[[1]](#footnote-1)

ENGN6528 Literature Review on

Steganography

31 May, 2017

Mohit Reddy Kondreddigari (u6114363)

The Australian National University

*Abstract*— Steganography, it is oldest form of data encryption dating from the era of Roman and continuing all the way through to the 19th century But, with the dawn on the computer age encryption has moved well into the field of Cryptography while leaving the Steganography vastly underdelivered. This review looks at the current advances critiques and then proposes a few new directions in through which steganography proceeds.

# INTRODUCTION

Steganography is the art of hiding information in plain sight intrinsically providing a measure of security and safety allowing a message to be transmitted. Steganography is not to be confused with cryptography which involves modifying a message so that it is unreadable or unintelligible to everyone other than the intended recipient.

Cryptography has the inherent weakness that regardless of how strong the encryption technique is, it is still possible to recognize that a hidden message is being passed around. This is can be better visualized by an example. Say Person A wants to communicate secretly to Person B, and sends an encrypted message. Another person say C can still recognize that there is a form of clandestine communication taking place. But if Person A sends a message using steganography even if person C is able to intercept it they would not be able to recognize that is a form of secret communication.

The next question one might ask why does Steganography matter? If Person C is not able to decode the hidden message there is still no loss of important message. Steganography comes to play when it is necessary to even hide the fact a form of communication is taking place. For example, contact between CEOs of two different companies who are going in for a merger but want to keep the ordeal a secret.

# Literature Review on Steganography

Sushil and Neil’s [1] paper on modifying the Least Significant bits in a lossless format such as BMP or Gray scale GIF image paves way for basic steganography using an image file. The use of the LSB allows for the image to be changed while still appearing to be visually similar to the human eye. Although some changes to the images LSB are still discernable by the human eye a masking technique to deal with this problem is suggested. They focus on their paper on BMP images which are very costly in terms of storage space required and has long since been phased out by more efficient image formats and remains only as a legacy standard.

Anju *et al.* [2] Improve upon Sushil’s and Neil’s a paper on using LSB in a BMP image. They use a user defined key to encrypt the message to be encoded and then then further improve security by applying and XOR function on the LSB bits. This XOR function is done using a special cycle which maybe varied, in their paper they use a cycle of RGBBGRRG further trying to improve on the security of the data. While they make an improvement, they are still restricted to using BMP images and they still have the same failings of the previously discussed paper.

Fabien and Ross [3] in their paper explore on potential new methods to use steganography on images. They glance on upon the existing method of using LSB modification and further suggest the use of the Fourier Transform of an image as potential technique. While they provide no detail as to the process they note that it requires a pre-shared key which makes their method crack-able after a while or if the key is leaked.

Peter and Neil [4], use the techniques mentioned by Fabien and Ross and use Discreet cosine transformation 8x8 blocks on JEGP images to hide the entire first chapter of “The Hunting of the Snark” in the redundant data held in a JEPG image. Their method also uses a shared -secret key to encode data. An inverse transform is applied to get back the original message. The use of discreet transforms allows the image to be transferred though the compression technique employed by JEPG. But they do note that because of the use of the lossy JEPG format they expect some data loss. This is loss is sometimes unacceptable in the transmission of data. They also use only one image encode their data into.

While using discreet transforms to store image on lossy formats is a great idea, the loss of data is still a problem. Leading us back to the steganography methods of using LSB of a BMP or a Gray scale image, but work done by Jessica *et al.* [5]show that is possible to recover data by grouping the pixels of the image into a mathematical model and locating pixels upon which LSB modification could be performed upon. These selected pixels could then just be sent to a decryption software and the encoded message would be cracked. This paper shows us the weakness of encrypting a message using the LSB method.

A unique take on Steganography is mentioned in this paper by Yining *et al.*[6] which postulates that the inherently humungous size of the internet means that any message can hidden in the form of an existing webpage found online and all the characters required by the secret message would be present on the cover page of webpage. This in itself provides a uncrackable method as it uses only existing webpages and the only message being transmitted would be the URL.

# Conclusion

From the analysis of existing literature, we can conclude the following common characteristics of current steganography.

1. Only a single image is used to encrypt the message in.
2. Losses Image formats are required to successfully implement steganography but they are limited only to BMP or grey scale so far.
3. Most techniques don’t make use of the internet itself as method of steganography and the one which does only postulates the possibility.
4. Use a single pre-shared key

Condensing the above points we can predict the direction steganography need to take in the future to be as upto date as Cryptography techniques. The recommend directions of this review are

1. Multiple image steganography, where the image in encoded over many images and not just one.
2. Use of more modern formats like PNG which retain the losses quality of BMP images while being compressible like JEPG.
3. Using the shear variation of URLs found online to generate a unique key
4. Generating single-use keys which change every time a message is sent regardless of the message content.

# References

|  |  |
| --- | --- |
| [1] | S. J. Neil F. Johnson, "Exploring Steganography:," *Computing Practicess,* no. 1998, pp. 26-35. |
| [2] | A. a. B. Anju, "An Approach to Improve Image Steganography using Random Key genration," *International Journal of Information and Computation Technology,* vol. 3, no. 4, pp. 235-240, 2013. |
| [3] | F. A. P. P. Ross J. Anderson, "On the Limits of Steganography," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,* vol. 16, no. 4, pp. 474-482, 1998. |
| [4] | P. H. NIELS PROVOS, "Hide and Seek: An Introduction to Steganography," *IEEE SECURITY & PRIVACY,* vol. 3, pp. 32-45, 2003. |
| [5] | M. G. a. R. D. Jessica Fridrich, "Detecting LSB Steganography," *Multimedia and Security IEEE,* pp. 22-29, 2001. |

1. [↑](#footnote-ref-1)