ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CASCADED IMAGE STEGANOGRAPHY TO INCREASE ROBUSTNESS AGAINTS ATTACK OF THE STEGO IMAGE

[1]E.I.H.UJIANTO, [2]A.HARJOKO, [2]R.WARDOYO, [3]A.MOESRIAMI

[1]Doctorate Candidate of Computer Science, Gadjah Mada University, INDONESIA

[2]Assoc. Prof., Department of Computer Science & Electronics, Gadjah Mada University, INDONESIA

[3]Asstt Prof., Department of Information Technology, Telkom University, INDONESIA

E-mail: [1]erik_iman@yahoo.com, [2]aharjoko@ ugm.ac.id , [2]rw@ugm.ac.id,[3]imairsoem@gmail.com

ABSTRACT

Information hiding is the most important method in hiding secret information from unauthorized party. The purpose of information hiding is to protect the secret information. One of the method commonly used is steganography. In this research, Cascaded Image Steganography based on spatial and tranformational domain is proposed. This method utilizes two steganography algorithms and double cover information hiding. There are two main processes which are encoding and decoding. The encoding process consists of two steps which are Encoding level-1 and Encoding level-2. The decoding process also consists of two steps which are Decoding level-1 and Decoding level-2. The robustness test is then performed against stego image that undergo images processing operations such as filtering, cropping, rotating, and compression. The results show that stego image undergoes filtering has SNR value of 53.6361 dB indicating good picture quality and high fidelity, whereas stego image undergoes JPEG compression has SNR value of 52.7693 dB indicating good picture quality and high fidelity. Image undergoes rotating(-) has poor image quality indicating low fidelity level, whereas image undergoes rotating(+) and cropping has unusable image quality indicating very low fidelity level. The Cascaded Image Steganography method is more secure due to the double cover information hiding.

Keywords: *Cascaded Image Steganography, Image, Encoding, Decoding, Picture Quality*

1. INTRODUCTION

Information hiding is the most important method in hiding secret information from unauthorized party. The purpose of information hiding is to protect the secret information, especially from other uninterested party. To perform information hiding, one of the technique commonly used is steganography.

The needs of the hiding secret message during transmission by digital communication media may utilized a number of secret communication techniques, one of them is steganography**[1]**. Steganography**[2]** is the art of *fact hiding*, the communication occured by hiding the information inside other information. Whereas, the definition of image steganography **[3]** is the art of information hiding inside the *cover image*.

One of the measurement of strength in steganography method is robustness factor. To know about the robustness of a image steganography product, it needs testing. Robustness**[4]** shows the ability of hidden information (*payload*) to persist from the embedding process and extraction, including some manipulations like *filtering*, *cropping*, *rotating*, and *compression*. Then, the measurement of image quality is performed to compare between the orginal image and the modified image**[5].** The quantitative measurement can be done using two measures which are SNR (*Signal to Noise Ratio*) and NC (*Normalized cross Correlation*).

This research proposes Cascaded Image Steganography method. This method utilizes Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) steganography algorithms which means this method can be categorized as spatial and tranformational domain steganography. The information hiding processes in this method is using two phases in double cover processes. The encoding process is also using two steps. The text message is hid inside cover object image (cover-1) resulting in stego object. The stego object is then hid inside cover image (cover-2) resulting in stego object.

2. RELATED WORK

The related researches about image steganography have been done by other researchers**.** *Secure Steganography using LSB, DCT and Compression techniques* (SSLDC) is proposed by **Raja[6],** using steganography algorithm *Least Significant Bit* (LSB) and *Discrete Cosine Transform*(DCT). Moreover, **Sarreshtedari[7],** in his research also used steganography algorithm *Least Significant Bit* (LSB) and *Discrete Cosine Transform* (DCT), in which message image is hidden inside the cover image.

Steganography research using double cover method has been done by **Sharma[1],** steganography algorithm using *Least Significant Bit*, in which audio and text messages is hidden inside the cover image. In this research, if the size of the hidden message is bigger than the image cover, compression of the hidden message was performed using lossy and lossless compression. The information hiding process was done by 2 (two) levels (double cover), which also include the processes analyzing the information.

There is significant differences between the proposed Cascaded Image Steganography with other methods. In the Cascaded Image Steganography the information hiding process is performed in 2 (two) steps using double cover, which are cover-1 (image) and cover-2 (also image).

