International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10570-10576
© Research India Publications. http://www.ripublication.com

A Proposed Method for Secure Steganography on PNG Image Using Spread Spectrum Method and Modified Encryption

Bogy Oktavianto
College Student, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia.
Orcid : 0000-0003-4846-3306

Tito Waluyo Purboyo
Lecturer, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia.
Orcid ID : 0000-0001-9817-3185

Randy Erfa Saputra
Lecturer, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia.
Orcid ID : 0000-0002-8537-2086

Abstract

Nowadays the development of technology and information is very rapid and fast. Anyone can easily access or send any data and information which creates a problem to improve system security. Therefore, we can use steganography to protect confidential data and information by hiding a message. This paper will discuss the application of steganography on Portable Network Graphics (PNG) image media with the spread spectrum method which is done by encryption process first

Keywords: Steganography, Spread Spectrum, Cryptography, Encryption, PNG

INTRODUCTION

Steganography is becoming the most important research topic in information security such as digital images, video, and audio. Steganography is the science and art of hiding messages inside the other messages so the existence of the first message is unknown [1]. Steganography comes from the Greek word '*steganos'* which means hidden text. Steganography is not cryptography, but both are complementary. Cryptography conceals the meaning of the message while the existence of the message persists, while the steganography obscures the existence of the message [2]. Messages on steganography are encrypted first, then hidden on a medium so that third parties are unaware of the existence of the message. Media that inserts messages in steganography is called cover-object. Cover-object used can vary, for example in the image archive.

Steganography is a technique to hide a good message in communicating so as not to arouse suspicion towards anyone other than the sender and recipient of the message. This application is used by military and intelligence agencies, detection of confidential messages towith cryptanalysis, techniques can quickly lead to attacks on agents [4]. In addition, steganography can be used for enterprise data protection protection for secure circulation of confidential data, and in accessing control systems for digital content distribution.

There are two general stages in digital steganography, namely the process of embedding or encoding (insertion) and the process of extracting or decoding (expansion or disclosure). The results obtained after the embedding or encoding process called Stego Object (if the media container only in the form of image data then called Stego Image).

There are several criteria that must be met in hiding messages [1].

1. ***Imperceptibility*** is the existence of a message that unable to perceived by the senses. If a message is inserted into an image, it must be indistinguishable from the original image by the eye.
2. ***Fidelity*** is the quality of the container that does not change much due to insertion.
3. ***Recovery*** is the ability of revealing the hidden message.

Cryptography is the art and science of securing messages. In cryptography, messages are called plaintext or cleartext. The process of disguising the message in such a way as to hide its original content is called encryption. The encrypted message is called ciphertext. The process of returning a ciphertext to plaintext is called decryption.

RESEARCH METHOD

Steganography

Steganography is the art of communicating using hidden messages. Generally, steganographic message will look like a regular picture, but the picture has been inserted with a hidden object. Steganography techniques can be applied to images, video or audio files [4]. The purpose of steganography is to protect against piracy that infringes copyright. Common examples are usually applied to digital media files, as this is the best way to store a great size of messages and inconspicuous general properties.

As for some advantages and disadvantages of steganography:

1. Only the senders and recipients of messages which can know the contents of the inserted information.
2. If a hijacker and terrorist can open it, then it is biased to be a very dangerous thing.

This technology is prioritized for the protection of a data, so the algorithm has different requirements for steganography. A good steganographic algorithm requirement will be discussed here. In the watermarking method all instances of an object will be "marked" in the same way. The type of information hidden in an object when using watermarking typically uses a "marked" to signify ownership for copyright protection purposes [14].

The recent image steganography techniques can be classified into:

1. Spatial (image) domain.
2. Compressed domain based on vector quantization (VQ).
3. Transform domain.
4. Spread spectrum.
5. Statistical technique
6. Distortion technique

Spread Spectrum

Spread spectrum is a signal generation technique that is deliberately spread over a bandwidth range larger than it should be. The term spread spectrum is used because in this system the transmitted signal has a bandwidth that is much wider than the bandwidth of the information signal (reaches thousands of times). The process of spreading the bandwidth of this information signal is called spreading. The first type of spread spectrum developed is known as the frequency hopping.

