Journal of Engineering and Applied Sciences 15 (1): 247-251, 2020
ISSN: 1816-949X

A Comparison of Steganography in the GIF Image using LSB and Spread Spectrum Method

Andika Amirulhaqi, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni
Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

Abstract: Graphics Interchange Format (GIF) is a graphics format that is most often used for the purposes of website design. The GIF has a bit more color combinations than JPEG but able to store graphics with background transparent or in the form of a simple animation. Because of the ability possessed by the GIF that is could make an animated GIF from any number of images, it is sometimes still considered to be good to use when to want to download loads of sources in large sizes, then the GIF image can be shown in advance, so that, users don't feel strange when the load occurs. The GIF image has a specific format that has the color map containing as many as 255 entries and entry consists of a number of images in the GIF animations or one image if not an animation. Spread Spectrum method of treating the cover-image as both a noise (noise) or as an effort to add artificial noise (pseudo noise) into the cover image. On a method of steganography with Least Significant Bit (LSB) of the image to GIF images, basically, consist of a part of the image, so that, it can be applied with LSB method inserts a message in the LSB of each byte of an image from the image. Both of these methods certainly have advantages and disadvantages of each. One of the advantages of each method of spread spectrum is on better security compared with the method of Least Significant Bit (LSB). While the algorithm of least significant bit was to allow the message size in the embed dynamic depending on the size of the GIF image. In addition, in terms of the calculation of the peak signal-to-noise ratio and speed of embed course will also differ on the use of both methods.

Key words: GIF, steganography, spread spectrum method, pseudonoise, least significant bit method

INTRODUCTION

Now hide the message not only can be done by disguising the message. But it can also insert those messages in other media. So, people would not be suspicious of the message we send because the message is not visible, the look is simply a media holding our messages.

For example, we want to send a message to someone who is far away by email. Fearing our message known to others then we insert the message in a media that is larger. For example, in the media image file. So that, other people will not suspect will be the image that we send. This is certainly going to be more practical than we are sending the message in the form of a file that is encrypted. This is certainly going to make others suspicious and started doing the attack to find out the contents of the message that we send (Morkel *et al*., 2005a, b).

The technique of insertion messages in other media larger named steganography. A storage medium that can be used in steganography can be files of songs, images or other files that are large and can put the message that we want to hide (Morkel *et al*., 2005a, b).

By using steganography then people will not become suspicious if it turns out we are sending a secret message. But there is a price to be paid in steganography, i.e., magnitude file size stuffed secret messages. We need to transfer large amounts of data but important data required only small sized.

MATERIALS AND METHODS

Steganography: Steganography is a technique to hide information that is personal with something that the result will look like other normal information. The medium used is generally a different media with media bearer of confidential information where this is a function of technique of steganography using disguises techniques as other media are different so that confidential information in the initial media is not clearly visible (Morkel *et al*., 2005a, b).

GIF image: Graphics Interchange Format (GIF) is a format that is often used in the world of web as well as in the world of digital imagery. This format is often used because of its small relative size and also the number of image editor software that has supported this image. The GIF is small because it limits the color to 256 colors to save the file size (Munir, 2016).

Corresponding Author: Andika Amirulhaqi, Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

