Journal of Engineering and Applied Sciences 15 (2): 373-379, 2020
ISSN: 1816-949X

Analysis of Steganography on TIFF Image using Spread Spectrum and Adaptive Method

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

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 the system. The hidden message technique called steganography is a technique that allows users to hide a message in another message. We can use steganography to protect confidential data or information. This study will discuss about spread spectrum and adaptive method on Temporary Instruction File Format (TIFF). By using these methods, we compare how many characters from each method can be inserted in to TIFF image. Analysis using PSNR and MSE are also presented in this study.

Key words: Steganography, spread spectrum, adaptive method, TIFF, presented, information

INTRODUCTION

The rapid development of technology makes it easy for the human to do something because technology can shorten the distance and time. In the field of technology such as computers and the internet, many people are using and utilizing technology. One obvious example of the use and utilization is the amount of information transmitted over the internet network. Of course, sending information via. the internet is very profitable because in addition to fast, low cost. But on the other hand, there is also a weakness that is information that can be sent easily and not aware of the owner of the information, stolen by people who are not responsible for the data or information.

Steganography is not a new term but has been used thousands of years ago. This is a technique for allowing two or more people to silently communicate with each other by hiding any secret message on a media cover. Files used as media can be text, audio, image or digital video formats. The secret message embedded in the media cover using the appropriate algorithm and demanding the stego file itself to be sent to the receiver. There are some important things to be kept in mind before applying or performing the procedure of steganography:

Embedding capacity: Data is embedding in a larger data called cover or carriers file. The carrier that used is computer files such as image, audio, video even text files without affecting its original quality. The embedded capacity is the amount of data can be hidden or embedded on the cover and will be compared to the cover size because if the size of data that will be inserted on the cover is greater than the cover size then steganography can't be done (Johri *et al*., 2016).

Undetectability: Data should be hidden or embedded into a carrier file in such way that any secret message or information can't be seen accidentally in the original file by anybody. If anyone detects the message in the original file then the steganography is failed (Johri *et al*., 2016).

Robustness: This is the capability of the embedding algorithm to store embedded data even after going through the process of compression and decompression a file (Johri *et al*., 2016).

Security: In most cases, security including perceptional transparency of the hidden data is considered the most important issue of hiding data in many different formats. The definition of security in steganography cases is as likely to be embedded secret messages unknown to outsider people that have no connection between sender and recipients.

Tamper resistance: Resistance to intentional malfunction or sabotage of a product or system by users that have access to it. There are many reasons why tamper resistance is so, important. One of the important things for steganography is how strong the carrier file that used for embedding a secret message or file will not easy to be cracked by users. The purpose of this research is to find out how many character that can be inserted into the TIFF image of the media using spread spectrum and adaptive method. The study has limits on the following issues:

Corresponding Author: Aryfandy Febryan, Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung indonesia

- Concealment of a secret message is done by the method of spread spectrum and adaptive
- The file or secret message is hidden in form of a character or text
- The image is used as the carrier's image or stego image of the digital image with TIFF format

MATERIALS AND METHODS

Steganography methods: This study will be discussing about the TIFF digital image, spread spectrum and adaptive method.

TIFF image: The TIFF format is the best image format with its meaning all data and information (RGB data, CMYK data and others) related to manipulation of images that are not lost. The usual TIFF format is used for printing needs with very high image quality. Font size for format this is usually very large this format is capable of storing images with quality up to 32 bits. The TIFF file format can also be used for inter-platform streaming purposes (PC, macintosh and silicon graphic). In addition, this format is easy to use for transfer between programs almost all programs are able to read bitmap file formats as well capable of reading TIFF format file TIFF format using LZW compression algorithm (Kim *et al*., 2017).

Spread spectrum: Spread spectrum method is a technique that using pseudo noise code that is independent of the data information as the modulator waveform to spread the energy signal in a communications line (bandwidth) that greater lines of communication signal information. By the receiver, the signal is collected again using pseudo noise 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 (pseudo noise) into the cover image.

