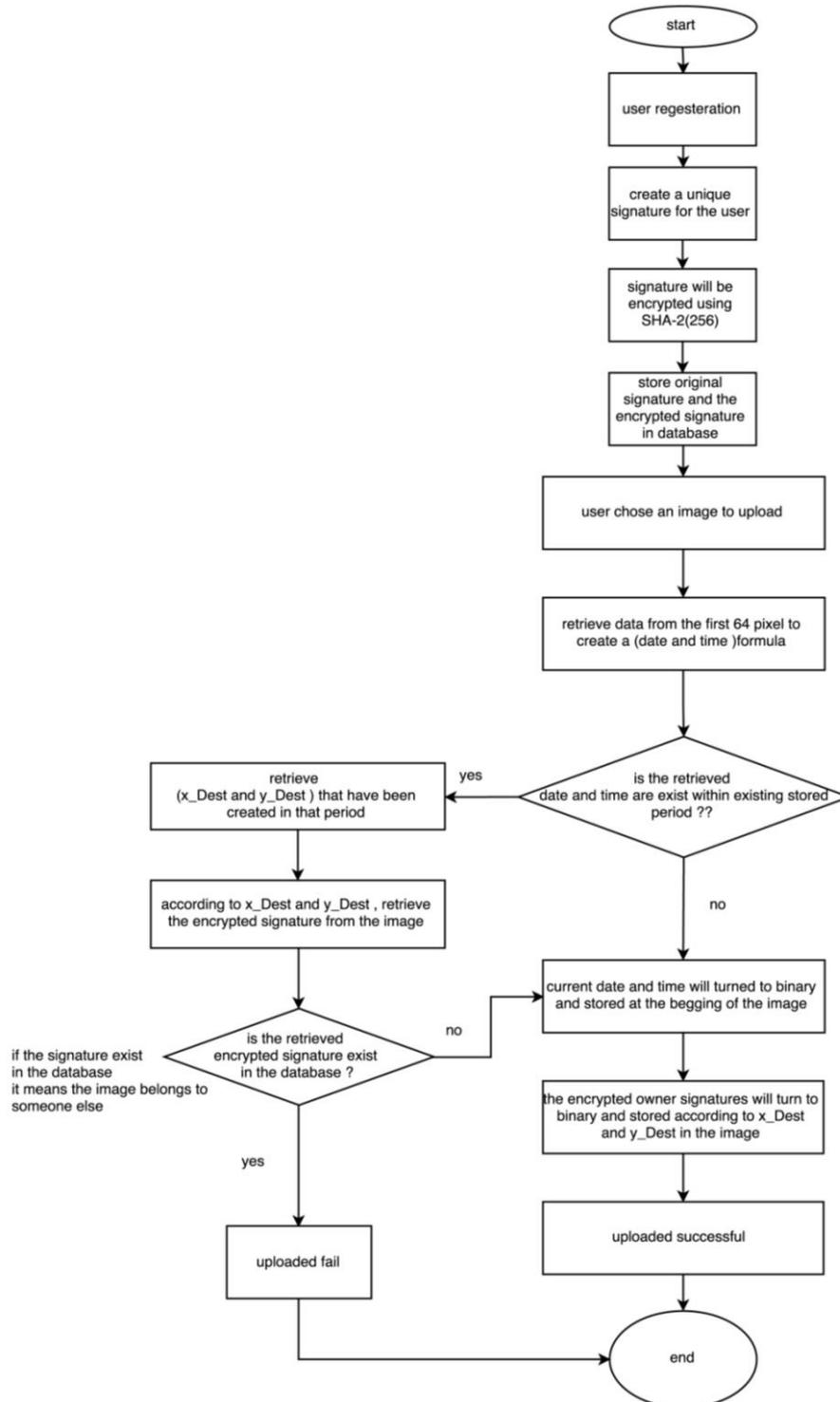


Fig (8) : technique flow-chart

IV. CONCLUSIONS

This paper introduces the development of an enhanced steganography technique based on using least significant bit and hash algorithm (SHA-2 256), the new technique is applied to implement in online social networks, using (ASP.net) or any other web development programming language.

Two main steps are used, i- registration and signature creation ii-image uploading and embedding, which will embed the uploading (date and time) and (encrypted signature) according to random values generated depending on uploading time, these values represent (X-axis destination and Y-axis destination), random values will determine the destination of pixels that include the encrypted signature, the technique will check any uploaded images, if the retrieved signature exists in the database, uploading will fail.

REFERENCES

- [1] Boyd, D., & Ellison, N. (2007). "Social Network Sites: Definition, History, and Scholarship". *Journal of Computer-Mediated Communication*, 210-230.
- [2] Patsakis, C., Zigomitos, A., Papageorgiou, A., & Galván-López, E. (2014). "Distributing Privacy Policies Over Multimedia Content Across Multiple Online Social Networks". *Computer Networks*.
- [3] Niimi, M., Noda, H., & Kawaguchi, E. (1999). "Steganography Based on Region Segmentation with a Complexity Measure". *Systems and Computers in Japan*.
- [4] Por, L., & Delina, B. (2008). "Information Hiding: A New Approach in Text Steganography". *Advances on Applied Computer and Applied Computational Science*, 685-695.
- [5] Shilbayeh, N., Khuffash, S., Allymoun, M., & Al-Saidi, R. (2014). "Protecting the Privacy and Trust of VIP Users on Social Network Sites". *World Academy of Science*, 1488-1498.
- [6] Jang, Y., & Kwak, J. (2013). "Access-control-based Efficient Privacy Protection Method for Social Networking Services". *International Journal of Security and Its Applications*.
- [7] Yuan, X., Wang, X., Wang, C., Squicciarini, A., & Ren, K. (2014). "Enabling Privacy-preserving Image-centric Social Discovery". *IEEE 34th International Conference on Distributed Computing Systems*, 198-207.