3. PROPOSED METHOD

In this paper, the "Cascaded Image Steganography" method is proposed based on the spatial domain and transform domain.This method uses 2 (two) steganography algorithms and 2 (two) levels of information hiding processes (double cover).The steganography algorithm used is Least Significant Bit (LSB) and Discrete Cosine Transform (DCT).The image that used in this research is *greyscale type*, in the format of *bitmap*.

3.1 Positioning "Cascaded Image Steganography"

The position of "Cascaded Image Steganography" than the other steganography can be positioned based on: the characteristic and input/ output combination**[8],** the information hiding media**[2],** the domain**[9]** and the cover type**[10].**

The Cascaded Image Steganography combines LSB and DCT algorithms to obtain optimum result of processing time and security. LSB algorithm is used to hide information in first level (encoding level-1). Since LSB is considered simple steganography algorithm with short processing time, the DCT algorithm is then used to hide information in second level (encoding level-2). DCT algorithm is used since this algorithm is considered strong steganography algorithm that can increase robustness in protecting the hidden message from various attacks.

3.1.1 The Characteristic and Input/Output Combination

Steganography based on its characteristics and input/output combination is divided into *pure steganography, secret steganography* and*public key steganography***[8].** Cascaded Image Steganography is based on the characteristics and input/output combinations which can be categorized into *pure steganography* category.In this case, Cascaded Image Steganography do not use secret key like in the secret steganography or the combination of other techniques, like (*cryptography*) on the*public key steganography*.

3.1.2 The Information Hiding Media

Steganography based on the media in information hiding consists of *text, image, audio/video*, and *protocol* media**[2]**. Cascaded Image Steganography based on the media used for information hiding belongs to image steganography category.Cascaded Image Steganography uses image as the cover for information hiding.

3.1.3 Domain

Steganography based on its domain consists of *spatial domain, frequency domain,* and*parametric domain***[9]**. Cascaded Image Steganography based on its domain is the combination category between *spatial domain* and *frequency domain*. Spatial domain is using of *Least Significant Bit* (LSB) algorithm that is used for text hiding into the image, whereas frequency domain is using of *Discrete Cosine Transform* (DCT) algorithm that is used for image hiding into the cover image.

3.1.4 The Cover Type

Steganography based on its cover type used in the embedding process is divided into *substitution systems, transform domain techniques, spread spectrum techniques, statistical methods*, *distortion techniques,*and*cover generation methods***[10]**. Cascaded Image Steganography based on its cover type is the merging category between *substitution systems transform domain techniques*. Substitution system is to substitute the *redudant* parts from the cover with one secret message, it shows in the using of LSB algorithm, and *transform domain techniques,* that is embedded secret information in a substitute signal room (for example in the frequency domain), shown in the using of DCT algorithm.

3.2 Cascaded Image Steganography Framework

In general, this method consists of 2 (two) main processes, they are *encoding*and *decoding.Encoding* is the information hiding process inside the cover, whereas *decoding* is the information extraction process inside the cover. The information hiding process (encoding) is performed in two steps (double cover). The unhiding process (decoding) is also performed in two steps.

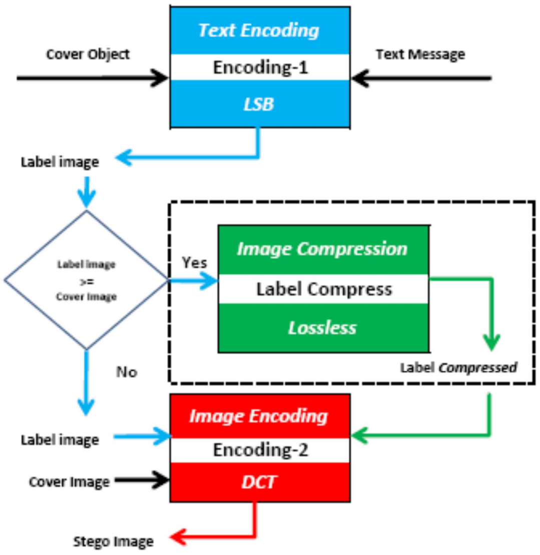

Figure 1: Encoding Process

The encoding process consists of 2 (two) levels, they are ***Encoding level-1*** and***Encoding level-2.*** So that the *decoding* process also consists of 2 (two) levels, they are ***Decoding level-1*** and***Decoding level-2.*** The "Cascaded Image Steganography" *encoding* process consists of 3 (three) sub-processes, they are: (1).Encoding level-1, (2).Label Compress, that is the process of compressed image using *Lossless* compression, and (3).Encoding level-2.

