Pictographic steganography based on social networking websites

Feno Heriniaina R.[1], Xiaofeng Liao[2]

[1]College of Computer Science, Chongqing University
Chongqing, 400044, China
fenoheriniaina@cqu.edu.cn

[2] College of Computer Science, Chongqing University
Chongqing, 400044, China
xfliao@cqu.edu.cn

Abstract

Steganography is the art of communication that does not let a third party know that the communication channel exists. It has always been influenced by the way people communicate and with the explosion of social networking websites, it is likely that these will be used as channels to cover the very existence of communication between different entities. In this paper, we present a new effective pictographic steganographic channel. We make use of the huge amount of photos available online as communication channels. We are exploiting the ubiquitousness of those social networking platforms to propel a powerful and pragmatic protocol. Our novel scheme exploiting social networking websites is robust against active and malicious.

Keywords: *Information hiding, steganography, online social networking, pictogram*

1. Introduction

The art of covered writing or steganography has a long history and has always been influenced by the way people communicate. It is often understood as the prisoners` problem where two inmates Alice and Bob, imprisoned in two different cells are trying to formulate a plan for escape. The only way to communicate with each other is through a channel that is monitored by the Warden. Alice and Bob should then find a way for communicating under monitoring without raising the Warden`s suspicion. The expansion of the virtual world has created a wide range of possibilities in the world of secret communication. Although, cryptography is enough to keep the content of a given information unreadable from praying eyes. If the Warden (also referred as person in the middle) who monitors the communication is not favorable to encrypted data, and whenever he knows that something encrypted and suspicious is within the channel, he might decide to stop and interrupt the communication (Fig. 1). Given such situation, the communicating parties should rather use steganography to make the very existence of the message transmission unnoticed.

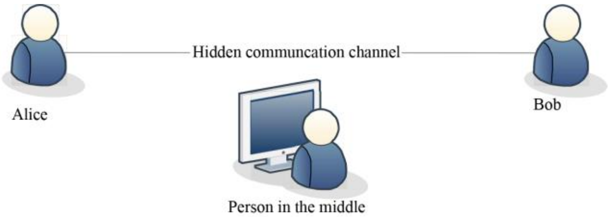

Fig. 1. Hidden communication channel between two entities (Alice and Bob) with the presence of a warden (the person in the middle).

Steganography has been recorded in the literature since the 1953 [1-2] and has evolved a lot to adapt into the 21st century. There are different types of technical steganography: text, audio, images and video [3] and among the most commonly used and studied to date are all based on images.

This is no big surprise because of the huge amount of photos already available online and the new uploads generated by social networks and photo services users. Publishing and sharing images online have now become very easy. Yet the trend in enhancing the image quality and in making the process of high quality content creation much simpler is not stopping, as almost all mobile phone manufacturers are now trying to provide a good embedded camera as a main component of their products. Above all that, higher and better computation resources are available on most mobile handheld devices nowadays, and steganography based on images would be more promising than ever.

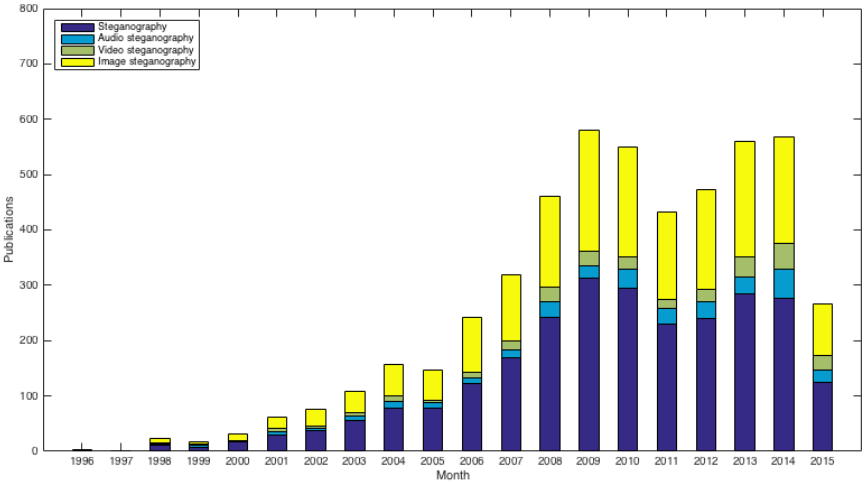

Fig. 2. Growth of the field of steganography witnessed by the number of articles annually published by IEEE that contains the keywords "steganography", "audio steganography", "video steganography", and "image steganography".

