Journal of
Engineering and
Applied Sciences

SINCE 2000
MEDWELL PUBLICATIONS

Implementation of Steganography in BMP Format Images Files using Spread Spectrum Method

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

Key words: Steganography, spread spectrum method, digital image, bitmap image, distribute, people

Corresponding Author:
Andrew Ivander
Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

Page No.: 3042-3047
Volume: 15, Issue 16, 2020
ISSN: 1816-949x
Journal of Engineering and Applied Sciences
Copy Right: Medwell Publications

Abstract: The exchange of information is experiencing a significant development. It can be seen from the media widely used today that is a digital media. Today, digital media is used by the world with a lot of simplicity, especially, image. But this ease can have a negative impact. For example, the digital data theft sent in the form of images can be misused by irresponsible people. With that ease one can easily copy, distribute and or modify the contents of digital data. So, it takes a technique that can handle this problem, especially, related to the security of information messages. One technique that can be used is steganography. Steganography is a technique to disguise or hide data or image on digital media, called cover image with a specific purpose. There are many types of steganography methods. In this study, we discuss the spread spectrum method.

INTRODUCTION

Archery has been existing, since, ancient time, according to the discovery of Information hiding techniques have become an important research area in the last few years, since, the researchers realized that the development techniques for solving the copying, destruction and distribution of multimedia data through unauthorized The Internet is very urgent. The technique for keeping messages on communication is usually cryptography. Advanced steganography methods so as not to be easily solved. But the message does not have to be encrypted, there is a way to hide the message. from here try a new technique that is steganography[1].

Steganography is currently widely used in the computer with the digital data into a carrier and the network became a high-speed delivery channels. Steganography using the media seemed innocent called image host for inadvertently carrying confidential data to the intended recipients. Image embedded with confidential data look like normal images. Ordinary people will not know hidden messages are inserted. Secret messages on steganography can be images, audio, text or video anything that represents a bit. The message will be mapped on the cover image to hide the message. techniques and methods of embedded also vary depending images that have been inserted message called stego image. The message embedded in the cover image depends on the size of the cover. So, as not to arouse suspicion, the stego image and the resulting image should look as invisible. The message embedded in the cover image depends on the size of the cover. In addition, to providing transparent messages hidden for higher security requirements, data messages can be encrypted before putting it into the cover-image to bestow further protection. Spread spectrum in communications, signal energy is put into one frequency is too small to make a visible artifact and image secrets scattered in various frequencies so be strong against many common signal distortions. Because of the nature of a good correlation, characteristics such as noise, easier pose and impervious to distractions, the sequence of pseudo noise used for steganography[2].

MATERIALS AND METHODS

Basic theory

Steganography: Steganography is a technique of hiding the information into a container (media), so, it's hard to hide data recognized by human senses. The technique of making people aware that there are no important information we submit hidden in another media such as image, audio or video. If the information had been hidden on a matter of such media is stolen, the thief is not necessarily the person can figure out information in it, because there's a password (key) to open the bias of the information contained in the information media such. The password is known only by the sender and the recipient. One of the methods of steganography is spread spectrum. The method spread spectrum transmit a tape signal information into a canal with the spread of broadband frequency. Own frequency dispersion function adds a level of redundancy. By adding redundancy level of the code is not easily solved[3].

There are four main components of steganography, namely: the embedded message (hidden text), the hidden message; cover-object (covert text) that is used for message hiding embedded message; the stego-object (stego text) that is a message that already contains a message embedded message; the stego-key that key is used to insert the message and extract the message from the stego text. The following diagram of the insertion and extraction of the message.

Figure 1 inserted diagram and message extraction. Wide range of requirements that need to be considered when designing the system of steganography is:

- Invisibility-steganography is not detected by the human eye but when the image becomes damaged, then the algorithm steganography error
- The capacity charge-steganography aims to put message depending on image capacity, unlike water marking that adds copyright information

Robustness against attack statistics-in order not to be detected, steganography does not change images visually or statistically. Robustness against image manipulation-manipulation of the image such as cropping, rotation, scaling, etc. can be finish before it reaches its destination. This manipulation can destroy a hidden message. Steganography algorithms should be strong against unwanted changes or unintentional on the image[4].