The following overview of calculations going on in spread spectrum method. On the process of encoding can be described as follows. With a picture with JPEG format, the content of the message "test", the keyword "sonny". The function will read the message entered and checked the size of messages that are included are smaller than the size of the image on that is plugging into the eqution:

$$\text{Length of message} = \left((\text{message size}+28)*4*8\right)$$

Number 28 is to tag marking on an image that is already inserted, number 4 is a large multiplier for the dissemination of useful bits and the number 8 is a bit of the image. After checking my file size is completed then do checking of the image size, the used steganography method and keywords, if these terms all have met continued into the process of insertion. Before insertion is performed, the function will read the image and take a header of a JPEG image prepared in advance, then a picture of the body that will be inserted later into the message. Before the deployment process does is change the message to binary form. The result of converting binary from the message "test" is 01110100 01100101 01110011 01110100. Then binary messages scattered with scalar magnitudes multiplier his four, so that, it will produce new segments, namely:

- 00001111111111110000111100000000
- 00001111111100000000111100001111
- 00001111111111110000000011111111
- 00001111111111110000111100000000

Then the next step is the generation with the generation seedlings pseudonoise is determined based on the keyword "sonny". After getting the value of the keyword (101) that value is used as the initial seed the random number generation. Calculation of random number generation in accordance with the random number generation LCG eqution is as follows:

$$Xn+1 = \left(a * Xn+c\right) \bmod m$$

$$a = 17,\ c = 7,\ m = 84$$

Where:
Xn : An integer n calculation is as follows.
X1 : (17*101+7) mod 84, X1 = 44
X2 : (17*44+7) mod 84, X2 = 83
X3 : (17*83+7) mod 84, X3 = 74

And so on for X4, X5, X6, X7, X8, ..., Xn. For example do five times the dissemination of results and the result is "44 83 74 5 8" if modified in binary form into "00101100 01010011 01001010 00000101 00001000". To get the modulation, a segment of the message will either signal is modulated with a pseudonoise function XOR (Exclusive OR).

Message segment:

- 00001111111111110000111100000000
- 00001111111100000000111100001111
- 00001111111111110000000011111111
- 00001111111111110000111100000000

Pseudonoise signal:

- 00101100010100110100101000000101000010000

Then the results of the process of modulation between segment message with the pseudonoise signals using the XOR function is:

- 00100011101011000100010100000101
- 00000111111100000000111100001111

- 00001111111111111000000011111111
- 00001111111111111000011110000000

The result of the modulation process which will be inserted into the bits images. For example, suppose that taking ten pixels from the image and take thirty the first bit of the message and the segment between modulation pseudonoise signals.

- Red = 180 181 185 182 181 183 186 184 184 187
- Green = 166 172 174 171 170 173 176 174 176 179
- Blue = 163 169 172 169 168 171 175 173 174 177

Then converted to binary and inserted between the modulation process results segment message with the pseudonoise signals be as follows. The step continues until the modulation between segments of the message and signal pseudonoise inserted all. The last process after last insertion process is the return header, so that, the image is not damaged.

On the process of the extraction process is the opposite of the encode. Select the picture that will be extracted, use the same keywords as the encode "sonny". The first step is to read the image if the image has already been inserted by the message or not. If not yet then a function header will take pictures first, next on the body pictures did screening process in order to get a bits result of modulation. The results of the screening process are done will get bits is as follows:

- 00100011101011000100010100000101
- 00000111111100000000111100001111
- 00001111111111111000000011111111
- 00001111111111111000011110000000

After all bits modulation results obtained, then conducted the process of with demodulation pseudonoise signals of the same keywords on the process of modulation in order to gain bits correlated. Results filtering:

- 00100011101011000100010100000101
- 00000111111100000000111100001111
- 00001111111111111000000011111111
- 00001111111111111000011110000000

Pseudonoise signal:

- 00101100010100110100101000000101000010000

Demolation result:

- 00001111111111111000011110000000
- 00000111111100000000111100001111
- 00001111111111111000000011111111
- 00001111111111111000011110000000

The next process that is dividing the four results of demodulation which is useful for shrinkage results demodulation into the actual content of the message. The process of shrinkage (de-spreading) these segments become:

- 01110100 01100101 01110011 01110100

The end result "01110100 01100101 01110011 01110100" is a segment of the same message when hidden in the encoding. The results are then converted to the form of the character would be a "test".