Many techniques and research papers about image-based steganography have been made available to the public to date. A simple search query with the key words "image steganography" at ieeexplore.ieee.org, combining journals and conference research papers from 1996 to 2015 gave a total number of 1855 in September 2015. A comparison using other search keywords related to steganography is represented in the figure 2. In term of digital image steganography, many are based on the exploitation of the least significant bits embedding as this is one of the easiest to implement [4] and the identification and replacements of the redundant bits [5]. Almost all these methods recorded in the literature focused on how to hide enough information within an image because an image consists of a large number of individual pixels that can be imperceptibily modified to encode a secret message. But the transmission of a single stego-image would require a great covering technique to go unnoticed from a warden that could apply steganalysis [6], it is important that the produced stego image has no drastic change in the image spectrum in order to preserve the quality as similar to the cover image as possible [7]. Nowadays, sharing photos and other digital media is part of our daily life. The intense use of social networking websites and the millions of photos uploaded everyday have opened new opportunities to an old communication technique to meet the digital world. So far, no one to the best of our knowledge has presented a digital image steganographic method that is leaving the cover image untouched to vehiculate a secret message and respect the most important property of steganography, i.e: undetectability.

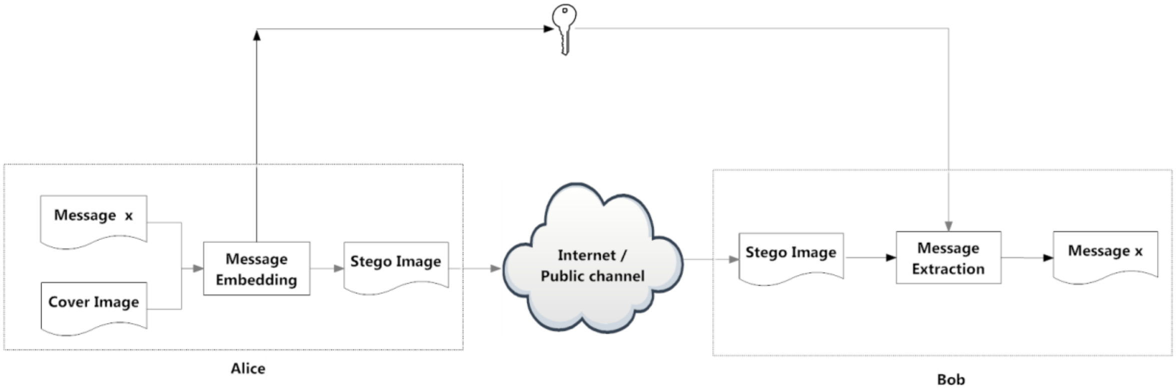

Fig. 3. General summary of image steganography

In the remaining of this paper, we will introduce a pictographic steganography scheme using online social networking with Facebook as our case study. In section 2 we provide an overview on the social networking mechanism. In section 3 we review the current work related to image steganography. Section 4 introduces our image steganography using pictograms. In section 5 we provide a security analysis of the proposed protocol. Section 6 is a study on the performance of the presented pictographic protocol. In section 7 we summarized the main advantages of the proposed steganographic system. The last section 9 is devoted for the discussion and conclusion.

2. Social networking system: creation, utilization and notification.

Online social networking has drastically changed the way Internet users interact with one another. One main characteristics of social networking sites is the free user registration, the user generated content, sharing and collaboration, and the convergence of intelligence.

Facebook (https://facebook.com) is one of the internationally used online social networking websites. Despite its restrictions in some areas, Facebook has users in almost all parts of the globe ranging from the economically poorest to the richest countries. Creating a personal account on Facebook is totally free and a registered user can upload images, post contents and connect to any other Facebook users without physical border limitation. Facebook users can set the security settings of their accounts based on their preferred privacy requirements [8]. This will define the users` account visibility to other Facebook users and the general Internet users. Given a working Facebook personal account, one can create a Facebook page and post in some news, stories and other updates targeting some specific people. Those could click on the “Like” button and become followers of the page which is also referred as a Facebook page in this paper. Following a page will allow them to receive instant notifications each time there is an update.