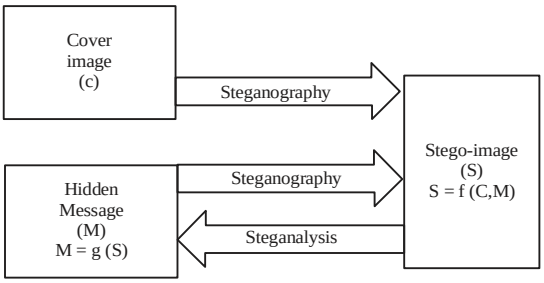

Fig. 1: Steganography process

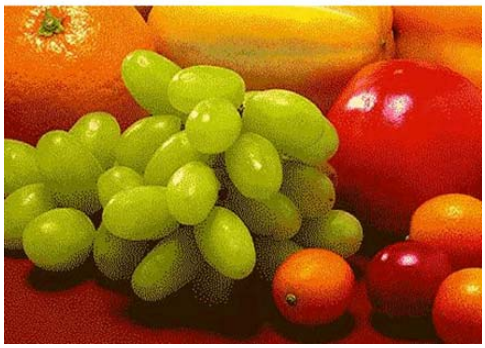

Fig. 2: Image with GIF format

Fig. 3: Image with JPEG format

Clearly visible in the above two images that image with the GIF format has a bad outcome when compared to the JPG format in Fig. 2 and 3.

Least Significant Bit (LSB): Method of a least significant bit is the standard method that is widely used to perform steganography, especially on digital image media changes one bit at least significant bit will not result in a color change that is large enough, so as not too visible are visible by others (Fridrich *et al*., 2001).

This method uses the least significant bit of the byte-byte on a digital media substitution with one bit-one-bit message is inserted, so that, the size of files that can be stored is likely to be much smaller than the original size of a digital image. The extraction process of this method can be done by arranging bits-bits of the image foisted on forming a message that has been inserted (Fridrich *et al*., 2001).

However, if the insertion is done on a byte-byte data sequentially, it will be easy for others to extract messages inserted because the person simply crafts a bit-bit byte and the end of all chances of getting the text the easier it is. The steps of the method of a least significant bit are (Akhtar *et al*., 2017):

- Read GIF files
- Do some checking to find the position of the image block
- Generate a random value between {1.5}, so, the next position is between 1-5 bytes from the byte positions now
- Insert the bit at the least significant bit in the byte
- Repeat steps 3 and 4 until all of the bits of the message pasted already inserted at random
- Save back into the new file

Spread spectrum: Spread spectrum method is a technique of transmission using pseudonoise code, that are independent of the data information as the modulator wave form to spread the energy signal in a communications line (bandwidth) that greater lines of

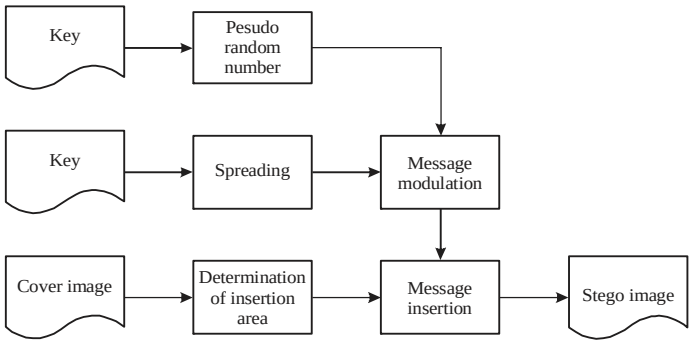

Fig. 4: Scheme of massage insertion

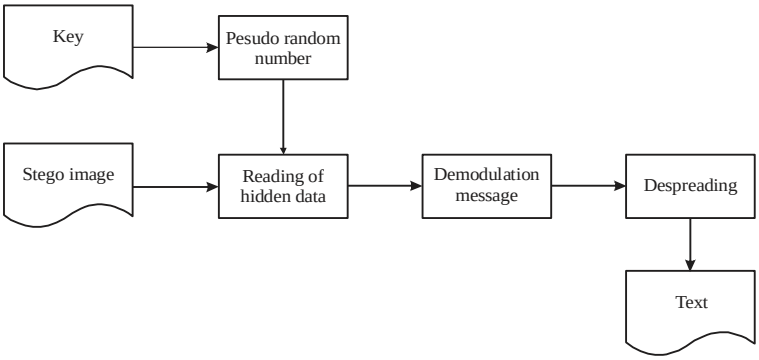

Fig. 5: Scheme of massage extraction

communication signal information. By the receiver, the signal is collected again using pseudonoise code synchronized replica. Based on the definition, it can be that steganography using spread spectrum method of treating the cover-image as both a noise (noise) or as an effort to add artificial noise (pseudonoise) into the cover-image (Marvel *et al*.,1999).