The spread spectrum method transmits a narrow band of information signal into a broadband with frequency deployment. The spreading frequency will increase the level of redundancy. By increasing the redundancy level, the code will not easily be solved.

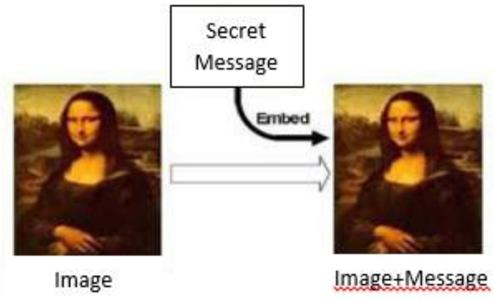


Figure 1: The example of a picture inserted by a hidden message

In Figure 1 it is clear that the images that have been dis titled secret messages have no significant change. Spread Spectrum Image Steganography (SSIS) is a technique of storing secret messages using keywords known only to senders and recipients. SSIS provides the ability to hide and restore an image without making suspicions to others. Furthermore, SSIS is a very secure method since the original image is not required to extract the hidden information. The recipient only needs to have a key from the sender to reveal a hidden message. The existence of the hidden information is almost undetectable [14].

The calculation of the generation of random numbers on spread spectrum using LGC formula, namely:

$$X_{n+1} = (aX_n + c) \bmod m \qquad (1)$$

Portable Network Graphics (PNG)

Portable Network Graphics or commonly abbreviated as PNG is one of the image storage formats which uses a compacting method that does not remove part of the image. In general, the PNG format is used for Web images that created to replace GIF formats with better compression.

Steganography techniques can be classified into:

1. Transparency
2. Gammba (lighting setting)
3. Progressive image viewing

Cryptography

Cryptography is the art and science of securing messages. In cryptography, messages are called plaintext or cleartext. The process of disguising the message in such a way as to hide its original content is called encryption. The encrypted message is called ciphertext. The process of returning a ciphertext to plaintext is called decryption. Cryptography aims to keep messages or documents unreadable by unauthorized persons and falsification of message documents so that the person sending the message can not escape the responsibility of sending the message. Cryptographer is a person who practices cryptography while cryptoanalysts are people who practice cryptanalysis , art and science in solving ciphertext.

RESULTS AND ANALYSIS

The Results with Spread Spectrum Method and Encryption

In this section will discuss about the experiments and the results of experiments using spread spectrum method that first performed the encryption process. The example uses 3x3 pixel image with PNG image format.

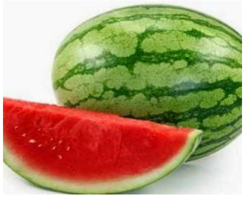


Figure 2: A watermelon

In Figure 2 there is a watermelon that will be experimented using spread spectrum method. The first step is to convert the pixel of the image to 3x3 pixels and find the value of RGB that is still valuable in decimal form and convert it into binary form so that characters can be inserted, as shown below.

Red value in decimals:

243	128	155
211	110	58
199	193	185

Green value in decimals:

255	195	193
113	72	96
70	47	177

Blue value in decimals:

255	101	122
95	4	5
58	41	158

Afterwards, all RGB values are changed into bit forms.

Red value in binary:

11110011	10000000	10011011
11010011	01101110	00111010
11000111	11000001	101110011

Green value in binary:

11111111	01100101	01111010
01011111	00000100	00000101
00111010	00101001	10011110

Blue value in binary:

11111111	11000011	11000001
01110001	01001000	01100000
01000110	000101111	10110001

To determine the number of characters in RGB digital image that can be inserted by multiplying the pixels of digital image then multiplied by 3 bytes and divided by 8 bits. For example, 3x3 pixels, then

Number of pixel: 3x3 = 9

9 pixel x 3 byte = 27 byte

27 byte : 8 bit = 3,375

Each byte contains 1 bit character, then if rounded characters that can be inserted amounted to 3 characters or letters.

A picture with PNG format and 3x3 pixels will be inserted by a message "DAN" with keyword "s". Before the process of spreading, the message "DAN" is changed into binary form. The result of converting the message "DAN" is 01000100 01000001 01001110. Then the binary message is spread with one as the scale multiplier, so that the message segment obtained is 01000100 01000001 01001110 same as the message before multiplied.