Using Facebook as a case study for our communication channel between Alice and Bob located in different places, we present the following stego-system to allow them communicate without anyone knowing the existence of the used communication channel. For the scheme to be effective, both Alice and Bob should know the communication protocol prior the real communication using the presented stego-system. They should also know how to read the images, which we will introduce later, as only in knowing how to read the image will one be able to retrieve the secret message.

3. A review of image steganography

Embedding and extracting algorithm are the techniques through which the secret messages are embedded and extracted. Being an important part of a steganography system, there are three fundamental ways that determine its internal mechanism, i.e: cover synthesis, cover selection and cover modification.

- Steganography by cover synthesis: a cover is generated for the sole purpose of concealing a secret message.
- Steganography by cover selection: from a set of data, a cover that conceals best the conveyance of the secret information is chosen.
- Steganography by cover modification: regular data is changed or substituted with the secret information. Depending on the type of cover and the amount of hidden data, the substitution method can degrade the quality of the original cover drastically.

The latter is the most extensively studied steganography model to date [9-12]. Many of the released steganography techniques are based on the least significant bits replacement and / or matching [13-14]. Some are a combination of cover selection and modification [15-17]. Such steganography techniques involve the modification of the cover image to produce the stego-image [14]. In general, the steganography techniques based on images released to date are embedding the message into the cover in order to get the stego-file. The extraction of the hidden message is later feasible for those who know the extraction algorithm and have access to the key (Fig 3).

In this era of the digital world, the Internet is generally the public channel used for transmitting the message in stego format from Alice to Bob. However, there could exist a third party observer in this public channel. A pure steganography scheme will make an assumption that the third party observer also known as the warden does not have any idea of the embedding and decoding algorithm. Robustness then is referred as the difficulty of removing the hidden information from the stego object. While removal of secret data might not be a much serious problem as its detection, robustness is a desirable propriety when the communication channel is distorted by random errors or by systematic interference with the aim to prevent the use of steganography [18]. The warden can also interfere between the communicating parties. Based on its involvement, we assume three different roles for the warden: a passive warden, an active warden and a malicious warden [10, 18].

Usually, a passive warden simply examines the message and tries to determine if it potentially contains a hidden message. The warden has read only access to the message being sent. If he suspects the existence of a secret message, then the document is stopped. Otherwise it will go through without any further inspection [18].

But an active warden and a malicious warden are often times merged into one. An active warden refers to a third party that attempts to disrupt the steganographic channel by modifying the message. In case of an image file to be transferred, the warden might try to compress or resize the file. Under such condition, any steganographic scheme would be broken unless it is robust to such processing. A malicious warden does not necessarily intend to entirely disrupt the stego channel, but rather uses it to determine whether or not steganography is taking place [10, 19].

Finally, embedding information on photos uploaded on most social networking websites is tough as different processing such as compression is made before having the photos available worldwide, in this paper we introduce this steganographic scheme using pictograms which is resistant to both compression and cropping as long as the main content of the image remains visible.

4. Image steganography using pictograms:

The proposed scheme has three main steps: converting the message into pictogram, uploading the images and from the receiver side only reading the pictogram is required.

4.1 Converting a text into pictogram:

Both Alice and Bob should know how to read the pictogram images and only their creativity is the limit on how to represent things using images. The example below presents a sample of a word conversion into an image.

P denotes a finite set of possible plain text,
I denotes a finite set of images, y is each photo $\in I$,
Enc is the encoding rule,
Dec is the decoding rule,
Each $\mathrm{Enc} : \mathrm{P} \to \mathrm{I}$ and $\mathrm{Dec} : \mathrm{I} \to \mathrm{P}$ are functions such that $\mathrm{Dec}(\mathrm{Enc}\,(\mathrm{x})) = x$ for every word element $x \in P$.