3.2.1 Encoding Level-1

In this research, *encoding* is an information hiding process both in the form of *text* and *image* inside the cover. The first *encoding* process in the form of *text encoding* or called **Encoding level-1** is a text information hiding inside the *Cover Object* using *Least Significant Bit* (LSB) algorithm, and it produces *Stego Object / Label image*.

The Least Significant Bit (LSB) is a simple approach to insert information inside cover image [4]. To hide an information inside an image without altering its noticeable properties, the cover image can be modified in the area of "noise" that has many color variations, so makes it unnoticeable when modification is performed [11] using masking, filtering, and transforming of the cover image [12].

3.2.2 Encoding Level-2

After that, the second *encoding* in the form of *image encoding* or called **Encoding level-2** is a process of *Label image* hiding inside the *Cover Image* using *Discrete Cosine Transform* (DCT), and it produces *Stego Image.* If the size of the message that will be hidden more than the *Cover Image*, so the *Lossless* compression happened. In this experiment the compression process was not performed since the size of the *Label image* is smaller than the *Cover Image*.

Discete Cosine Transform (DCT) transforms points in spatial domain into similar points in frequency domain. The formula for two dimensional DCT [13] is shown in formula (1) and its inverse is shown in formula (2).

(1)

$$DCT(i,j)=\frac{2}{N}C(i)\,C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}pixel(x,y)\,Cos\left[\frac{(2x+1)i\pi}{2N}\right]Cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

$$C(x)=\begin{cases}\frac{1}{\sqrt{2}} & \text{untuk} \quad x=0\\ 1 & \text{untuk} \quad x>0\end{cases}$$

Where:

i = row position for DCT coefficient

j = column position for DCT coeffient

x = row position for pixel

y = column position for pixel

N = the number of row or column

DCT is performed by transforming square matrix NxN from pixel values into similar NxN square matrix in frequency coefficients.

(2)

$$Pixel(x,y)=\frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}C(i)\,C(j)\,DCT(i,j)\,Cos\left[\frac{(2x+1)i\pi}{2N}\right]Cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

$$C(x)=\begin{cases}\frac{1}{\sqrt{2}} & \text{untuk} \quad x=0\\ 1 & \text{untuk} \quad x>0\end{cases}$$

Where:

i = row position for DCT coefficient.
j = column position for DCT coeffient
x = row position for pixel
y = column position for pixel
N = the number of row or column

Pixels is shown inside a square matrix N x N of DCT's coefficients, and the result is a square matrix N x N in frequency domain.

3.2.3 Decoding Level-1

The *decoding* process is the inverse of *encoding* process.In this research, the *decoding* process is an extraction process both in the form of *text* and *image* inside *the cover image*.The *decoding* process of "Cascaded Image Steganography" consists of 2 (two) sub-processes which are: (1).Decoding level-1, and (2).Decoding level-2.

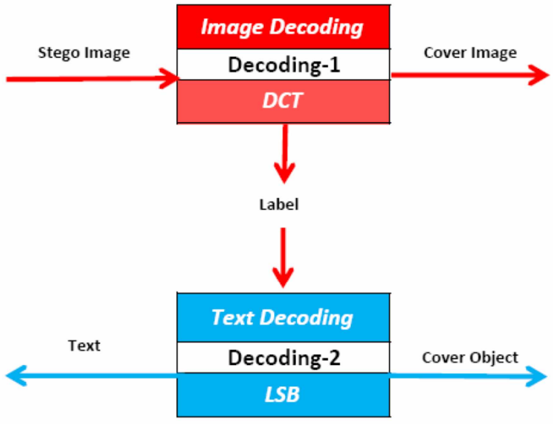

Figure 2: Decoding Process

The first *decoding* process in the form of *image decoding*or called **Decoding level-1** is the extraction process of the *image* inside the *Stego Image* using *Discrete Cosine Transform* (DCT) algorithm, and it produces *Label image.*

3.2.4 Decoding Level-2

Then, the second *decoding process* in the form of *text decoding* or called **Decoding level-2** is the extraction process of the text inside the *Label image* using *Least Significant Bit* (LSB) algorithm, and it produces *text* message.

