Journal of Computer Science 6 (3): 320-322, 2010
ISSN 1549-3636


# Stego Encrypted Message in Any Language for Network Communication Using Quadratic Method

Ahmed Ch. Shakir
Department of Computer Science, Kirkuk University, Kirkuk, Iraq

**Abstract: Problem statement:** Extensive use of digital media like text, images, audio and video on the internet generated a requirement for providing traffic security. For carrying out confidential communications over public networks, it was found that simply concealing the contents of a message using cryptography was not adequate. Concealing the very fact that a communication has taken place could provide an additional layer of security. In this study several methods are used to fulfill this goal. This study produced new procedures in steganography for hiding ciphered information inside a digital color bitmap image. **Approach:** In this project we were using quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. **Results:** Very immune information from hacking and breaking. **Conclusion:** In this study, we had concluded that the conjunction between cryptography and steganography produce immune information. The Unicode made any language to be used. The conversion to binary image is for selecting the locations of the message to be saved and it gives somewhere randomly locations for the pixels to be used for hiding.

**Key words:** Public key cryptography, steganography, binary image and binary number

## INTRODUCTION

Security and secrecy of information has always been important to people, organizations and governments (Solanki *et al*., 2006). The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party (Bandyopadhyay, 2008).

In this study, we consider the problem of steganography: Steganographic techniques can be used to hide data within digital images with little or no visible change in the perceived appearance of the image and can be exploited to export sensitive information (Currie and Irvine, 1996).

In particular, steganography becomes one of the most powerful tools of hiding information that is transferred through the Internet. Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not (Johnson and Jajodia, 1998).

In the framework presented here, the message is to be encrypted by using the public key cryptography before it would be hidden. The covered media (the image that will use to embed the message) is color image with extension ".bmp "that contains much information without compression.

This image is converted into binary image for selecting the locations in the color image to save the encrypted message. Finally the Quadratic method would be used for hiding the encrypted message in the color image in which the locations are selected using the binary image for the covered medium.

## MATERIALS AND METHODS

**Selecting the pixels from covered medium:** The color image (covered medium) is converted to the binary image (0 represents black and 1 represents white); the location of the pixel whose value is 1 is used in the color image to hide the cipher text in these locations whose values are 1.

**The quadratic method:** This method depends on the new system that has four numbers (0, 1, 2 and 3). The

number which is coming from the Unicode of the character to be hidden is in binary system and it is 16-bit. This number is divided in two eight number individually to produce numbers among 0→3. In example:

(1010) in binary is equal to (22) in quadratic, because each two bits are taken individually 10 = 2, 10 = 2

Because of that, in each pixel (8 bit for red, 8 bit for green and 8 bit for blue) three numbers in quadratic are added to it, then for one character to be hidden we need 3 pixels. So, we add to the left of the number two zeros for balancing which have no effects, that is mean the number of digits in quadratic system must be 9 (three for each pixel) not 8 digits.

In example: Character A is equal to 65 in decimal. It converted to the Unicode as follows:

(000000000001000001) it would be converted to quadratic as follows:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 01 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

Let we have the following pixels(each three values RGB represents one pixels) which are selected from locations of ones in binary image of the color image which is used as an covered medium:

| | | | |
|---|---|---|---|
| 45 | 60 | 81 | 10 |
| 83 | 255 | 74 | 110 |
| 201 | 235 | 101 | 15 |
| 9 | 78 | 159 | 48 |

Now, we add the Unicode to the above pixels as follows:

| | | | |
|---|---|---|---|
| 45+0 = 45 | 60+0 = 60 | 81+0 = 81 | 10+0 = 10 |
| 83+0 = 83 | 255-1 = 254 | 74+0 = 74 | 110+0 = 110 |
| 201+1 = 202 | 235 | 101 | 15 |
| 9 | 78 | 159 | 48 |

If the pixel value exceeds 255 when adding the Unicode to it like (255+1, 255+2, or 255+3), then in this case the subtraction is taken instead of addition. So that the changing is very small in comparing with taking the mod o 255 if exceeds it.

For the de-steganography the receiver converts the original image which is stored previously in him to the binary image, to find the locations in which the receiving color image used to hide the text in it.

Let we say that:

- a(i, j) is the binary image
- b(i, j) is the original color image
- c(i, j) is the received image

The locations in which the message is hided is found by finding the pixels in the binary image whose values are equal to 1, then the value of this location in the color image is subtracted from the original image to find the difference between them.

Then each pixel in the received image whose a(i, j) of it = 1 is subtracted from the original image c(i, j) - b(i, j). The result of the subtraction may be (0, 1, 2, or 3) which are in quadratic system. Here the absolute is always taken to prevent the negative value of pixels. Finally, each digit is converted into two digits (0 = 00, 1 = 01, 2 = 10, and 3 = 11) and the last two digits are ignored, the remaining 16 bits represents the encrypted character which is hided.

## RESULTS AND DISCUSSION

The public key cryptography is used before the steganography. The locations that are selected from the binary image whose values are 1 made somehow randomness of the pixels that are used in the color image for hiding the encrypted text. The quadratic system gives the ability to hide more characters because each 16 bit character is converted to 8 digits that increase the capability of hiding twice.

## CONCLUSION

There is a tradeoff among the power of security, time of processing, the number of characters to be hid and the quality of the image. Our study is concentrate on the power of security by designing the new system in quadratic. Any text in any language can be used in this study because it depends on the Unicode in which each character is represented by 16 bits.

## REFERENCES

Bandyopadhyay, S.K., 2008. A tutorial review on steganography. http://www.jiit.ac.in/jiit/ic3/IC3_2008/IC32008/APP2_21.pdf

Currie, D.L. and C.E. Irvine, 1996. Surmounting the effects of Lossy compression on steganography. Proceedings of the 19th National Conference on Information System Security, Oct. 1996, Baltimore, Md., USA., pp: 194-201. http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper014/STEGOX.PDF

Johnson, N.F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. Computer, 31: 26-34. DOI: 10.1109/MC.1998.10029

Solanki, K., K. Sullivan, U. Madhow, B.S. Manjunath and S. Chandrasekaran, 2006. Provably secure steganography: Achieving zero K-L divergence using statistical restoration. Proceeding of the IEEE International Conference on Image Processing, Feb. 20-20, IEEE Xplore Press, Atlanta, GA., pp: 125-128. DOI: 10.1109/ICIP.2006.312388