Example:

$$Enc(car) = y_{photo\ of\ a\ car} \qquad (2)$$

$$Enc(love) = y_{photo\ of\ a\ heart} \qquad (3)$$

$$Enc(money) = y_{photo\ of\ a\ bank\ note} \qquad (4)$$

In the above example, we chose a straightforward encoding from a word to an image representative of its meaning. Instead of directly $Enc: P \to I$, an additional substitution could precede this step giving a rather uncorrelated meaning to the encoding output. A shifting method based on the ordering or location of the words in a chosen dictionary is proposed as presented in figure 3. The key for the encryption and decryption of the image (message) is the combination of the shift cipher and the selected dictionary.

The structure of the dictionary can be considered like one of those empirical hardcopy books mainly used in the year nineties; such an example is the Oxford dictionary 2nd edition. It will be used to locate the exact position of the word derived from the image pictogram. The shift cipher is used for the mapping of the plain word to its cover (encrypted version).

For a correct shift mapping, a word should first be located in the chosen dictionary. For a shifting based on the location of the words in the dictionary, the exact position of the word on the page will be localized. The shift number will be used to map this exact position on the corresponding page-shift; which is the page number of the word location added with the shift number and then modulo n. n is the total page number of the dictionary and $\mathbb{Z}_n$ forms the arithmetic modulo n of set $\{0, \dots, n\text{-}1\}$.

S denotes a finite set of possible shift cipher. For each $s \in S$ there is an encryption rule $e_s \in E$ and a corresponding decryption rule $d_s \in D$,

$$e_s: P \to I \text{ and } d_s: I \to P,$$

are functions such that $d_s\big(e_s(x)\big) = x.$ (1)

Additionally, because each event is dated on most social networking websites, including our case study Facebook, the date of upload could be used as mask to be added to the shift cipher each time an image needs to be uploaded.

Combining the encoding-encrypting parts above, we have Enc $\big(e_s(x)\big)$ and the decoding-decrypting is $d_s(Dec(y))$.

4.2 Uploading the images in a manner that facilitates the reading

When uploading a batch of images on Facebook, by default the ordering is done according to the image file name in the local machine with the assumption that the arrangement is also set based on that. Each update given to a Facebook page has to have a time stamp when published and the availability to the public is based on the first uploaded first visible. Let us assume Alice would like to send the message “money loves car” to Bob. M be the message and x_i each word that makes it. The number of images to upload to transcribe the message M is i and it is the same as the number of $x_i$needed to be uploaded. After a minute selection of the images representatives of the message to be sent, if the image-upload is done in a batch, Alice should rename the images based on how the ordering of the reading should be done. In the previous example, were $M = x_1 + x_2 + x_3$, the name of the images to upload together in one batch should be organized so that

the image to be viewed first has the smallest name number. If Alice chooses to use a name with numbers, it should look something like: IMG_1, IMG_2 and IMG_3.
Doing so will permit the correct reading of the message transmitted in a general manner such that:

$$\mathrm{Dec}(y_1)+\mathrm{Dec}(y_2)+\cdots+\mathrm{Dec}(y_n)=x_1+x_2+\cdots+x_n \quad (5)$$

4.3 Reading the pictogram

In the next section, we introduce two protocols that can be used for this proposed steganography using pictograms on Facebook. The way for retrieving and reading the message will vary based on the chosen protocol. A summary of the two protocols are presented in the table below:

Table 1: the protocols for knowing whether a new message has been made available

Protocol One	Protocol Two
Alice has a Facebook account.	Alice has a Facebook account.
Bob has a Facebook account.	-
Alice creates a Facebook page.	Alice creates a Facebook page.
Bob follows (likes) Alice`s Facebook page.	Bob knows the links to Alice`s Facebook page.
Each time Alice posts something on her page, Bob should receive a notification.	Bob has to check periodically Alice`s Facebook to find out whether new posts have been published.

If Alice and Bob chose to use the proposed protocol one, both Alice and Bob should have a Facebook account. Alice will need to create a Facebook page and Bob should follow her page. Each time Alice makes an update (writing a post or uploading a photo) on her Facebook page, Bob should instantly get a notification information. This notification is the trigger for Bob to view what was the update about and to reconstruct the message if some pictographic images were uploaded.