4. RESULT AND DISCUSSION

In the real condition of *Stego Image*, the product of "Cascaded Image Steganography" process by the sender is transmitted by a *network channel* into the destination place, then the *receiver* analyzes information (*decoding*) to extract the original message.However, that image can get "difficulties" during the process that it is assumed as the *attack* in this paper.The attacks meant in this research are the *image processing* operations, such as: *JPEG Compression, Filtering*, *Rotating*, and *Cropping*.

4.1 Message

Message is the information that will be hidden. In this research, message in the form of a *bas.txt* text file in the size of 64 bytes.

Dengan menyebut nama Allah Yang Maha Pemurah lagi Maha Penyayang

Figure 3: Text file (bas.txt)

4.2 Cover Object

Cover object is an image that has a function as the information hiding media. In this research, *cover object* is the image of *bitmapsa64.bmp* with 64x64 dimension.

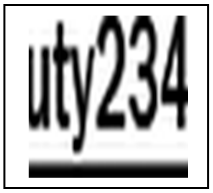

Figure 4: Cover Object (*Sa64.Bmp*)

4.3 Stego Object

Stego object is the image product of *encoding level-1* process that is the *text* hiding inside the *cover object*. In this research, the *stego object* is an image in the form of *sam64.bmp* bitmap with64x64 dimension. Then, *stego object* as the product of *text encoding* process in this paper named as *Label image*.

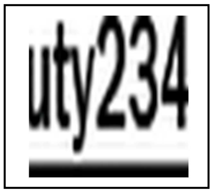

Figure 5: Stego Object (*Sam64.Bmp*)

4.4 Cover Image

Cover image is an image that has a function as the *Label image* hiding media. In this research, the *cover image* is an image in the form of *Kamp512.bmp* bitmap with512x512 dimension.

Figure 6: Cover Image (Kamp512.Bmp)

4.5 Stego Image

Stego image is the image product of *encoding level-2* process that is the *Label image* inside the *Cover image*. In this research, the *stego image* is an image in the form of *StKamp512sam64.bmp* bitmap with512x512 dimension.

Figure 7: Stego Image (Stkamp512sam64.Bmp)

The *stego image* as "Cascaded Image Steganography" has SNR=62,8822 (*Excellent*) value.

4.6 Stego Attack

In this research, the *stego image* gets attack, they are *image processing* operations that consist of *JPEG Compression, Filtering*, *Rotating*, and *Cropping.*

4.6.1 Measure of SNR

SNR metrics is used to compare the cover and stego images. The formula to measure SNR is shown in formula (3).

$$SNR = 10 * Log_{10} \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} (A_{ij})^2}{\sum_{i=1}^{n} \sum_{j=1}^{m} (A_{ij} - B_{ij})^2} \quad (3)$$

Where: Aij represent one pixel in the original image (before embedding the hidden data) and Bij represent one pixel in the stego-image (after embedding the hidden data) [14].

Stego image after the attack is calculated by its *Signal to Noise Ratio* (SNR) value, the result as followed:

Table 1: SNR Value

Image Processing	SNR (dB)	Picture Quality
Jpeg Index 25	52,7693	Good
Jpeg Index 50	55,6974	Good
Jpeg Index 75	58,5901	Good
Jpeg Index 100	76,7972	Excellent
LowPass Filtering	50,5668	Good
Median Filtering	53,6361	Good
Rotating(+)	28,3247	Unusable
Rotating(-)	35,8622	Poor
Cropping	26,9607	Unusable

The calculation of SNR value done to measure the image product quality of "Cascaded Image Steganography" after the attack happened.The low SNR value shows that the developed image has bad quality, inversely if the SNR has high value, it has good image quality.The graphic followed shows the image quality after the *image processing*operations.