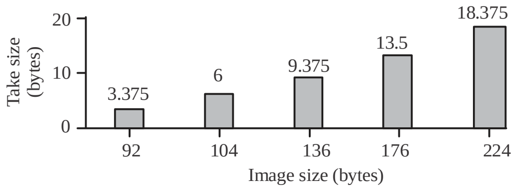


Fig. 1: Th maximum size of the text inserted in image RGB

Spread spectrum method: Spread spectrum method in steganography scheme of inspired spread spectrum communications which transmits a signal into a narrow ribbon of canals with the spread of broadband frequency. Spread spectrum terpencar-pencar steganography as contrary message (encrypt) via. images. To read a message, recipients, require crpto, i.e., l-key algorithm and a stego-key. This method also still vulnerable, i.e., destruction or damage from compression and process image (image)[4].

By the receiver, the signal is collected again using a replica of the pseudo-noise signal is synchronized. Media that already contain the confidential information is filtered first by pre-process filtering to get ¬ noise. The resulting noise selanjutnyad is modulated using pseudo-noise signal to get the bits-bits that are correlated. Bits-the bit that correlates the specific calculation of analyzed to generate bit-bit real information[5].

On the basis of definitions, we can say that steganography using spread spectrum method of treating the object as both cover-noise (noise) or as an effort to add artificial noise (pseudo noise) into the cover-object. Cover the object system that treats noise as cover-object as noise can add a value into the cover-object. This value must be transmitted under the noise level added value into it. This means the capacity of sangatd is determined by the cover-object[6].

Digital image: A digital image is the image that is stored in a digital format (in the form of files). Only the digital image can be processed using a computer. Other image types will be processed if the computer must be changed first into digital imagery. Digital images are usually stored as image files with a size of 24-bit or 8-bit. Image size 24-bit known as true color image. About 24-bit image is scattered with 3 bytes at each pixel represents the color Red, Green and Blue (RGB), respectively. The color is derived from combining the light red, green and blue with different proportions. For 8-bit image, each pixel is represented by 1 byte which has a range of values from 0-255 with 256 possibilities, so, there are 256 color or grayscale values for black and white images.

About 24-bit image is more often used than the 8-bit image for steganography as it offers a great space to hide information. Therefore, it is obvious that 24-bit image has a size >8-bit image.

The data type of the most instrumental in this system is RGB. This type is used to perform the manipulation of a pixel in the image. RBG is the record which has three members, namely RGB red, RGB green, RGB blue that sequentially represent the RGB value of a pixel[7].

Bitmap image: Bitmap graphic image is a representation of a Bitmap image is a representation of the graphics are composed of contiguous point stored in computer memory. Developed by Microsoft and the value of each point by a single bit of data for an image in black and white or more for color images. The density of dots is called the resolution which shows how sharp the picture is displayed, shown by the number of rows and columns. Excess BMP file type is to be opened by almost all image processing programs. Either the compressed BMP files or uncompressed. Excess is the Bitmap Image supports the use of up to 32 bit color 1bit. Suitable for bitmap images such as logo design, banner and so on. While the shortage of bitmap image is larger than the size of the image to other formats.

On the representation of the bitmap an image divided into small boxes where each box stores the value of the intensity of color called pixels. As for the detailed format of the bitmap image is composed of:

- Bitmap information header
- Color table
- Bitmap data

In general, the bitmap image file resolution is 1, 4, 8 and 24 bits per pixel but in this final task uses only 24 bits as a form of public image and an image of 24 bits image handling is equal to 8 bits, the value in terms of the intensity of the color is will be translated into a representation which is equal to 8 bits. For an image of 24 bits do not use table of colors as for image 1, 4, 8bit color palette table must have a maximum size of each is 2, 16 and 256 entry, named each entry is an RGB color[3].

RESULTS AND DISCUSSION

Experiments and result: The following overview of calculations going on in spread spectrum method. On the process of encoding can be described as follows. With an image with the BMP format, the content of the message "A", "S" key words. Before the insertion process is done, the function will read the image and take a header of a BMP image already inserted before, then a picture of the body that will be inserted later this message. Before the deployment process does is change the message to binary form. The result of converting binary from the message "A" is 01000001. Then the next step is the generation with the generation seedlings pseudo noise is determined based on the keyword "S"[8]:

- S = 01110011
- Decimal = 227

After getting the value of the keyword (227) 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 formula is as follows:

$$Xn+1 = (aXn+c) \bmod m$$

- a = 2, c = 7, mod = 9
- Xn = number-n
- $X_1 = (3 * 227+7) \bmod 9$ result $X_1 = 5$

Then the results are modified in the form of binary 00000101 becomes. To get the result of the modulation, the message will be segments is modulated with a pseudo noise signals using function XOR (Exclusive OR):

- Message segment = 01000001
- Pseudo noise signal = 00000101
- The then XOR result is 01000100

