Journal of Engineering and Applied Sciences 13 (12): 4442-4446, 2018
ISSN: 1816-949X
© Medwell Journals, 2018

Comparison of Digital Image Steganography Based on Techniques

I. Gede Arya Putra Dewangga, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni
Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

Abstract: Steganography is a cryptographic method used to hide data in digital images so that transmitted data can not be identified by irresponsible parties. By developing a steganographic method then sending data that does not have a good level of security but also has a level of security to protect the copyright of a digital image. But there are many types of steganography techniques, in this study described the comparison of some steganography techniques. Steganography technique compared with the existing parameters.

Key words: LSB, transform domain, masking filtering, spread spectrum, comparison, steganography

INTRODUCTION

Steganography is a method of cryptography used to hide data in a digital image, so that, data transmitted cannot be identified by irresponsible parties. Steganography is derived from two words: Greece stegos means roof or covered and graphia, writing means (Saha *et al*., 2011). Steganography has been known, since, the year 500 BC where Herodotus (historian of Greece) write a message on the slave's head and wait until the hair grows back his head, so that, the message is not visible and the next he was sent to deliver a message those without causing suspicion by the Persians (Saha *et al*., 2011).

Currently in the world of digital steganography techniques, widely used to hide secret information with different intentions. One goal of steganography is submitting confidential information without causing suspicion. Besides that steganography can also be used to perform authentication against an artwork as the utilization of watermarking (Saha *et al*., 2011).

Steganography requires at least two properties. The first property is the container (cover) and the second is data or messages that are hidden. To increase the level of security of the data stored can be done by adding a key property (key) the secret. This key property can be either a symmetric key or a public key or private. A file is the result of a process of steganography is often referred to as the stego file (stego file) or stego object (Febryan *et al*., 2017).

MATERIALS AND METHODS

Spatial domain steganography: In the spatial domain techniques, the hidden messages that are embedded directly. In this case, the most common steganography method and the simple from another methods is the method of insertion bit (LSB) of the most significant. In the technique of LSB, most significant bit pixel is replaced by the message bits are tranpose before inserting (Karim *et al*., 2011).

LSB steganography method: The simplest method for hiding data in pictures is a method of LSB (least significant bit) (Karim *et al*., 2011). LSB method exploiting human visual senses in the observed changes a bit in the picture. Figure 24 bit or often called with RGB true color, very suitable for the insertion of this because the LSB method consists of 3 components, i.e., red, green and blue. When using a RGB image which have 24 bits, bits of channel RGB red, green and blue, so the bits for every pixel can be inserted as much as 3 bits. For example, the image of 3 pixels of a 24 bit image uses 9 bytes of memory (Dewangga *et al*., 2017):

(00100110 11101111 11001010)
(00100101 11001010 11101011)
(11001100 00100011 11101101)

When the letter D (ASCII 68) with the binary number 1000100, inserted and the results were as follows:

(00100111 11101110 11001010)
(00100100 11001011 11101010)
(11001100 00100011 11101101)

In the example above is not significant pixel replacement done in order. No significant pixel replacement can also be sorted by, even this can increase

Corresponding Author: I. Gede Arya Putra Dewangga, Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

the level of data security (imperceptibility). Beside that also might do the conversion pixel is not at the beginning of the file container. Conversion pixels can also be selected starting from the middle or from another point from the file container that it is possible to keep all information confidential without causing problems when the disclosure of the data.

Although, the methods are easy to implement LSB, steganography with this method will produce an easily broken stego file (botched). Using LSB steganography technique, a little change on the file stego is very likely also would damage the confidential information stored on it Arora *et al*. (2016).