Then the message segment 01000100 01000001 01001110 or in cryptographic language is the plaintext is encrypted to become a chipertext with keyword "B". Change the keyword "B" into the binary form and the resulting conversion is 01000010. After that the plaintext is encrypted with the keyword "B" using the XOR function.

Plaintext: 01000100 01000001 01001110

Keyword: 01000010

Chipertext: 00000110 01000001 01001110

The next step is the generation of *pseudo noise* by changing the keyword "s" into the binary form and the resulting conversion is 01110011. Afterwards, the binary shape is changed into decimal form and the value obtained is 227.

After getting a decimal value of 227 as a keyword, then the value is used as the initial seed of the generation of random numbers. The calculation of the generation of random numbers using the LCG formula(1).

With the value a = 2, c = 7, m = 9 then the calculation value X_1 = (2 x 227 + 7) mod 9 and the result is 5. Next, the number of 5 is changed into binary form to 00000101.

Then for the chipertext is modulated by pseudo- logise signal using XOR function.

Chipertext: 00000110 01000001 01001110

Pseudonoise signal: 00000101

Result of XOR: 00000011 01000001 01001110

Furthermore, the modulation results will be inserted into the pixel bits by changing the last digit on the rightmost of RGB. The following is the result of modulation process between message segment and pseudonoise signal.

Red value after insertion:

1111001**0**	1000000**0**	1001101**1**
1101001**1**	0110111**0**	0011101**1**
1100011**0**	1100000**1**	10111001

Green value after insertion:

1111111**0**	0110010**0**	0111101**1**
0101111**0**	0000010**0**	0000010**0**
0011101**0**	0010100**1**	10011110

Blue value after insertion:

1111111**0**	1100001**0**	1100000**0**
0111000**0**	0100100**0**	0110000**1**
0100011**1**	0001011**1**	10110001

The next process is the extraction by demodulation. The demodulation process is performed by pseudo noise signals from the same keyword in the modulation process to obtain correlated bits.

Filter results: 01000001 01000001 01001110

Pseudonoise signal: 00000101

Demodulation result: 01000100 01000001 01001110

The above demodulation result is chipertext. Chipertext must be converted to plaintext, this process is called decryption. The decryption process is performed using the XOR function between the chipertext with the previously defined "B" keyword.

Chipertext: 00000110 01000001 01001110

Keyword: 01000010

Plaintext: 01000100 01000001 01001110

The above plaintext is the initial message segment which then splits one plaintext to know the actual message idea. The process of de-spreading the segment becomes:

01000100 01000001 01001110

If it is changed into the character form, it can be known that the message is "*DAN*".

Analysis of RGB and Grayscale Digital Image

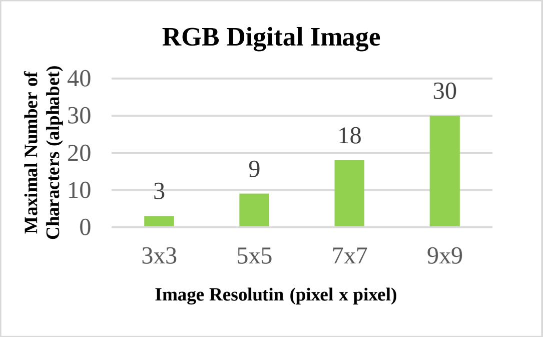


Figure 3: The maximum number of characters that can be inserted into RGB

In figure 3 explains the RGB digital image on the y-axis is the maximum number of characters in the letter that can be inserted. On the x axis is the image resolution in pixels. The larger the pixels, the more letters can be inserted. RGB digital image has 3 channels that is Red, Blue, Green. Thus the number of characters in letters that can be inserted in RGB digital images can be more than in Grayscale digital images with the same pixels.