The result of the modulation process which will be inserted into the bit-bit images. For example, suppose 9pksel're getting a picture of "kapalrgb":

- Red = 144 129 104 111 138 130 138 121 149
- Green = 168 147 119 109 137 153 120 107 146
- Blue = 190 166 131 110 144 161 111 100 143

Then converted to binary number and inserted between the modulation process results segment message with the pseudo noise signals becomes as follows:

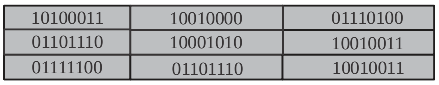
10010000	10000001	01101000
01101111	10001010	10000010
10001010	01111001	10010101
10101000	10010011	01110111
01101101	10001001	10011001
01111000	01101011	10010010
10111110	10100110	10000011
01101110	10010000	1010001
01101111	0110010	10001111

Binary image to RGB before inserted a message

10010000	10000000	01101000
01101111	10001010	10000010
10001010	01111001	10010101
10101000	10010010	01110110
01101101	10001001	10011001
01111000	01101011	10010010
10111110	10100111	10000011
01101110	10010000	1010001
01101111	0110100	10001111

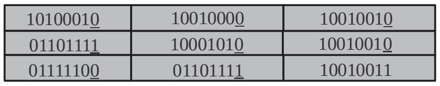
Binary image to RGB after inserted a message

Subsequent experiments attempted messages on the image Grayscale with spread spectrum method with the same message and the same keywords as in RGB, so, get the modulation of the same message. In this section inserted message on the Grayscale image. Grayscale = 163 144 116 110 138 147 124 110 147.



10100011	10010000	01110100
01101110	10001010	10010011
01111100	01101110	10010011

Grayscale binary before inserted a message



10100010	10010000	10010010
01101111	10001010	10010010
01111100	01101111	10010011

Grayscale binary after inserted a message

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 which is “S”. The first step is to read the image if the image has already been inserted images or not. If not yet then a function header will take pictures first, next on the body pictures done screening process in order to get bit-bit result of modulation. The results of the screening process is done will get bit-bit as follows:

- Message segment = 01000001
- Pseudo noise signal = 00000101
- Then the XOR result is 01000100

After all bit-bit modulation results obtained, then conducted the process of with demodulation pseudo noise signals of the same keywords on the process of modulation in order to gain bit-bit correlated. The results of filtering:

- Filtered result = 01000100
- Pseudo noise signal = 00000101
- Demodulation result is = 01000001

The end result is “01000001 segments the same message when hidden in the encode. The results are then converted to the form of the character will be “A”[9].

Analysis and discussion: The maximum message size that can be inserted in a 3×3 pixel sized RGB image. The number of pixel 3×3 = 9; Each pixel consists of 3 byte; 9 pixel×3 Byte = 27 Byte.

Each byte of the message insert 1bit: So, the size of the maximum message that can be inserted is 3.375 bytes. The maximum message size that can be inserted in the image Grayscale pixel-sized 3×3. The number of pixel ini 3×3 is 9; Each pixel consists of 1 byte; 9 pixel×1 Byte = 9 Byte; Each Byte of the message insert 1 bit (Fig. 2-5).

Table 1: Image and image size

Image	Dimensions (Pixel)	Size
	3×3	92 Byte
	4×4	104 Byte
	5×5	136 Byte
	6×6	176 Byte
	7×7	224 Byte
	3×3	1,06 kB
	4×4	1,06 kB
	5×5	1,09 kB
	6×6	1,09 kB
	7×7	1,10 kB