LSB+1 steganography method: The process of inserting messages into a digital image using LSB+1 almost tantamount to LSB method, the difference is on bit place the insertion of messages. If the method message, inserted on the LSB bit LSB (8 bit) then on the+1 LSB method, the message pasted on the 7th bit. For example, suppose three of the pixels (9 bytes) with the order RGB code (Arora *et al*., 2016):

00110101 11010110 11101010
01110001 00111001 11100001
01110001 10010001 11100001

The message will be inserted is the character "R" which is the value of binary is "01010010". The message will be inserted using LSB+1 then the image will be produced results with the order of the bits as follows (Arora *et al*., 2016):

00110101 11010110 11101000
11110110 00111001 11100001
01110011 10010001 11100001

In the example above, it can be seen that some LSB+1 bit (bit 7) of the original image (original) replaced with a bit of a message that will be inserted. Just as in the method of LSB, LSB on the methods of +1 while the insertion of messages there are pixels that change from the original pixels there is also pixel doesn't change at all (Arora *et al*., 2016).

Transform domain steganography: Transform domain used steganography to hide large amounts of data and provide high security, both transparent and without losing the message confidential. The purpose behind It's to encapsulate information in the frequency domain by changing the magnitude of all DCT coefficients from the cover image. DCT 2-D converts image blocks from spatial domain to frequency domain. The cover image is divided into 8×8 DCT free blocks of overlapping and valid on each block of the cover image using DCT forward (Karim *et al*., 2011).

Discrete Cosine Transform Method (DCT): DCT is a method that has been implemented in various fields of knowledge. DCT is a transformation method that information from the domain space or time into the frequency domain with the aim to accelerate the transmission, reducing the storage in memory, providing compact representations, etc., DCT method is the change in the base that takes real-valued functions and changes them in the form of base orthonormal cosine (Al-Afandy *et al*., 2016). DCT method that is widely used in applications is the 2D DCT. The equation for the transformation of the 2D DCT (image size is m×n) shown in Eq. 1:

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\frac{\pi(2x+1)}{2N}\cos\frac{\pi(2y+1)}{2N}$$
$$\alpha(u)=\sqrt{\frac{1}{N^2}}\quad \text{untuk } u=0,$$
$$\alpha(u)=\sqrt{\frac{2}{N^2}}\ \text{untuk } u=1,2,3,\ldots,n-1 \tag{1}$$

For the inverse of the 2D DCT transformation can be seen in Eq. 2:

$$C(u,v)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)}{2N} \tag{2}$$

Method of Discrete Wavelet Transform (DWT): DWT is a method that can share information from one image into the approach and the detail signal. LL band includes coefficients of low pass and approaches to an image as well as other sub-signal detail shows the details of vertical, horizontal or diagonal or changes in an image. The general equation for DWT can be seen in Eq. 3 (Al-Afandy *et al*., 2016):

$$DWT\{f(t)\}=W_0(J_0,k)+W_\varphi(j,k)$$
$$W_\Theta(j_0,k)=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}x|n|\phi_{j_0,k}|n| \tag{3}$$
$$W_\varphi(j,k)=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}x|n|\varphi_{j,k}|n|,\ \varphi\quad j\geq j_0$$

In this research will be using wavelet transform. Haar wavelet can be used to represent an image with wavelet calculation process. Haar wavelet transform equation is shown in Eq. 4 and 5:

$$X[2k] = 1/2\left(x[2k]+x[2k+1]\right) \quad (4)$$

$$X[2k+1] = 1/2\left(x[2k]-x[2k-1]\right) \quad (5)$$

Masking-filtering steganography: According to Bhatt *et al*. (2015), the technique of masking and filtering is normally restricted to 24 bits image color or grayscale image. This method is similar to a watermark where an image is marked (marking) to hide secret messages. This can be done, for example, by modifying some parts of the image luminance. Although, this method will change the look of the image, it is possible to do it in a certain way, so that, the human eye cannot see the difference. Because this method uses aspects of the image does look directly this method will be more "robust" against compression (especially, lossy compression), cropping and some image processing when compared with other methods of modification LSB (Akhtar *et al*., 2014).

Masking technique and filtering, limited only to the 24 bit images and grayscale, hidden information by marking an image by means such as paper stego. Steganography techniques can be applied with the risk of the destruction of the image in relation to the lossy compression because bit-bit penyisip merges into the image (Akhtar *et al*., 2014).