In the case the protocol two is selected, only Alice needs to have a Facebook account and to create a Facebook page. Bob should visit Alice`s page periodically and see whether or not some updates that cover-up a message were uploaded. Although this method seems lacking the notification system to inform Bob, it has the advantage of strengthening the proposed steganographic system due to the absence of direct connection between Alice and Bob.

5. The proposed protocols

We introduce and analyze two schemes from which we compare based on how they preserve discretion. Prior to the establishment of communication, both Alice and Bob should already have access to the shift cipher and the dictionary. The difference between the schemes proposed is in the way Bob gets to know whether a new message has been released.

Protocol One: Both Alice and Bob should each own a Facebook personal account. Alice will create a public Facebook page where she can upload photos. Being a Facebook user, Bob would follow Alice by liking her Facebook page. When Bob starts following Alice`s page, he will be notified each time the page gets updated and he should just visit and check what was updated to reconstruct the message if something was sent. For this given protocol channel, what matters most is the photos that are uploaded on Alice`s Facebook page as they drive the information. It is important that Bob is able to view the photos in a timely and arranged manner.

Protocol two: Alice should own a Facebook personal account and create a public Facebook page where she could upload photos. The photos uploaded being the main message in the form of pictogram, Bob only needs to know the url address to Alice`s page, and needs to visit the given page in a timely manner. All posts in Facebook and including Facebook pages are time stamped, and knowing the ordering of the image uploaded will allow Bob to reconstruct the complete correct message by viewing the images in order.

6. Security of the proposed steganographic system

Our main focus while referring to steganography is to provide a secure channel where a successful attack would consist of a warden being able to identify that a given image uploaded on the network drives a hidden message to the viewer. Law enforcements and intelligence agencies have always been having difficulties deciding which electronic channel to scan and intercept because of the huge volume of traffic [20].
The use of social networking website will just increase the level of this difficulty as the amount of photos being uploaded on those online photo sharing, and social networking websites every day is exceeding 2 terabytes with a peak of 300 000 images served per second in 2008 [21]. Also, although we are using images to drive the message from Alice to Bob, we don`t introduce any additional artifact to those images. The well-known and standard steganalysis algorithms: regular and singular group analysis [22], sample pair analysis [23] and difference in the images histograms [24], are not applicable to our scheme as we are not introducing any artifacts in the core of the images. Relying on the cover channel undetectability, using a popular Facebook page as a network cover channel should not create any suspicions and strengthen the hiddenness of the proposed steganography system.

To improve the complexity of the decoding of the image (reading of the pictogram), further scrambling the ordering of the display of the images in one Facebook page album could be achieved by first uploading the photos in a batch in the correct reading order and then later changing the upload time and dates by editing each image description. Supposing a warden has access to all the pictures that make the complete message and has the correct dictionary allowing $\mathrm{Dec}\big(\mathrm{Enc}\ (\mathrm{x})\big) = x$. It is still required that the correct ordering of the image be found too, to properly make sense of all the images. In this case, only one arrangement out of n- permutations of the images which make the complete message will correspond to the correct message. So if we have the image set $E(y_1, \dots, y_n)$ that makes the message $x_1, \dots, x_n$, then we have :

$$p(n,k) = \frac{n!}{(n\text{-}k)!}, \tag{6}$$

$$with\ k = n, \tag{7}$$

$$p(n,k) = \frac{n!}{0!} = n! \tag{8}$$

With n images to make the complete message and $n!$ possible permutations, the longer the message is the better its security on an exhaustive search becomes.

If we considered that a robust steganographic approach should define its security based on the chosen secret key as presented in “La cryptographie militaire” In other words, if we assume that the protocol in use is known to a warden, and so the security must lie on the choice of the secret key (shift cipher for the encryption/decryption and the dictionary for encoding/decoding word to image) that Alice and Bob have managed to share based on Kerckhoffs principle [25]. An additional step for implementing a one-time dictionary would be a good the remedy.