The process of insertion of messages using the spread spectrum method consists of three processes, namely the spreading, modulation and insertion of a GIF image to the message. While the extraction process the message using the spread spectrum method consists of three processes, i.e., the retrieval of messages from the matrix of frequencies, demodulation and de-spreading (Chandramouli and Subbalakshmi, 2003).

Measurement error: The measurement of the quality of the image has been inserted the message done subjectively and objectively. Subjective measurement done by visually see the difference the shape and color of the image has been inserted with that yet. Measuring objectively the human rate visualizations are used by calculating the value of PSNR (Peak Signal to Noise Ratio). PSNR values in units of decibels (dB) are counted according the equation:

$$PSNR = 10 \times \log_{10}\left(\frac{MAX^2}{MSE}\right)$$

where, MSE values (Mean Square Error) obtained from the equation:

$$MSE = \frac{1}{mn}\sum_{t=0}^{m-1}\sum_{j=0}^{n-1}\left\|\left\|I(i,j) - K(i,j)\right\|\right\|^2$$

MSE equation requires two input images and then look for its value. After that calculated the value of PSNR. PSNR values are reasonable on the comparison of two image file is above 30 dB (Morkel *et al*., 2005a, b).

Table 1: Sample GIF image

Images	Image size (pixel)
	4×4
	6×6
	8×8
	10×10
	12×12

RESULTS AND DISCUSSION

Experiments: In this chapter, the experiment would be conducted against the two methods of steganography.

Least Bit Spectrum (LSB) method: In this experimental individually focused on testing how the maximum number of characters or the length of a message that can be inserted into a gif image using the method of Least Significant Bit (LSB). The way used to obtain maximum message length the results using the method of calculating with the formula:

$$P = \frac{m \times n \times 1}{8}$$

The calculation formula of obtained data the results of the experiments has been performed using the 5 sample image gif with different image size in the following Table 2.

Spread spectrum method: In this experimental individually-focused on testing how the maximum number of characters or the length of a message that can be inserted on a gif image using spread spectrum method. The way used to obtain maximum message length the results using the method of calculating with formula.

Checking of PSNR and MSE value: After checking the value of PSNR and MSE by inserting the character ‘n’ and ‘o’ then obtained the following results.

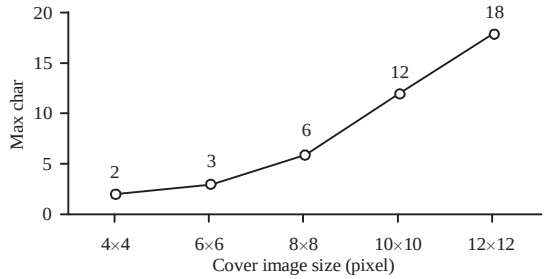

Fig. 6: Graph of cover image size vs. maximum char using LSB method

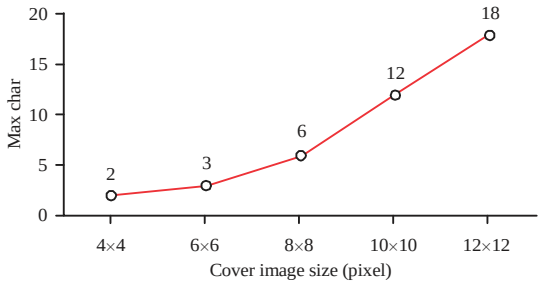

Fig. 7: Graph of cover image size vs. maximum char using spread spectrum method

Table 2: Experiment results using the spread spectrum method

Image size (pixel)	No. of char
4×4	2
6×6	3
8×8	8
10×10	12
12×12	18

Table 3: The results of experimental calculations of PSNR and MSE

Image size (pixel)	No. of char	MSE	PSNR
4×4	2	0.3125	58.23380318
6×6	2	0.222222222	61.19505388
8×8	2	0.15625	64.25440309
10×10	2	0.08	70.06900387
12×12	2	0.076388889	70.47019975

Analysis: From the results of previous experiments against gif image about how much the message maximum number of characters that can be inserted by the method of Least Significant Bit (LSB) and also the spread spectrum method, then the maximum number of characters can be seen from both that method on the following Fig. 6.