Spread spectrum steganography: 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 steganography as a contrary message (encrypt) via. images. To read a message, recipients, require crypto, i.e., key algorithm and a stego-key. This method also still vulnerable, i.e., destruction or damage from compression and process image (image).

On the process of concealing the data, bits-bits of information which have undergone the process of spreading these and then will is modulated by pseudo signal-noise generated at random based on key concealment. The result of this demodulation process is then incorporated as the noise into a media file in bits-bits of media files.

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-processing 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.

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.

RESULTS AND DISCUSSION

The most important of any steganography technique is to be invisible to the invisible human eye. However, the following criteria have been proposed to assess from a steganographic technique.

Invisibility: In steganography techniques, invisibility is a very important criterion. Advantages of steganography is exploiting the weaknesses of the ability of the human eye. Humans can not see visually the small changes of the bit-bits inserted into the image (Thangadurai and Devi, 2014).

Capacity: Steganography need not require much capacity. Although, few can however, insert information from copyright (Akhtar *et al*., 2014).

Robustness against statistical attacks: Steganalysis is one way to detect hidden information in steganographic images. Many steganographic techniques leave "signatures" when inserting secret information or messages into images, so, they can be easily detected through steganalysis (Akhtar *et al*., 2014).

Security: When messages go through the transmission process, messages can be altered by attackers aimed at deleting information or messages from images that have been inserted hidden messages. Examples such as cutting or rotating images, giving noise to the image. This can destroy hidden messages in images that have been inserted hidden messages. Strong steganographic techniques are needed in order to withstand attacks (Akhtar *et al*., 2014).

Independent of file format: Steganography techniques can be able to have the ability to be able to enter information into all types of image files (Akhtar *et al*., 2014).

Unsuspicious files: This requirement is a technique of steganography. Steganography can produce images that are not visible to the human eye and the image form does not cause suspicion (Akhtar *et al*., 2014).

Table 1: Perposed method

Techniques	Method	Invisibility	Payload capacity	Robustness	Security	Independent	Unsuspicious	PSNR
Spatial domain	LSB	High	High	Low	Low	Low	Low	Medium
LSB+1	High	High	Low	Low	Low	Low	Medium	
Transformati	DCT	High	Low	Medium	High	High	Low	High
on domain	DWT	High	Low	High	High	High	High	Low
Masking filter	High	Medium	low	Medium	Low	low	Medium	
Spread spectrum	High	Medium	High	Medium	High	High	Mediumc	

PSNR: Compare the algorithms in the aspect of PSNR. Compute the PSNR value by the following Eq. 6 (Karthikeyan *et al*., 2017):

$$PSNR = 20\log_{10}\left(\frac{b}{RMSE}\right) \quad (6)$$

Where:

$$RMSE = \sqrt{MSE}$$

And:

$$MSE = \frac{1}{N}x\left(SUM_{ij}\left|Org_{ij}\text{-}Wink_{ij}\right|^{2}\right)$$

Table 1 following is the result of imperceptibility of an algorithm:

Domain spatial:

- Advantages: the greatest advantages of the algorithm LSB this is quick and easy
- This algorithm also has a steganography software support with work among the principal elements of color LSB through image manipulation

Disadvantages:

- If using 8 bit pixels, the LSB can drastically change the principal elements of the color of the pixel. This can indicate the real difference of cover image being the stego images
- Between 8 and 24 bit image is easily attacked in the processing of the image such as cropping and compression

Masking and filtering:

- Advantages: suitable in the case of lossy compression algorithm as in the JPEG image
- Disadvantages: only to be used on the image-image 24 bit and grayscale

Transformations:

- Advantages: the quality of the original image is almost not affected
- Disadvantages: requires intricate mathematical calculations

Spread spectrum:

- Advantages: unlikely to be detected
- Disadvantages: still vulnerable to the destruction or damaging of compression and process images
- Increased complexity in the process of calculation