For this scheme to be most effective, we consider the worst case of a warden that could intervene as soon as a known communication channel is suspected to exist between Alice and Bob. Considering our case study, the platform and service provider is at the highest level in knowing whether a direct relationship exists between Alice and Bob. With the stegosystem depending on Facebook, it could be very easy for them to analyze users`log data containing information about browsing habits [26].

When creating a Page, we are giving Facebook information about our interests. For the proposed method one, where Bob should like Alice`s page in order to instantly get notification each time Alice has some updates, a direct connection has to be established. Unlike some users who tend to feed their online profile with a tone of information that aim at providing a complete and accurate representation of themselves; in the proposed stegosystem, avoiding direct connection between Alice and Bod is a must in order to increase the degree of separation.

The proposed protocol one does require a connection between Alice and Bob with this later needing to like the Page. But, the method two does not necessitate Bob to have this direct connection with Alice. Bob could simply access Alice`s Facebook page without being logged in to his own Facebook personal account. Although possible individualization could be achieved based on the connecting IP address, used operating system, fingerprinting and browser information [27], no direct identification of Bob within the social nodes could be easily realized.

Another potential imminent third party threat on Bob`s side is the internet service provider, which has access to all the url requests he makes. But if being very active on Facebook, visiting different pages repeatedly is just a normal activity that users do especially when it comes to a Page that is frequently updated and getting high traffic.

To reduce the risk of the channel interruption and clear any doubts or suspicions of any communication between Alice and Bob, we found out that the more active and engaging the content of a Facebook page is, the more disguised and innocent looking the communication channel remains. This is very important because Alice should constantly maintain her page but not only bring some updates when an important message needs to be transmitted.

It is also really important to choose a topic that interests a great number of audience and that deserves a great amount and varied image galleries. In our experiments, we have categorized Facebook pages in two categories; one for posts that gives joy and another that shows violence and sadness. It has been noticed that most pages that bring good feelings are receiving more likes (followers) and are highly viral on the network. Creating pages that will have engaging followers will make the proposed scheme hard to detect and despite its simplicity it makes it more efficient.

7. Performance of the proposed steganography scheme

The performance of the covered channel proposed in our scheme could be analyzed based on the three (3) main indexes, characteristics of a steganographic covert channel: capacity, robustness and undetectability. Capacity represents the data sent per time unit by using a given method. Robustness refers to the amount of manipulation the stego-file can withstand while still being able to preserve the information to be transmitted. Undetectability represents the main security of any steganographic channels; in other word, it is the ability to keep the communication channel hidden.

Capacity: with pictograms being ideograms, they are very flexible in terms of complexity. In our proposed scheme, we derived words from what the images represent. In this sense, each image can correspond to one word. And as images can be sent in a batch to make a gallery in a given social networking website, a presumably long message could be transmitted at each creation of a gallery. Moreover, unlike other image based steganography where each stego-image (which is the cover image + the message) is fed at the limit till avoidance of statistical steganalysis, this proposed scheme does not require any artifacts to be applied on the cover image making it free of any risks from the most renowned steganalysis in the literature to date.

Robustness: unlike the other image based steganography methods that embed information within the cover, the proposed scheme enables a message transmission while leaving the cover image untouched. Compression, moderate contrast and brightness manipulations, which are really common practices won`t have any effect on the proposed scheme. Even cropping is tolerated up to the point that the main content of the image expressive of the ideogram is still visible.

Undetectability: using images that are presumably free of any artifacts, no steganalysis related work has been made available to fight against pictogram images online to date to the best of our knowledge. This Pictographic Steganography Based on Social Networking Websites requires no extra binary to be added to the cover image. Only identification of the ideogram with no further processing of the image is enough whether on the sender or the receiver side. Social networking websites like Facebook are extensively used for posting photos. Releasing pictograms on such platform would go unnoticed especially if the Page is well maintained and has a lot of visitors. The implementation of the proposed protocol does not have to be limited on a single Facebook Page. Multiple Pages could be used to enable a diversification of the image used.

8. The main advantages of the proposed steganographic system

Communication from one to many: Social networking websites main purpose is to connect people without border limitation. This could be used in the proposed steganographic system where Alice would publish the images that convey the message and anyone knowing the exact protocol and have the key shall be able to retrieve and make a proper reconstruction of its content (Fig. 4).