And then experiments against gif image about how much the message maximum number of characters that can be inserted by the spread spectrum method, then the max number of characters can be seen from Fig. 6.

Figure shows that the blue line illustrates the method of LSB, whereas a red line depicting the spread spectrum method. From Fig. 6 and 7 can be seen that the maximum number of characters that can be inserted using the LSB method and method of spread spectrum in the same magnitude. It happened because in calculation formulas in use in finding the length of the message is the same, the difference method of the least significant bit with spread spectrum method is in terms of the image will be inserted when processing the message. On the methods of LSB data to be inserted directly inserted into the picture without processed while the at a spread spectrum method of data that will be on the insert must be in advance processed through XOR.

From the level of security is clearly spread spectrum method is more secure compared with the method of least significant bits because already in explain earlier that spread spectrum methods on the data that you want to insert in the process first before inserted. So, others will be more difficult to decipher the message in a picture that has been in the sport with a spread spectrum method.

From the results of checking the value of the MSE and PSNR in getting results either, value of PSNR>30 dB, then it can be said that the performance of image restoration is nice. If the value of PSNR>50 dB then it can be said that the performance of the image of the perfect restoration results approaching the original image.

CONCLUSION

The conclusion that can be drawn from the experiment and analysis as well as the discussion towards how much the number of characters that can be inserted into the application of steganography using method of Least Significant Bit (LSB) and the method of spread spectrum is the number of characters that can be inserted in the same.

But in terms of security is clearly spread spectrum method is more secure compared with the method of least significant bits because the method of spread spectrum data in the insert in the first process that is inserted before the XOR process compared to the method of least significant bits that directly inserts a message without processing it first. So, others will be more difficult to decipher the message in a picture that has been in the sport with a spread spectrum method.

From the results of checking the value of the MSE and PSNR in getting results either, value of PSNR>30 dB, then it can be said that the performance of image restoration is nice. If the value of PSNR>50 dB then it can be said that the performance of the image of the perfect restoration results approaching the original image.

REFERENCES

Akhtar, N., V. Ahamad and H. Javed, 2017. A compressed LSB steganography method. Proceedings of the 2017 3rd International Conference on Computational Intelligence and Communication Technology (CICT), February 9-10, 2017, IEEE, Ghaziabad, India, ISBN:978-1-5090-6219-5, pp: 1-7.

Chandramouli, R. and K.P. Subbalakshmi, 2003. Active steganalysis of spread spectrum image steganography. Proceedings of the 2003 International Symposium on Circuits and Systems ISCAS'03 Vol. 3, May 25-28, 2003, IEEE, Bangkok, Thailand, pp: 830-833.

Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. IEEE Multimedia, 8: 22-28.

Marvel, L.M., C.G. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE. Trans. Image Proc., 8: 1075-1083.

Morkel, T., J.H. Eloff and M.S. Olivier, 2005a. An overview of image steganography. Proceedings of the 5th Annual Conference on Information Security South Africa, June 29-July 1, 2005, ISSA, Sandton, South Africa, pp: 1-11.

Morkel, T., J.H.P. Eloff and M.S. Olivier, 2005b. An overview of image steganography. Proceedings of the 5th Annual Information Security South Africa Conference, June 29-June 1, Sandton, South Africa, pp: 1-12.

Munir, R., 2016. Application of the modified EzStego algorithm for hiding secret messages in the animated GIF images. Proceedings of the 2016 2nd International Conference on Science in Information Technology (ICSITech), October 26-27, 2016, IEEE, Balikpapan, Indonesia, ISBN:978-1-5090-1722-5, pp: 58-62.