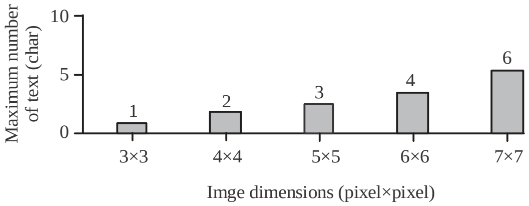


Fig. 2: Character that inserted in Grayscale image

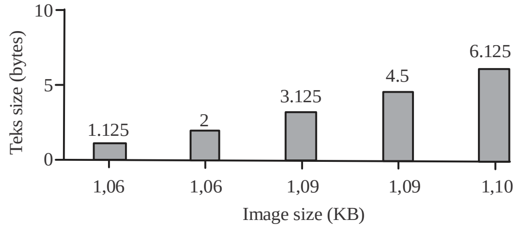


Fig. 3: The maximum size of the text to insert in Grayscale

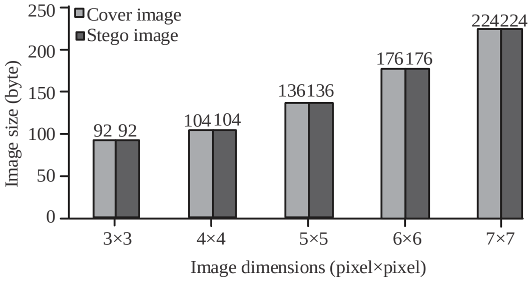


Fig. 4: Comparison of the cover image and the image stego RGB

So, the size of the maximum message that can be inserted is 1.125 bytes. From Table 1 can be concluded that the greater dimensions of the message then the greater the size of the image, so that, it is also the number of characters of the message can be inserted more and more.

From the graphic image of RGB and Grayscale can be concluded that the overall dimensions ozdklf the large-sized image can inserted characters of the message. The larger the dimensions of the image then the more the character of a message that can be inserted.

Table 2: Data results

Image resolution	Image type	Maximum number of text (Char)	Maximum of text size	Cover image size	Stego image size
3×3 pixel	RGB	3	3,37 Bytes	92 Bytes	94 Bytes
4×4 pixel	RGB	6	8 Bytes	104 Bytes	106 Bytes
5×5 pixel	RGB	9	9,37 Bytes	136 Bytes	138Bytes
6×6 pixel	RGB	13	13,5 Bytes	176 Bytes	178 Bytes
7×7 pixel	RGB	18	18,37 Bytes	224 Bytes	226 Bytes
3×3 pixel	Grayscale	1	1,125 KB	1,06 KB	1,08 KB
4×4 pixel	Grayscale	2	2 KB	1,06 KB	1,08 KB
5×5 pixel	Grayscale	3	3,125 KB	1,09 KB	1,11 KB
6×6 pixel	Grayscale	4	4,5 KB	1,09 KB	1,11 KB
7×7 pixel	Grayscale	6	6,125 KB	1,1 KB	1,3 KB

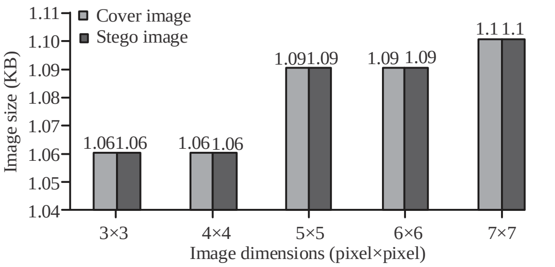


Fig. 5: Comparison of the cover image and stego image grayscale

Insertion of messages also do not change significantly the message dimensions or means. From the graphic image of RGB and Grayscale images that can be viewed on RGB image has the character message insertion capacity more than Grayscale image. This is because on the image RGB has three canals namely R, G and B whereas on the image Grayscale only has one channel only (Table 2).

CONCLUSION

After comparing the results of the design and the results obtained, it can be inferred that steganography text into digital image files using a spread spectrum method of randomization in the message and paste messages can be done and can be inferred from some testing as follows.

The capacity of the bmp image file before and after insert data of the message does not change the meaning. The test is carried out by comparing the digital image file prior to steganography and digital image steganography results file. From the test results obtained that the quality of the digital image files not experience significant changes.

Testing performed by looking at the data hidden must be resistant to manipulation is done on image buffers. From the test results it is known that the process of editing on the image steganography results can damage the bmp data messages that are in a bmp image file because the binary layout of the change message that inserted. This can be evidenced by the extraction process from destructive results image bmp. The larger the image size, the more the number of characters of the message pasted on the image[10, 11].

REFERENCES

01. Marvel, L.M., C.G. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 18: 1075-1083.

02. 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.

03. Goswami, S., J. Goswami and R. Mehra, 2014. An efficient algorithm of steganography using JPEG colored image. Proceedings of the 2014 IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE'14), May 09-11, 2014, IEEE, Jaipur, India, ISBN:978-1-4799-4041-7, pp: 1-5.

04. Sampath, T.S. and T.S.R.K. Prasad, 2016. Hiding of data in image using spread spectrum technique. Intl. J. Comput. Sci. Inf. Technol. Secur., 6: 11-14.

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

06. 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.

07. Johnson, N.F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. Computer, 31: 26-34.

08. 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.
09. Dhore, V. and P.M. Arfat, 2015. Secure spread spectrum data emebedding and extraction. Intl. J. Sci. Res., 4: 743-747.
10. 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.
11. 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.