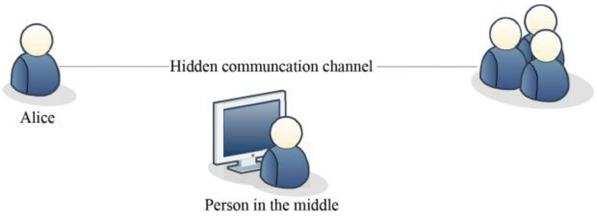

Fig. 4. Hidden communication channel from one to many.

Pervasive platform: Many social networking platforms have emerged in the recent years and photos of different kinds are submerging the Internet. Photo sharing is now a part of the social netizens daily activities. Because the proposed steganographic scheme does not introduce any artifacts in the images to drive the information, an attempt in investigating all nodes connected on a social networking website and trying to make sense of all the submitted images would be practically infeasible. Also it is quasi-impossible to correctly retrieve the images that form the complete message without the key and the dictionary.

Enough images to exploit: One main resource we need in this scheme is a bank of image. There are many free images available online, but as we have selected Facebook for this case study, we could also get the images from Facebook. For a long text to be converted into pictograph, we need a great amount of images and that is of no issue. Facebook allows its users to download and save the images that are publicly available on a Facebook Page. Using an original content although preferable (as it is more likely to be beneficial for some other Facebook users making the page popular, and a popular Facebook page will reduce suspicions) is a bit time consuming. So, in the presented method, Alice (as she is the one who should upload the images) could rip some images from other Facebook pages of her choice by simply retrieving the link to a Facebook page, opening the selected page in a browser, going to the album gallery, selecting the album to rip, clicking on the first photo, and refreshing the page. From there, to automate the download of all the images in the selected gallery starting from what was selected, Alice could simply use a solution for web automation browser add-on like iMacro (http://wiki.imacros.net/) to run the script below straight from a browser such as Firefox, Google Chrome or Internet Explorer.

```
VERSION BUILD=8601111 RECORDER=FX
TAB T=1
TAG POS=1 TYPE=A ATTR=TXT:Next
TAG POS=1 TYPE=A ATTR=TXT:Download
```

To discharge any doubt that placing images that are not related to the event of the author in a Facebook Page is somewhat odd and confessing that these might be pictogram communications. Alice and Bob are and should not be limited to only just use one Facebook Page for their communication channel. Multiple pages relating to different interests could be used and is a good practice to void the raise of suspicion.

9. Conclusion

In this paper we have presented an image steganographic scheme for social networking websites using pictograms mixed with other innocuous images. The secret message is concealed in a form of pictograms leaving a third party observer unaware of the very existence of the communication channel. The global reach of online social networking websites forms the main platform for this proposed method. And so, by using pictograms to vehiculate secret messages on social networking pages, we could have a mass delivery. The security of the proposed steganography relies on the abundance of images on those social networking websites, the omnipresence of the pictogram within the selected online social network, the complexity of any attempt to brute force the meaning of the pictograms without the key and the dictionary. A higher level of security could be achieved by adding an extra step for using a one-time use dictionary in the scheme. In our case study, the page popularity would reduce the creation of suspicion about the existence of the steganography channel.

It would also enable a communication from one to many and make it look as if is they are ordinary connections. Apart from being simple and very pragmatic, the case study presented in this paper of a steganographic system based on social networking website using pictogram could be implemented in most similar websites with just a minor adjustment.

References

[1] Myres, John Linton. Herodotus, father of history. Clarendon Press, 1953.

[2] Waterfield, Robin, and C. Dewald. "Herodotus: The Histories." Herodotus:(translation (1998).

[3] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A Study of Various Steganographic Techniques Used for Information Hiding." arXiv preprint arXiv:1401.5561 (2014).

[4] Kawaguchi, Eiji, and Richard O. Eason. "Principles and applications of BPCS steganography." Photonics East (ISAM, VVDC, IEMB). International Society for Optics and Photonics, 1999.

[5] Anderson, Ross J., and Fabien AP Petitcolas. "On the limits of steganography." Selected Areas in Communications, IEEE Journal on 16.4 (1998): 474-481.