Adaptive method: Steganography information by means of the insertion of the LSB is performed on a bit-the most insignificant bits of a pixel image, so as not to cause a difference in sensing with the human eye. However, steganography does not have enough resilience and easily damaged when facing the digital image processing operations carried out such as lowpass filtering.

Therefore, to create more robust against attacks steganography, steganography preferably implanted on bits more significant. This has led to a kind of trade-offs because the stylish image steganography produced will look a lot of distortion and contrary to the needs of the unseen by the eye senses. To qualify the solidity and transparency, then inserted steganography adaptively by modifying the intensity of certain pixels as much as possible and are not visible to the human eye.

In the process, the adaptive method utilizing sensitivity of human vision system by modifying the level of intensity of the pixels of a digital image block adaptively. In addition to maintaining the level of transparency of steganography in digital imagery, this technique is also reliable in the face of digital image processing in general like cropping, scaling, rotation, low-pass filtering or lossy compression. The technique of insertion of messages on steganography techniques can be categorized into two categories, namely:

The technique of adaptive process message insertion of nontechnique nonadaptive not correlating feature on media insertion with a message that will be inserted in the case of images. An example is the insertion with the LSB method inserts a message bits randomly in the media insertion.

The technique of adaptive process of insertion of messages on adaptive technique modification media insertion process that occurs at the insertion of the message be correlated with features and image content. This technique of analyzing and selecting pixels that will be inserted into a message and the pixels which will be pasted depends by the media insertion. An example of this technique can avoid the areas in the image that has the same color (solid color) and so this technique will select pixel based on parity of pixels that will be inserted into the message is compared to the value of the parity of the message will be inserted.

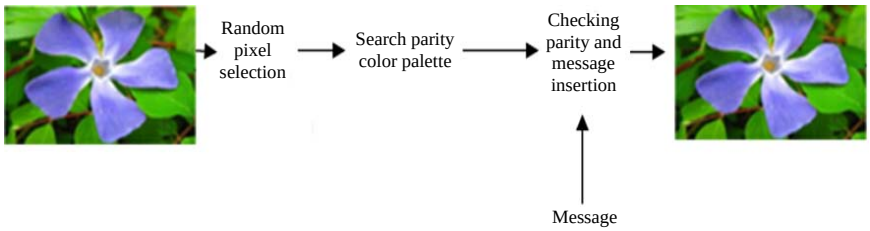

Fig. 1: The concealment of messages with the adaptive method (Singh and Singh, 2014)

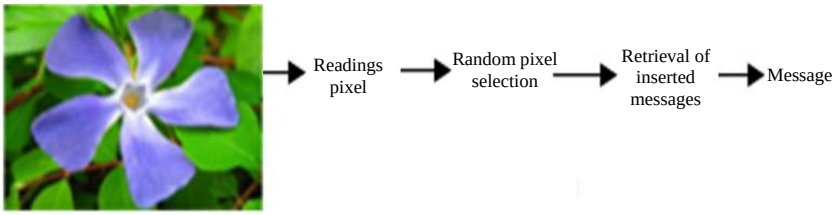

Fig. 2: The message extraction using adaptive method (Singh and Singh, 2014)

The adaptive method is a method that uses the techniques of adaptive insertion techniques as his message. This method has the advantage that is on a high level of security for steganography in palette-based images (palette-based image), GIF and PNG images. This method will analyze and select pixels that will not produce a great suspicion by the change of color values, for example, this method will avoid inserting a message in an area that has the same color in an image. On the image of the TIFF, adaptive method is called because the insertion and modification of the pixel, this method will select the colors available in the color table of the inserted image message. Because each TIFF image has a color table content.

