ENGN6528 Literature Review on Steganography

30 May, 2017

Javed Ashraf (U6272684)
The Australian National University

Abstract— **The domain of image steganography has developed many techniques over the year, however it is still restricted to encoding messages in a single image. Also, some concepts of cryptography have been incorporated into the messages or security. In this survey, LSB based steganography techniques are discussed along with a method to detect such encoded image. Also, a novel approach based on internet search for steganography is reviewed, followed by analyzing new areas of improvement in this domain.**

I. INTRODUCTION

In this review, the domain of steganography is considered, which is often confused with cryptography. Cryptography is the process of encrypting a message so that anyone who intercepts the message can't understand them. Steganography on the other hand is to hide the message into an image in this case, so that only the sender & receiver know how to extract & read the message. However, both steganography and cryptography are used together for better hiding of data and improved security in case the data is found by an opponent.

A small question may be why do we need steganography? According to many rules, for example in corporate world, passing on sensitive information or documents like a design of a new product or details about a merger, which are necessary. These are often sent via digital means like e-mails, cloud share or FTP clients. But, they are also prone to external opponents who can intercept such information and leak them publicly which may cost the company some revenue. Steganography provides a new secure method of sharing such information under the pretext of sharing some casual images for fun.

Image based steganography currently work on a single image & use multiple masks to encode messages in them. In this Literature survey, the current development in this domain will be reviewed and new areas of research will be determined by analyzing them.

II. Background on current methodologies

Ross & Fabien, have reviewed some of the commonly used techniques in steganography [1]. A simple technique to encode message would be to use a cryptographic style key based encryption to encrypt the message on to the image on the pixel values. Another method involves altering the images values in the frequency domain via discrete transformation techniques. However, their message is vulnerable to loss in data when saved in commonly used image compression techniques. Also, as mentioned in the paper, the crypto key needs to be shared to be successfully implemented. If the key is leaked, the message could be compromised easily.

Neil & Sushil's paper [2], an encoding based on 24-bit color scheme used in images. The image is split into R, G & B components with an 8-bit pixel value. The Least Significant Bit (LSB) for 3 pixels are used to represent a single character of a message. Though, in some case the change in pixel values seem to make significant changes in pixel intensity in color images, some color palette modification is required to ensure the message pixels are not distinctly visible to the naked eye. This method required the image to be stored in BMP image compressing techniques to work. Hence masking techniques are used to compensate for pixel changes in compression of image.

In Niels & Peter's paper, they have approached a frequency domain encoding of the message [3]. A discrete cosine transform is applied on the image for an 8x8 block of pixels. Then, the image is encrypted with a key and message is made into bits. The LSB of the pixel in the transformed image is then changed with the message bits. Then an inverse transform is done to retrieve the encoded image. One of the key aspects in this method is that, since the encoding is done in a transformed domain, image compression formats like JPEG could be used.

Babita *et al.* presents a randomized key generation method for the encryption of steganography image [4]. A 16-character user defined encryption key is used here. The key is used to encrypt the message using an XOR operation with another randomly generated key. Then, the encrypted message is converted to an 8-bit code per character. This is then applied on either R, G or B plane component of the image, changing in a pre-defined sequential order. In this method, they require to save the encoded image as a bitmap file to avoid losing data.

Jessica *et al.* made a methodology to detect LSB changes in steganography implemented images [5]. They segment pixel into groups based on a statistical discrimination of pixel with its neighbors. Then on a mathematical model, the range of pixels with encoded message is determined. This data could be passed on to any decryption software to extract the message encoded in the image.

Shangwei *et al*. has discussed an internet search based methodology to steganography [6]. The concept they proposed is to search the internet for webpages with the data similar to the message. Then, these web pages are then used to map parts of the message to content in the pages. Finally, the set of webpages along the position of the message is sent. In this method, the data is made hidden in plain sight, that web-pages that people generally read through are used. Hence, unless the receiver gets the exact key of the message, the message can't be recovered.

III. Analysis of current methodologies

In the work done by Ross & Fabien [1], it could be seen that the compression techniques which is automatically applied when saving an image may sometimes corrupt the message data embedded in the image. Hence, it is important to ensure the data format in which the steganography image is stored doesn't change the pixel values and in-turn losing the message. In addition, it can be inferred that public keying system may not be very secure in case any opponent could get the actual data on hand. Hence, the security of the key is necessary to protect the data.

