Journal of Engineering and Applied Sciences 14 (13): 4611-4616, 2019
ISSN: 1816-949X

Steganography Analysis on PNG Image RGB Using Spread Spectrum Method

Bogy Oktavianto, Tito Waluyo Purboyo and Randy Erfa Saputra
Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

Abstract: In this study, focusing on the security level in the delivery of confidential information on a media. One technique that can be used is steganography which explains a way to hide the confidential information on a media. As a result, only senders and recipients who are able to know the information without arousing suspicions against others. In this study, we examine the steganography design manually on colour image media which is RGB with PNG format using spread spectrum method and analyse image quality by calculating PSNR value.

Key words: Spread spectrum, steganography, PNG, PSNR, RGB, analysis

INTRODUCTION

Steganography is a technique of inserting a message into a medium in which the secret message to be transmitted is not changed in shape but rather inserted on a cover-object used in life daily (Chandramouli and Subbalakshmi, 2003). New media that has been inserted a secret message (stego-object) and then sent to the recipient without raising the suspicion of the outsider, because the difference from the media (cover-object) with media that has been inserted a secret message (stego-object) can not be realized directly by humans. Steganography at present is done on digital media in the form of image, audio and video. Message saving process requires input media insertion, messages to be inserted and keys (Kumar, 2013). The output of this insertion process is the media that already contains the message. Extraction process messages require media input that contains messages. The output of the message extraction process is a message that has been inserted. This technique makes others unaware that there is important information that we send hidden in other media such as images, audio and video (Satish *et al*., 2014). If the information has been hidden on a media was stolen, the thief is not necessarily able to know the information contained in it, because there is a password (key) to be able to open the information contained in the media information (Rojali *et al*., 2012). The password is known only to the sender and recipient. One method of steganography is spread spectrum.

MATERIALS AND METHODS

Steganography is a technique for hiding personal information with something that results will look like any other normal information. This technique makes others unaware that there is important information that, we send hidden in other media such as images, audio and video. Should the information that has been hidden on a media was stolen, the person who is the thief is not necessarily able to know the information contained in it because there is a password (key) to be able to open the information contained in the media information (Chandramouli and Subbalakshmi, 2003). The password is known only to the sender and recipient. Figure 1 it is clear that the picture before and after the inserted message with stegnography have no significant difference. This can reduce the suspicion of others to the image.

Spread spectrum is a communication method where all communication signals are distributed across the available frequency spectrum. It was originally developed for military and intelligence purposes. The basic idea is to spread information signals over a wider bandwidth to prevent interception of information and other disturbances (Gkizeli *et al*., 2004, 2007). The first developed spectrum spread is known as frequency hopping or frequency jump (Ruanaidh and Pun, 1998). The latest version is the direct squence spread spectrum. Both of these techniques are used in various wireless network products. In addition to other applications such as cordless telephone. A spread-spectrum system must meet the following criteria. On the sender occurs spreading process that spreads the information signal with the help of code signals that are independent of information. At the receiver there is a despreading process involving the correlation between the received signal and the replica signal code generated by a local generator.

Corresponding Author: Bogy Oktavianto, Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

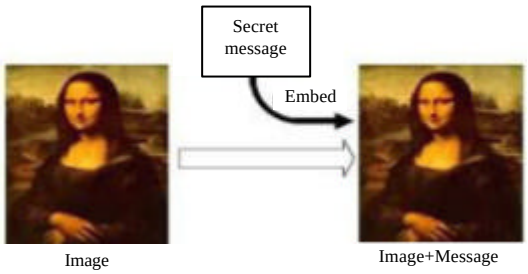


Fig. 1: Image steganography

$$Xn+1 = (aXn+c) mod m \quad (1)$$

Portable network graphics: Initially PNG was developed as an alternative to the GIF format. PNG is best suited for internet graphics because PNG supports transparency and has a beautiful uniqueness that does not exist in other formats such as JPG and GIF. PNG also supports images with color gradients. It can be said that PNG is a combination of JPG and GIF formats. PNG includes 24 bit class format and the transparency is not cracked. Because of that PNG is perfect for making screenshoot. PNG is also able to reproduce detailed desktop images from pixels to pixels. In addition PNG is able to compress images from the photography process without significantly reducing image quality (Cox *et al*., 1996, 1997).

However, PNG also has a weakness that is a large enough size compared to the format JPG and GIF. Also not all browsers support PNG format. Only the latest browsers can accommodate this format, while older browsers mostly do not support PNG. PNG format is suitable for images that have many colors and also if the image sutau will be re-edited without degrading the image quality.