This method of message insertion capacity depends on the insertion of media and in some cases, the capacity of a message that can be inserted in an image and in all insertion cannot be calculated before the insertion process began but can still be conducted analysis about the maximum capacity of the inserted message using the adaptive method. The workings of the adaptive method is shown in Fig. 1 on the insertion process begin with the selection of pixels that will be inserted by pseudo random messages. The process of inserting a message in TIFF image using adaptive method is as follows:

The pixel will be inserted a message selected at random from the set of all pixels in the image file. Then the color palette will be determined the bit using parity equation R+G+B mod 2 (Shetye *et al*., 2016). After that held checking each pixel and compare the parity of each pixel with a bit of the message. If the resulting equation of bit, then the pixel is not modified and continues checking the next pixel. If a pixel selection does not occur will be inserted randomly. A search of parity of color palette. The selection of a pixel will be inserted randomly. Original image stego-object messages 16-bit difference, then the color of the pixel in the modification by way of searching for the nearest neighbors of color have the same parity on the color palette.

If the modification process completes, then checking in continue on the next pixel. The procedure of inserting a message ensures that the collections of blocks on the original image and image files that are already on the modifications are identical. This allows the detection algorithms to restore messages from the parity of color by way of performing a search on the pixels in a pseudo random pattern similar to that of a pixel selection message will be inserted at the insertion process. The extraction process the messages which can be seen in Fig. 2 is the opposite of the order in the process of inserting a message in GIF image. At first the story already inserted a message will be read and the pixel will be read and selected at random, using pseudo pseudo random pattern that is similar to the pattern at the time of insertion of the message. After pixel containing a message is identified, then the message can be inserted will be taken.

Error measurement: The measurement of the quality of the image has been inserted the message done subjectively and objectively. Subjective measurement done by visually sees the difference the shape and color of the image have been inserted with that yet (Gupta and Dhanda, 2015).

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 to the equation:

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

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

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

Description:

- F : represents the matrix data of our original image
- G : represents the matrix data of our degraded image in question
- M : represents the numbers of rows of pixels of the images and i represents the index of that row
- N : represents the number of columns of pixels of the image and j represents the index of that column
- MAX : the maximum signal value that exists in our original "known to be good" image

MSE equation requires two input images and then looks 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.

Because of the image of the logo of the paste in the form of binary image format, then the measurement against attacks on stego images used the calculation of Bit Error Rate (BER). The smaller value the results of calculation of BER, then the better the quality of the resulting image. Calculation of the BER is calculated by the following equation:

$$BER\ S, S' = \frac{\sum Pi}{N}$$

Where:

S : The original
S' : Steganography is steganography extracted
N : The number of bits and the value of pi is defined as follows

$$pi = 1 \text{ for } Si \neq Si'$$
$$pi = 0 \text{ for } Si = Si'$$

The test is said to be successful if each way, the obtained results using adaptive method that has been implemented in accordance with the following equation:

$$P = \frac{mxn}{8}$$

Where:

p : Message size
m : Length of the image size in pixels
n : Size of image width in pixels

RESULTS AND DISCUSSION

In this study, it is explained the results of spread spectrum, adaptive method and PSNR and MSE stego image at the same time is given the comprehensive discussion (Table 1).