From Neil & Sushil [2], it can be inferred that a bit wise operation of pixel values may limit the visual changes to the image, but again the data format would pose a threat when saving the image. They end up using BMP format which is not a very efficient means. Also, it doesn't have a very good compression of file size, making the size of image file higher than other types. This may not restrict the modes of communication between the sender and receiver as huge image files not only make sharing difficult but also arises suspicion among any opponent checking for messages.

As per Niels & Peter [3], in order to avoid data loss from the effects of data compression in lossy formats like JPEG, the message data has to be encoded in the frequency domain of the image. This gives the advantage of the file size being small and a means to use commonly used formats like JPEG to avoid suspicion. However, this ignore the aspect of how secure the image is to random check done by an opponent who could intercept this message.

To address the issue raised in Ross & Fabien's work, Babita [4] proposed a randomized key generation technique. Even though the key is encrypted at a 2nd level of encryption, it still has the aspect of a common key which is to be exclusively shared in order for both the parties to send & receive the message. Additionally, the message bits are not only changes in row or column wise sequential order, but they are changes individually in the plane coordinates as well. This may improve the complexity of the algorithm by one but still doesn't bring about a big jump to evade steganography detection algorithms.

As a means to intercept steganography encoded images, Jessica *et al.* [5] devised a technique to determine any changes to the LSB based steganography techniques. It uses statistical prediction type algorithm and checks the pixels along the general direction of changes.

One of the most common characteristics in existing steganography techniques is that the message bits are encoded in a sequential order, one after the other. Hence, it is possible to do force check a set of pixels using techniques like the one given by Jessica *et al.* and determine if the image is encoded or not. So, a question is, how do you escape such detection algorithms? Another common aspect those techniques share is that the data is encoded into a single image. This would be an issue, when the message to be passed is larger than the resolution of the image. A simple technique would be to resize the image, but that would damage the quality of the image and may make encoding pixel changes visible to the opponent, thus defeating the whole purpose. This would be another challenge to answer.

In the idea proposed by Shangwei *et al*. [6], there is an advantage in using commonly used web resources to transfer data. Their method focusses on sending URLs and data on which part of the webpage the message is held. In the case of large messages, multiple URLs could be shares. But the they do not focus on how the URL & position of message in the page are being sent. In addition, sometime there is the risk of certain messages data not existing in the internet. Such ambiguity is not clearly mentioned. However, the idea to use public webpage resources that are taken for granted to send messages is certainly a concept to consider for further development.

IV. Conclusion

From the above analysis, we can conclude the current steganography techniques rely on encoding a single image with the message. Though there are different methodologies involved, due to limitation of a single image, with the help of some computing algorithms, it is possible to detect them. The process of encrypting the data is a common process in steganography, but the concept of an encrypting key makes it both a boon and liability. The following areas to research were raised:

- Alternate methods to use the encryption key so that even if the key is discovered, the message can’t be deciphered.
- Encoding message data in image while ensuring it doesn’t get corrupted while image compression is done when saving the image.
- To solve the issue that arise when low resolution images are used in steganography.
- Design a detection-free steganography encoding technique.
- Incorporate public image sharing domains for steganography.

V. References

[1] R. J. Anderson and F. A. P. Petitcolas, "On the Limits of Steganography," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,* vol. 16, no. 4, pp. 474-481, 1998.

[2] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer,* vol. 31, no. 2, pp. 26-34, 1998.

[3] N. Provos and P. Honeyman, "Hide & Seek: An Introduction to Steganography," *IEEE Security & Privacy,* vol. 99, no. 3, pp. 32-44, 2003.

[4] Babita, Anju and Ayushi, "An Approach to Improve Image Steganography using Random Key Generation Method," *International Journal of Information and Computation Technology,* vol. 3, no. 4, pp. 235-240, 2013.

[5] J. Fridrich, M. Goljan and R. Du, "Detecting LSB Steganography in Color & Gray-scale Images," *IEEE MultiMedia,* vol. 8, no. 4, pp. 22-28, 2001.

[6] S. Shi, Y. Qi and Y. Huang, "An Approach to Text Steganography Based on Search in Internet," in *2016 International Computer Symposium (ICS),* Chiayi, Taiwan, 2016.