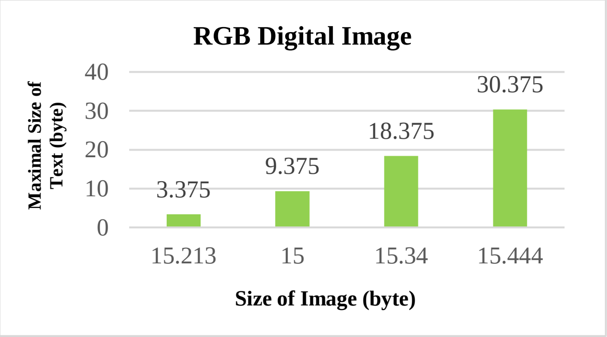


Figure 4: Maximum text size that can be inserted in RGB

In figure 4 describes the RGB digital image on the y-axis is the maximum text size in the letter that can be inserted. On the x axis is the image size in bytes.

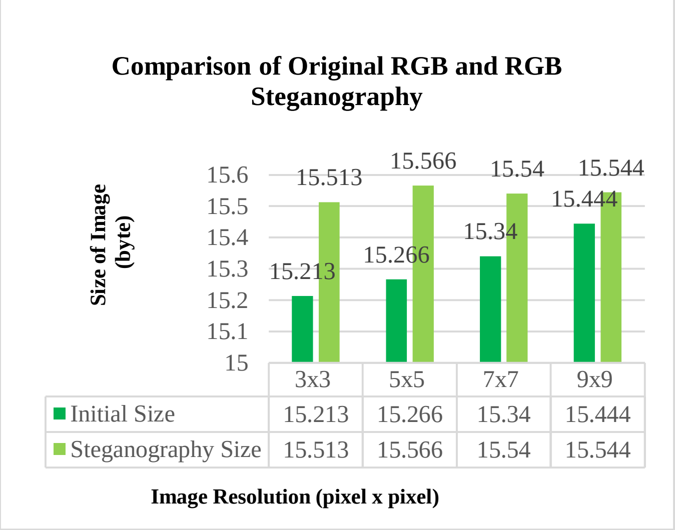


Figure 5: Comparison of Original RGB and Steganography RGB

From figure 5 RGB digital image above, the analysis obtained that the greater the pixel, the greater the number of characters that can be inserted in a picture. The comparison of the image size before and after the inserted message does not significantly change the size of the image. To determine how many characters can be inserted by multiplying the pixel and then multiplying by 3 because digital RGB image has 3 channels, then divided by 8 bits and obtained results that can determine the number of characters in letters. Thus the number of characters in letters that can be inserted in RGB digital images can be more than in Grayscale digital images with the same pixels.

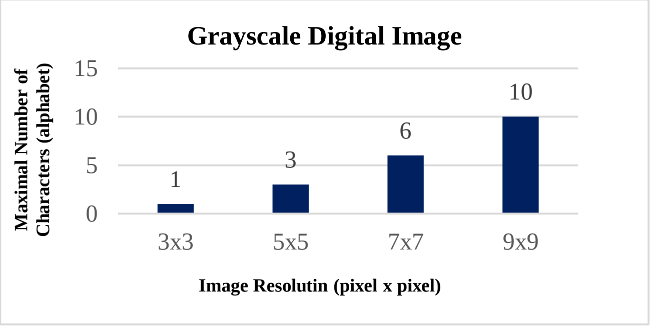


Figure 6: The maximum number of characters that can be inserted in Grayscale

In figure 6 explaining Grayscale's digital image on the y-axis is the maximum number of characters in the letter that can be inserted. On the x axis is the image resolution in pixels. The larger the pixels, the more letters can be inserted. This rule also applies to RGB digital imagery. Grayscale digital image has 1 channel only while RGB has 3 channels that is Red, Blue, Green. Thus the number of characters in letters that can be inserted in the Grayscale digital image is less than the RGB digital image with the same pixels.

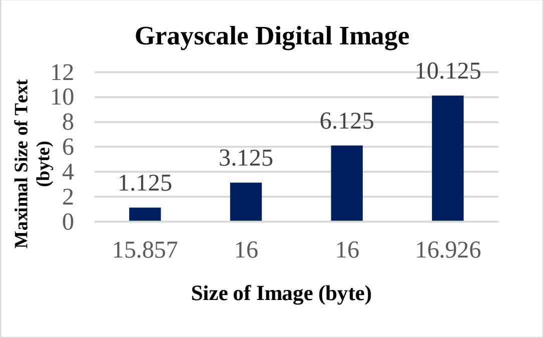


Figure 7: Maximum text size that can be inserted in Grayscale

At figure 7 explaining Grayscale's digital image on the y-axis is the maximum text size in which letters can be inserted. On the x axis is the image size in bytes.