CONCLUSION

Steganography is the art and science of writing secret messages in discussing media such that it is not realized by the human senses. There are many techniques that can be used in applying for steganography in digital media. Each of these techniques has advantages and disadvantages of each technique and each match is assigned to a specific digital media. For the media pictures, a pretty good technique is used in is the transformation and spread spectrum because these techniques though complicated enough to be implemented but the result is quite good and will not be realized immediately. To be able to determine where the best steganography, depending on their needs applies depends on size of the data message to be hidden and the desired level of security on the data. By knowing the techniques that can be used in digital image steganography on and know the advantages and disadvantages of each technique, so, the public can choose the technique that best suits their needs. Regarding the comparison is the most appropriate for the message that you need to hide well which has been described in several of the previous paragraphs is not an absolute must do. However, the explanation above helps facilitate and provide an explanation regarding is steganography.

REFERENCES

Akhtar, N., S. Khan and P. Johri, 2014. An improved inverted LSB image steganography. Proceedings of the 2014 IEEE International Conference on ISSUES and Challenges in Intelligent Computing techniques (ICICT'14), February 7-8, 2014, IEEE, Ghaziabad, India, ISBN:978-1-4799-2899-6, pp: 749-755.

Al-Afandy, K.A., O.S. Faragallah, A. ELmhalawy, E.S.M. El-Rabaie and G.M. El-Banby, 2016. High security data hiding using image cropping and LSB least significant bit steganography. Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt'16), October 24-26, 2016, IEEE, Tangier, Morocco, ISBN:978-1-5090-0752-3, pp: 400-404.

Arora, A., M.P. Singh, P. Thakral and N. Jarwal, 2016. Image steganography using enhanced LSB substitution technique. Proceedings of the 4th International Conference on Parallel, Distributed and Grid Computing (PDGC'16), December 22-24, 2016, IEEE, Waknaghat, India, ISBN:978-1-5090-3670-7, pp: 386-389.

Bhatt, S., A. Ray, A. Ghosh and A. Ray, 2015. Image steganography and visible watermarking using LSB extraction technique. Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO'15), January 9-10, 2015, IEEE, Coimbatore, India, ISBN:978-1-4799-6480-2, pp: 1-6.

Dewangga, I.G.A.P., T.W. Purboyo and R.A. Nugrahaeni, 2017. A new approach of data hiding in BMP image using lsb steganography and caesar vigenere cipher cryptography. Intl. J. Appl. Eng. Res., 12: 10626-10636.

Febryan, A., T.W. Purboyo and R.E. Saputra, 2017. Steganography methods on text, audio, image and video: A survey. Intl. J. Appl. Eng. Res., 12: 10485-10490.

Karim, S.M., M.S. Rahman and M.I. Hossain, 2011. A new approach for LSB based image steganography using secret key. Proceedings of the 14th International Conference on Computer and Information Technology (ICCIT'11), December 22-24, 2011, IEEE, Dhaka, Bangladesh, ISBN: 978-1-61284-907-2, pp: 286-291.

Karthikeyan, B., A. Deepak, K.S. Subalakshmi, A.R. MM and V. Vaithiyanathan, 2017. A combined approach of steganography with LSB encoding technique and DES algorithm. Proceedings of the 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB'17), February 27-28, 2017, IEEE, Chennai, India, ISBN:978-1-5090-5435-0, pp: 85-88.

Saha, A., S. Halder and S. Kollya, 2011. Image steganography using 24-bit bitmap images. Proceedings of the 14th International Conference on Computer and Information Technology (ICCIT'11), December 22-24, 2011, IEEE, Dhaka, Bangladesh, ISBN:978-1-61284-907-2, pp: 56-60.

Thangadurai, K. and G.S. Devi, 2014. An analysis of LSB based image steganography techniques. Proceedings of the 2014 International Conference on Computer Communication and Informatics (ICCCI'14), January 3-5, 2014, IEEE, Coimbatore, India, ISBN:978-1-4799-2353-3, pp: 1-4.