MSE and PSNR: Are used to compare image processing results with preliminary images that have similarities between the two images (Joshi *et al*., 2016). The equation used to calculate these parameters is:

$$MSE = \frac{1}{(N \times M)^2} \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - Y_{ij})^2 \quad (2)$$

Where:

M = PDFHB pixel image of rows
N = Pixel image of coloums
X_{ij} = The intensity of picture before inserted message
Y_{ij} = The intensity of picture after inserted message

MSE is the sigma of the number of errors between the results of image processing with the original image. From the above equation has the following information:

$$PSNR = 10 \log_{10} \left[\left(\frac{1^2}{MSE} \right) \right] \quad (3)$$

The value of PSNR is inversely proportional to the MSE value. Good PSNR value is above 30 dB (decibels).

RESULTS AND DISCUSSION

The result of spread spectrum method: In this analysis will be used images with 3×3 pixel size with RGB color image in PNG format using spread spectrum method on steganography. Figure 2 is a piano image looking for 3×3. Next system will read RGB images with PNG format. Then the system will do the RGB value in decimal form and convert it into binary form as shown.

Red value in decimals:

242	127	154
210	111	59
200	194	184

Green value in decimals:

196	255	194
114	73	97
71	48	178

Blue value in decimals:

100	255	123
94	5	6
59	42	159

The RGB value in decimal form will be converted into binary form. Once changed, then the picture can be inserted message.

Red value in binary:

11110010	01111111	10011010
11010010	01101111	00111011
11001000	11000010	10111010

Green value in binary:

11000100	11111111	0111011
01110010	01001001	01100001
00111011	00101010	10011111

Blue value in binary:

01100100	11111111	01111011
01011111	00000101	00000110
00111011	00101010	10011111

Fig. 2: A piano

First, the system will determine how manycharacters of messages can be inserted in the image in the following way:

$$3\times3\times3\times/8 = 3.375$$

From the validation result, the number of 3×3 pixels can be inserted with 3 characters message count. Examples of messages to be inserted "NAD". Spread spectrum using keywords. The sample keyword used is "s". After that the "NAD" message in ASCII is converted to decimal form then converted to binary form. The result of the message "NAD" = 01001110 01000001 01000100. Then the message will be spread by multiplying 1 on each bit and the result is 01001110 01000001 01000100. After that change the keyword "s" to binary form and the resulting converst is 01110011. After that the result of keyword converst is done XOR process, then get the value in the form of decimal is 227 (Oktavianto *et al*., 2017).

Next is the generation of random numbers using the LCG (Eq. 1). With the value a = 2, c = 7, m = 9, then X1 = (2×227+7) mod 9 = 5. Then, the LCG result will be converted to binary form to 00000101. Then 00000101 will be done XOR process with message like.

Message segment: 01001110 01000001 01000100

Pseudonoise signal: 00000101

Red value after insertuion:
XOP result: 01001011 01000001 01000100

Next, modulation process will be done that is insertion of message in bits of image:

Red value after insertuion:

11110010	01111111	10011010
11010010	01101111	00111010
11001001	11000011	10111010

Green value after insertuion:

11000101	11111110	01111010
01110010	01001000	01100000
00111011	00101010	10011111

Blue value after insertuion:

01100100	11111110	01111010
01011111	01001000	00000110
00111011	00101010	10011111

When the message has been inserted in the image. After that done the extraction process with demodulation or encoding process. The encoding process must use the same keyword to enter the message.

Filter results: 010010110 1000001 01000100

Pseudonoise signal: 00000101

Demodulation result: 0100110 01000001 01000100

Then we will do the de-spread process on the image, which is filtering the final bits of the image to restore or find the hidden message.

01001110 01000001 01000100

From the demodulation and de-spreading results, the message will be read. The message is "NAD". This message is the same as the message inserted, then the process is successful.

The result of MSE and PSNR: In this study will be discussed experiments from MSE and PSNR. Please note, before calculating PSNR then must calculate the value of MSE first. This experiment uses a 3×3 pixel sample. Here, the first step is to compare the binary value of RGB digital image before and after the inserted message.