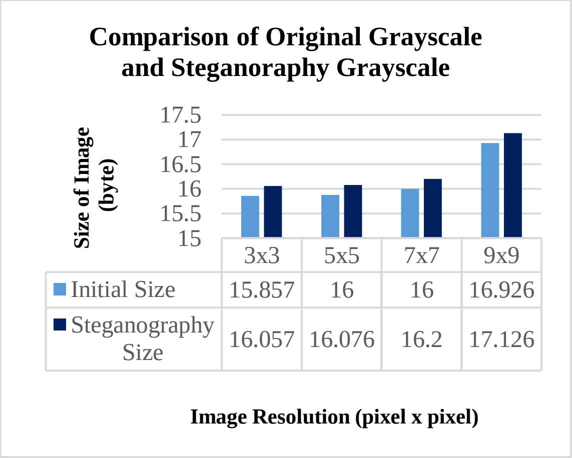
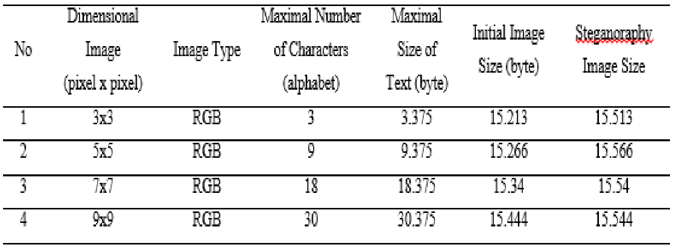


Figure 8: Comparison of original Grayscale and Grayscale steganography

From figure 8 Grayscale digital image above, the analysis obtained is almost the same as the digital image of RGB, the greater the pixel, the greater the number of characters that can be inserted in a picture. The comparison of the image size before and after the inserted message does not significantly change the size of the image. To determine how many characters in letters can be inserted by multiplying the pixels and then multiplying by 1 because Grayscale has only 1 channel, then divided by 8 and results are obtained that can determine the number of characters in letters. Thus the number of characters in letters that can be inserted in the Grayscale digital image is less than the RGB digital image with the same pixels.

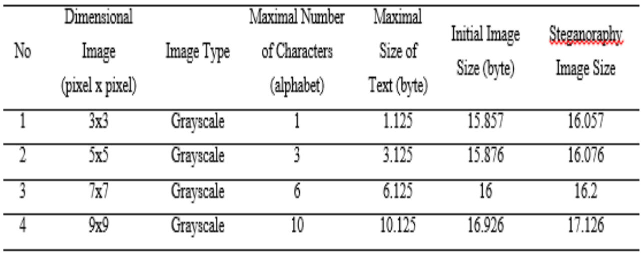
Table 1: The overall experiment result data on RGB



No	Dimensional Image (pixel x pixel)	Image Type	Maximal Number of Characters (alphabet)	Maximal Size of Text (byte)	Initial Image Size (byte)	Steganoraphy Image Size
1	3x3	RGB	3	3.375	15.213	15.513
2	5x5	RGB	9	9.375	15.266	15.566
3	7x7	RGB	18	18.375	15.34	15.54
4	9x9	RGB	30	30.375	15.444	15.544

Table 1 describes the results of the whole experiment on RGB digital imagery. There is a dimension of the image in pixels and then it can be known the maximum number of characters in letters that can be inserted. There is also a maximum text size in unedited bytes to know how many characters in the letter can be inserted. This table is also the size of the initial image before the disteganography and image size after the disteganografi in bytes.