Table 1: Experimental results using spread spectrum

Image size (pixels)	No. of characters
4×4	8
6×6	18
8×8	32

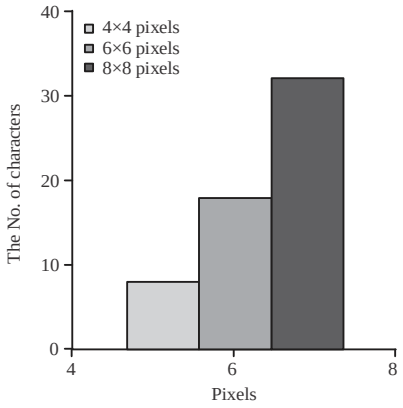

Fig. 3: A maximum No. of characters that can be inserted into CMYK pixels

Steganography using spread spectrum: Figure 3 is a graph that show how many characters that can be inserted to each pixels. Example in 4×4 pixels the maximum characters that can be inserted is 8 characters, 6×6 pixels maximum characters that can be inserted is 18 characters and in 8×8 pixels maximum characters that can be inserted is 32 characters.

A picture with TIFF format, the content of the message is "test", the keyword "aja". The result of converting binary from the message "test" is :

- t : 0111 0100
- e : 0110 0101
- s : 0111 0011
- t : 0111 0100

Then binary messages scattered with scalar magnitudes multiplier his four, so that, it will produce new segments, namely:

- 00001111111111110000111100000000
- 00001111111100000000111100001111
- 00001111111111110000000011111111
- 00001111111111110000111100000000

Then the next step is the generation with the generation seedlings pseudonoise is determined based on the keyword "aja":

- a : 0110 0001
- j : 0110 1010
  0000 1011
- a : 0110 0001
  0110 1010→106

After getting the value of the keyword (106) that value is used as the initial seed the random number generation. Calculation of random number generation in accordance with the random number generation LCG equation is as follows:

$$X(n+1) = (a * Xn+c) \bmod m$$

$$a = 2, c = 7, m = 15$$

Where:
Xn : An integer n calculation is as follows.
X1 : (2*106+7) mod 15, X1 = 14
X2 : (2*14+7) mod 15, X2 = 5
X3 : (2*5+7) mod 15, X3 = 2
X4 : (2*2+7) mod 15, X4 = 11

For example do four times the dissemination of results and the results is " 14 5 2 11", then modified into binary and it will become "00001110 00000101 00000010 00001011". A segment of the segment is modulated with a pseudonoise function XOR (Exclusive OR):

Message segment:

- 00001111111111111000011110000000
- 00001111111110000000011110001111
- 00001111111111111000000011111111
- 00001111111111111000011110000000

Pseudonoise signal:

- 00001110000001010000001000001011

Result:

- 00000000111110100000110100001011
- 00000001111101010000110100000100
- 00000001111101010000001011110100
- 00000001111101010000110100001011

The result of modulation process is inserted into the bits of image. For example, take the eight pixels from the image and take the thirty-two the first bit of the message and the segment will be modulation with pseudonoise signals.

- C = 171 133 172 127 82 0 91 73
- M = 187 107 181 125 60 30 94 79
- Y =146 109 154 108 33 44 97 76
- K = 255 255 255 255 255 255 255 255

Then, converted to binary and inserted between the modulation process results segment message with the pseudonoise signals be as follows (Table 2).

The step continues until the modulation between segments of the message and signal pseudonoise inserted all. The last process after last insertion process is the return header, so that, the image is not damaged.

Table 2: Modulation process results segment message with the pseudonoise signals

Cyan	Magenta	Yellow	Key
10101010	10111010	10010010	11111110
10000100	01101010	01101100	11111111
10101101	10110101	10011011	11111111
01111111	01111100	01101101	11111110
01010010	00111100	00100000	11111110
00000001	00100101	00101100	11111111
01011010	01011110	01100000	11111110
01001001	01001110	01001101	11111111

On the process of the extraction process is the opposite of the encode. Select the picture that will be extracted, use the same keywords as the encode "aja". The first step is to read the image if the image has already been inserted by the message or not. If not yet then a function header will take pictures first, next on the body pictures did screening process in order to get the bits result of modulation. The results of the screening process are done will get bits is as follows:

- 00000000111110100000110100001011
- 00000001111101010000110100000100
- 00000001111101010000001011110100
- 00000001111101010000110100001011

Pseudonoise signal:

- 00001110000001010000001000001011

Demolation result:

- 00001111111111111000011110000000
- 00001111111110000000011110001111
- 00001111111111111000000011111111
- 00001111111111111000011110000000

The next process that is dividing the four demodulation result which is useful for menyusutkan results demodulasi into the actual content of the message. The process of shrinkage (de-spreading) these segments become:

"01110100 01100101 01110011 01110100" the result is the same message when hidden in encoding.

Steganography using adaptive method: In this study, individually-focused on how much the maximum number of characters or the length of a message that can be inserted into cmyk image. The methods used to obtain the results of the use of manual calculations with eqution:

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

Retrieved data results from experiments that have been done before with to find out what the maximum

Table 3: Experimental results using adaptive methods

Image size	No. of characters
4×4	2
6×6	4
8×8	64

Table 4: PSNR and MSE stego image

Image size	MSE	PSNR
4×4	1.1875	46.6381
6×6	0.9444	48.6000
8×8	0.5468	53.4000

number of characters that can be inserted on a GIF image if taken five sample GIF images with different image size in Table 3:

MSE and PSNR stego image: After doing the insertion on the sample image with each image is inserted the characters 't', 'e', 's' and 't', then the PSNR value can be obtained and the following MSE (Table 4):

Contribution: This research contributes to a form of steganography techniques suitable to use on TIFF image. because generally, it's been an awful lot of steganography is applied to the digital image formats such as BMP, JPEG, TIFF or PNG. While the steganography is applied to the image as a tiff is extremely rare. So, this journal can give references or suggestions or good steganography method of suit against the TIFF image to be applied. In this study used methods of spread spectrum and adaptive method on the application of TIFF image. Of research results obtained by the maximum number of characters that can be inserted as well as value of PSNR and MSE which produces good value for a method of steganography is used. So, it can be inferred that the spread spectrum and also the adaptive method is very suited towards the application of steganography in TIFF image.

CONCLUSION

The conclusion after doing experiments and analysis on it. We can say that how many number of characters that can be inserted into the carrier file using spread spectrum and adaptive method on TIFF as a format image and the value of MSE and PSNR is depended on the image size and how much character that inserted into the carrier image. In general, many steganography techniques are applied to image formats such as BMP, JPEG, TIFF or PNG. While the application of steganography on the image with TIFF format quite rarely discussed and the discussion on this experiment is explained in detail. This paper may provide references or suggestions for good steganographic methods and in accordance with the TIFF image format to be applied. In this experiment, using the method of adaptive and spread spectrum on the application of TIFF image.

REFERENCES

Gupta, S. and N. Dhanda, 2015. Audio steganography using Discrete Wavelet Transformation (DWT) and Discrete Cosine Transformation (DCT). IOSR. J. Comput. Eng., 17: 32-44.

Johri, P., A. Mishra, S. Das and A. Kumar, 2016. Survey on steganography methods (text, image, audio, video, protocol and network steganography). Proceedings of the 3rd International IEEE Conference on Computing for Sustainable Global Development (INDIACom), March 16-18, 2016, IEEE, New Delhi, India, ISBN:978-1-4673-9417-8, pp: 2906-2909.

Kim, J., H. Park and J.I. Park, 2017. Image steganography based on block matching in DWT domain. Proceedings of the 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), June 7-9, 2017, IEEE, Cagliari, Italy, ISBN:978-1-5090-4937-0, pp: 1-4.

Shetye, O., C. Vanmali, M. Fernandes and P. Patil, 2016. Survey on different techniques of image steganography. Intl. J. Comput. Appl., 138: 36-38.

Singh, A. and S.J. Singh, 2014. An overview of image steganography techniques. Intl. J. Eng. Comput. Sci., 3: 7341-7345.