[6] Westfeld, Andreas, and Andreas Pfitzmann. "Attacks on steganographic systems." Information Hiding. Springer Berlin Heidelberg, 2000. APA

[7] Provos, Niels. "Defending Against Statistical Steganalysis." Usenix security symposium. Vol. 10. 2001.

[8] Facebook Help Center. 2015. Basic Privacy Settings & Tools. Retrieved April 12, 2015 from https://www.facebook.com/help/325807937506242/

[9] Özera Hamza, Avcıba Ismail, Sankura Bülent and Memonc Nasir. 2010. Steganalysis of Audio based on Audio Quality Metrics.

[10] Fridrich J. 2009. Steganography in digital media principles algorithms and applications. 1st Ed. Campbridge University Press.

[11] Johnson N.F and Jajodia S. 1998. Exploring steganography: seeing the unseen. IEEE Computer, (pp. 26-34).

[12] Srivastava, Lee A. B., Simoncelli E. P. and Zhu S-C. 2003. On Advances in Statistical Modeling of Natural Images. Journal of Mathematical Imaging and Vision.

[13] Fridrich Jessica, Goljan Miroslav and Du Rui. 2001. Reliable Detection of LSB Steganography in Color and Grayscale Images.

[14] Fridrich and Goljan M. and Du R. 2001. Detecting LSB steganography in color and grayscale images. IEEE Multimedia 8, pp. 22–28.

[15] Nabaee H. and Faez K. 2010. An efficient steganography method based on reducing changes. 25th International Conference of Image and Vision Computing New Zealand (IVCNZ), (pp.1 – 7).

[16] Toony Z., Sajedi H. and Jamzad M. 2009. A high capacity image hiding method based on fuzzy image coding/decoding. Computer Conference, CSICC 2009. 14th International CSI, (pp. 518 – 523).

[17] Sajedi H. and Harif. 2008. Cover Selection Steganography Method Based on Similarity of Image Blocks.

[18] Bohme R. 2010. Advanced Statistical Steganalysis (2010 edition). Springer.

[19] Marincola J. M. 1996. Herodotus: The Histories.

[20] Landau S., Kent S., Brooks C., Charney S., Denning D., Diffie W., Lauck A., Miller D., Neumann P. and Sobel D. 1994. Codes, Keys and Conflicts: Issues in U.S. Crypto Policy. Rep. of a Special Panel of the ACM U.S. Public Policy Committee.

[21] Beaver D. 2008. 10 billion photos. (October 2008). Retrieved April 12, 2015 from https://www.facebook.com/notes/facebook-engineering/10-billion-photos/30695603919

[22] Fridrich J., Goljan M. and Du R. 2008. Detecting LSB steganography in color, and grayscale images. IEEE Multimedia, vol. 8 no.4, pp. 22 – 28.

[23] Dumitrescu S., Wu X. and Wang Z. 2003. Detection of LSB steganography via sample pair analysis. IEEE Transaction on Signal processing, vol. 51, no. 7, pp. 1995-2007, 220.

[24] Zhang T. and Ping X. 2003. A new approach to reliable detection of LSB steganography in natural images. In Signal processing (Vol. 83, pp. 2085-2093, 2003).

[25] Kerckhoffs A. 1883. La cryptographie militaire (Vol. ser. 9). J. des Sciences Militaires.

[26] Nikiforakis N. and Acar G. 2014. Browse at your own risk. Spectrum, IEEE, Volume: 51, Issue: 8 , pp. 30 - 35.

[27] Eckersley P. 2010. How Unique is Your Web Browser? Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010). pp. 1-18

Feno Heriniaina R. received his Master's degree from the College of Software Engineering in 2011and is presently a Ph. D candidate at the State Key Lab. of Power Transmission Equipment & System Security and New Technology, College of Computer Science, Chongqing University.

Xiaofeng Liao received the B.S. and M.S. degrees in mathematics from Sichuan University, Chengdu, China, in 1986 and 1992, respectively, and the Ph.D. degree in circuits and systems from the University of Electronic Science and Technology of China in 1997. His current research interests include neural networks, nonlinear dynamical systems, bifurcation and chaos, and cryptography. He is a senior member of the IEEE.