Red value before insertation:

242	127	154
210	111	59
200	194	186

Green value before insertation:

196	255	194
114	73	97
71	48	178

Blue value before insertation:

100	255	123
94	5	6
59	42	159

The above value is the decimal value of RGB digital image before the message is inserted. After that it is compared with the decimal value of RGB image that has been inserted message. Here's, the decimal value after the message has been inserted:

Green value after insertion:

242	127	154

Green value after insertion:

197	254	122
114	72	96
59	42	159

Blue value after insertion:

100	254	122
95	4	6
58	41	158

The next step is to find the MSE value using the MSE (Eq. 2) by reducing one by one the value of picture before inserted message (X_{ij}) with picture after inserted message value (Y_{ij}). Having obtained the difference in value before and after the message inserted then the value is raised 2 kan. After that summed the results of previous operations. Then divided by the number of rows and columns of the image is 3×3 and the following results are obtained:

$$MSE = \frac{1}{(3\times3)^2}(243-242)^2+(128-128)^2+(155-154)^2+$$
$$(211-211)^2+(110-110)^2+(58-59)^2+(199-198)^2+$$
$$(193-193)^2+(185-185)^2+(255-255)^2+(195-194)^2+$$
$$(193-192)^2+(113-112)^2+(72-72)^2+(96-96)^2+$$
$$(70-70)^2+(47-46)^2+(177-177)^2+(255-254)^2+$$
$$(101-101)^2+(122-122)^2+(122-122)^2+(95-94)^2+$$
$$(4-4)^2+(5-5)^2+(58-59)^2+(41-40)^2+(158-158)^2$$

$$MSE = \frac{1}{(3\times3)^2}(1)^2+(0)^2+(1)^2+(0)^2+(0)^2+(-1)^2+$$
$$(1)^2+(0)^2+(0)^2+(0)^2+(1)^2+(1)^2+(1)^2+(0)^2+(0)^2+$$
$$(0)^2+(1)^2+(0)^2+(1)^2+(0)^2+(0)^2+(0)^2+(1)^2+(0)^2+$$
$$(0)^2+(-1)^2+(1)^2+(0)^2$$

$$MSE = \frac{12}{(3\times3)^2}$$

$$MSE = 0.135$$

After obtaining the MSE results, then calculate the value of PSNR (3) in the following way:

$$PSNR = 10\log_{10}\left(\left[\frac{255^2}{0.135}\right)\right]$$

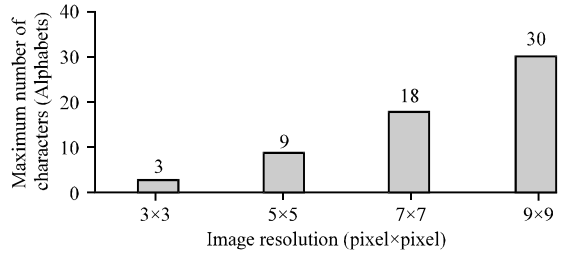
$$PSNR = 56.827$$

Therefore, after the calculation results obtained value of MSE = 0.135 and PSNR = 56.827 dB. Since, the MSE value is close to zero, both images have similarities and the PSNR value is above 30 dB, the similarity level can be said to be high.

Analysis steganography: Figure 3 capacity of messages on different images. Figure 3 explains that the larger the pixel size in the image, the greater the capacity of the message characters in the image. Figure 4 can be seen the size of the image in bytes and the number of messages that can be inserted.

Table 1: Data on overall PSNR and MSE experimental results

Dimension image (pixel×pixel)	Size of image cover (byte)	Size of image steganography (byte)	Size of character (alphabet)	MSE (1/(nm)^2 Σ (x-y)^2)	PSNR (log 10 1/MSR) (dB)
3×3	15.213	15.213	3	0.1480	0.8293
5×5	15.266	15.266	3	0.0192	1.7170
7×7	15.340	15.340	3	0.0110	1.8110
9×9	15.444	15.444	3	0.0134	2.0110