Table 2: Data on the overall experimental results in RGB



No	Dimensional Image (pixel x pixel)	Image Type	Maximal Number of Characters (alphabet)	Maximal Size of Text (byte)	Initial Image Size (byte)	Steganoraphy Image Size
1	3x3	Grayscale	1	1.125	15.857	16.057
2	5x5	Grayscale	3	3.125	15.876	16.076
3	7x7	Grayscale	6	6.125	16	16.2
4	9x9	Grayscale	10	10.125	16.926	17.126

Table 2 describes the results of the entire experiment on Grayscale digital imagery. There is a dimension of the image in pixels and then it can be known the maximum number of characters in letters that can be inserted. There is also a maximum text size in unedited bytes to know how many characters in the letter can be inserted. This table is also the size of the initial image before the disteganography and image size after the disteganografi in bytes.

So in terms of graph of digital images RGB and Grayscale above, the analysis obtained that the greater the pixel, the greater the number of characters that can be inserted in a picture. Message insertion also does not change the size of an image. But digital images of RGB and Grayscale have differences in the insertion of the number of karatkters. RGB digital images can insert more characters than Grayscale digital images because RGB has 3 channels Red, Blue, and Green.

CONCLUSION

The spread spectrum method has a very high level of security because it has keywords that only the sender and the receiver can know. From insertion with spread spectrum method and experimental and analysis on digital image of RGB & Grayscale, we can get some conclusion as follows.

1. Experimental results and analysis with spread spectrum method before and after disteganografi do not change the image size significantly. With that another person or a hijacker does not suspect a picture.
2. If the image size (pixels) is larger, then the number of characters or messages that can be inserted also more and more. But the number of characters that can be inserted in the RGB digital image is more than the Grayscale digital image.
3. The size of the image does not change significantly, so the image quality also does not change significantly
4. In digital images RGB has 3 channels Red, Blue, Green and Grayscale digital images have only 1 channel, so the number of characters that can be inserted in RGB digital image more than Grayscale digital image with the same pixels.

REFERENCES

[1] Chandramouli, Ramamurti, and Koduvayur P. Subbalakshmi. "Active steganalysis of spread spectrum image steganography." *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*. Vol. 3. IEEE, 2003.

[2] Rajeev Kumar, “Data Hiding Images Using Spread Spectrum in Cloud Computing”, International Journal of Technical Research and Application, Vol. 1, Issue 3, 2013

[3] G.Sudha devi and K.Thangadurai, “High Secure HDWT based Image Steganography and Genetic algorithm based chaotic Encryption”, International Journal of Applied Engineering Research, Vo.10, 2015

[4] Cox, Ingemar J., et al. "Secure spread spectrum

watermarking for images, audio and video." *Image Processing, 1996. Proceedings., International Conference on*. Vol. 3. IEEE, 1996.

[5] Ji, Rongrong, et al. "A new steganalysis method for adaptive spread spectrum steganography." *Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on*. IEEE, 2006.

[6] Marvel, Lisa M., Charles G. Boncelet, and Charles T. Retter. "Spread spectrum image steganography." *IEEE Transactions on image processing* 8.8 (1999): 1075-1083.

[7] Maria Gkizeli, Dimitris A. Pados, Michael J. Medley, "Optimal Signature Design for Spread Spectrum Steganography", IEEE Transactions on Image Processing, Vol. 1, No. 2, 2007.

[8] Ruanaidh, Joseph JK O., and Thierry Pun. "Rotation, scale and translation invariant spread spectrum digital image watermarking." *Signal processing* 66.3 (1998): 303-317.

[9] K. Satish, T. Jayakar, Charles Tobin, K. Madhavi, and K. Murali, "Chaos Based Spread Spectrum Image Steganography", IEEE Transactions on Consumer Electronic, Vol. 50, No. 2, 2004.

[10] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." *ISSA*. 2005.

[11] Lee, Che-Wei, and Wen-Hsiang Tsai. "A new steganographic method based on information sharing via PNG images." *Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on*. Vol. 5. IEEE, 2010.

[12] Ingemar J. Cox, Joe Kilian, F. Thomas Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transcactions on Image Processing Vol. 6, No. 12, 1997

[13] Marvel, Lisa M., Charles T. Retter, and Charles G. Boncelet. "Hiding information in images." *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*. Vol. 2. IEEE, 1998.

[14] T. Sai Sampath and T.S.R. Krishna Prasad, "Hiding of Data in Image using Spread Spectrum Technique", International Journal of Computer Science and Information Technology & Security, Vol. 6,Issue . 4, 2016.