3: Capacity of max text size in image

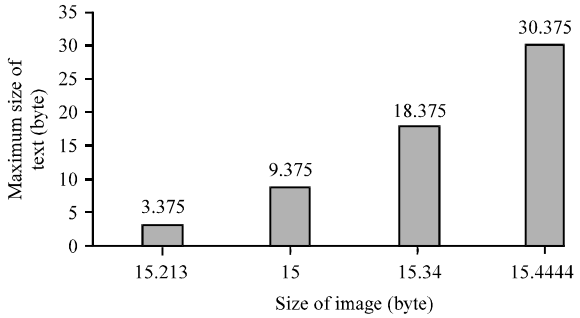


Fig. 4: Capacity of max text size in image

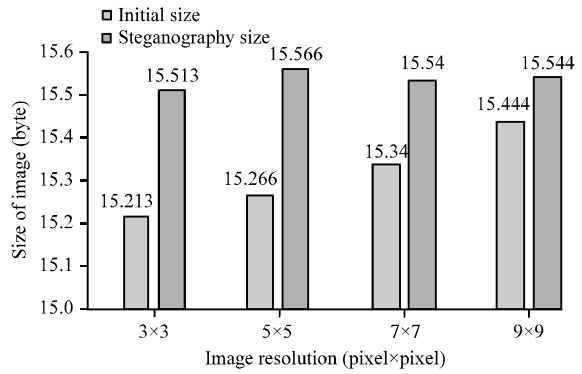


Fig. 5: Dimension image and value of PSNR

Figure 5 describes the image size in bytes when before and after a message has been inserted. The comparison of the size obtained did not change significantly. So, with this can reduce the suspicion of others to the image. The larger the image pixel size, the more number of characters can be inserted.

In Table 1 and Fig. 6, describes the overall data of PSNR and MSE obtained from several dimensions of the image dimension. From the picture it can be concluded that if the pixel of the picture is bigger,

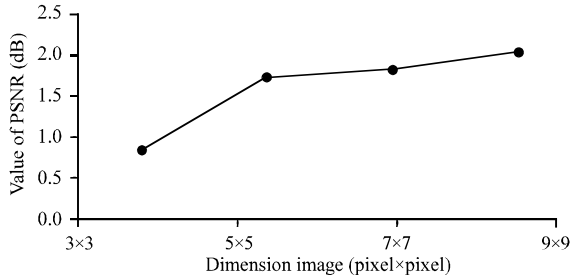


Fig. 6: Dimension image and value of PSNR

then the bigger the value of PSNR. And if the MSE value is getting smaller, the greater the value of PSNR. MSE values close to zero have a high degree of similarity.

CONCLUSION

We can get some conclusions as follows. The larger the image pixel size, the more number of characters the message can insert. Comparison of image size in bytes after and after inserted message does not experience big difference. The image quality after and before the inserted message has not changed significantly. So, do not arouse suspicion of others to the picture. A good PSNR score is above 30 dB to get a very high level of image resemblance spread spectrum methods on steganography have a good level of security with the results of the analysis.

REFERENCES

Chandramouli, R. and K.P. Subbalakshmi, 2003. Active steganalysis of spread spectrum image steganography. Proceedings of the International Symposium on Circuits and Systems, May 25-28, 2003, Bangkok, Thailand, pp: 830-833.

Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.

Cox, I.J., J. Kilian, T. Leighton and T. Shamoon, 1996. Secure spread spectrum watermarking for images, audio and video. Proceedings of the 1996 International Conference on Image Processing Vol. 3, September 19, 1996, IEEE, Lausanne, Switzerland, pp: 243-246.

Gkizeli, M., D.A. Pados and M.J. Medley, 2004. SINR, bit error rate and Shannon capacity optimized spread-spectrum steganography. Proceedings of the 2004 International Conference on Image Processing (ICIP'04) Vol. 3, October 24-27, 2004, IEEE, Singapore, pp: 1561-1564.

Gkizeli, M., D.A. Pados and M.J. Medley, 2007. Optimal signature design for spread-spectrum steganography. IEEE. Trans. Image Process., 16: 391-405.

Joshi, K., R. Yadav and S. Allwadhi, 2016. PSNR and MSE based investigation of LSB. Proceedings of the 2016 International Conference onComputational Techniques in Information and Communication Technologies (ICCTICT), March 11-13, 2016, IEEE, New Delhi, India, ISBN:978-1-5090-0082-1, pp: 280-285.

Kumar, R., 2013. Data hiding images using spread spectrum in cloud computing. Intl. J. Tech. Res. Appl., 1: 76-79.

Oktavianto, B., T.W. Purboyo and R.E. Saputra, 2017. A proposed method for secure steganography on PNG image using spread spectrum method and modified encryption. Intl. J. Appl. Eng. Res., 12: 10570-10576.

Rojali, R., A.G. Salman and T. Nugraha, 2012. [Steganography application program using spread spectrum method on Android-based mobile device (In Indonesian)]. ComTech. Comput. Math. Eng. Appl., 3: 762-773.

Ruanaidh, J.J.O. and T. Pun, 1998. Rotation, scale and translation invariant spread spectrum digital image watermarking1. Signal Process., 66: 303-317.

Satish, K., T. Jayakar, C. Tobin, K. Madhavi and K. Murali, 2004. Chaos based spread spectrum image steganography. IEEE Trans. Consumer Electron., 50: 587-590.