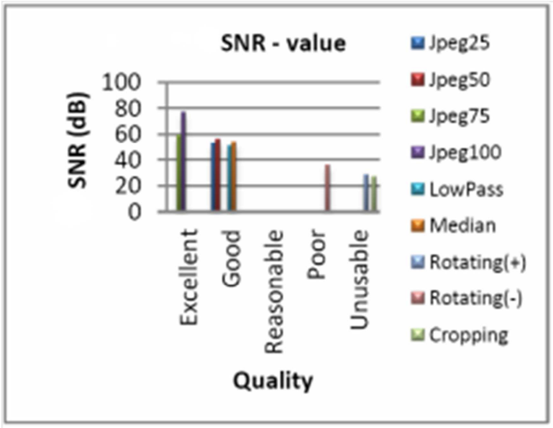

Figure 8: SNR – Value (Db)

When the stego image undergoes rotation, the image experiences resizing that makes the change of information in the Label Image inside the stego image. This change makes the poor and unusable image quality. Moreover, the cropping makes truncation of some part of the image to make new image. This operating will make significant change in information of Label Image in the stego image. This makes the unusable image quality.

4.6.2 Measure of NC

The result of *Label image*extraction process inside *stego image* after the attack happened is measured using NC (*Normalized cross Correlation*). The high NC value shows bad image quality[5], inversely the low NC value shows good image quality.NC is the measurement of the qualitative similarity of the original image compared to the extracted image.

$$NC = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{M-1} W(i,j) W'(i,j)}{\sum_{i=0}^{M-1} \sum_{j=0}^{M-1} [W(i,j)]^2} \quad (4)$$

Where :

$M \times M$ is the size of image (Label)

W' is the extracted image (Label)
W is the original image (Label)

Table 2: NC Value

Stego Image (Attacked)	Label (Extracted)	NC
AtStKAMP512sam64-Jpg100	sam64-Jpg100	0,94539
AtStKAMP512sam64-Rot-17	sam64-Rot-17	0,95873
AtStKAMP512sam64-Rot+17	sam64-Rot+17	0,96427
AtStKAMP512sam64-Jpg75	sam64-Jpg75	0,96945
AtStKAMP512sam64-MedFil	sam64-MedFil	0,97098
AtStKAMP512sam64-LowPass	sam64-LowPass	0,97288
AtStKAMP512sam64-Jpg50	sam64-Jpg50	0,97418
AtStKAMP512sam64-Jpg25	sam64-Jpg25	0,97656
AtStKAMP512sam64-Crop512	sam64-Crop512	0,98899

Table 2: it shows *Label image* of the extraction product that refers to the best into the worst in a series.

5. CONCLUSION

The findings of this research shows the image quality in the "Cascaded Image Steganography", for example: the image with *JPEG Compression* index 100 operation shows *Excellent* picture quality that means high *fidelity* level. The image with *JPEG Compression* index 75, index 50, and index 25 operation shows Good quality image that means high *fidelity* level. Similarly, the image with *Median Filtering* and *LowPass Filtering* operation shows *Good* quality image that means high *fidelity* level.

However, there is also "Cascaded Image Steganography" that has not expected result, for example: The image with *Rotating (-)* operation, it shows *Poor* image quality and it has low *fidelity* level. Similarly, the image with *Rotating (+)* and *Cropping* operation, it shows *Poor* image quality and it has the lowest *fidelity* level.

While based on NC calculation, the data which shows best order is *extracted Label image* after *JPEG Compression* index 100. Then, it is followed by *extracted Label image* after: *Rotating(-), Rotating(+), JPEG Compression*index 75, *Median Filtering*, *LowPass Filtering, JPEG Compression* index 50, and *JPEG Compression* index 25. The worst result is *extracted Label image* after *Cropping* operation.

6. FUTURE WORK

The attack form toward *stego image* in this research is *image processing* operation, like: *JPEG Compression, Filtering*, *Rotating*, and*Cropping*. It needs further research in expanding this method, which include image research with stego analysis.The other experiment that needed to be done is the using of media cover, the different message, and also the using of the other steganography algorithm, whether it is in the same domain or in the different domain.

REFERENCES:

[1] D.Sharma, 2010. A Two Level Message Adaptive Steganographic Approach, *International Conference on Advances in Computer Engineering*, New Delhi, India.

[2] T.Morkel, J.H.P.Eloff, M.S.Olivier., 2005. An Overview Of Image Steganography. *Information and Computer Security Architecture (ICSA) Research Group,* Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.

[3] A.Nag, S.Biswas, D.Sarkar, P.P.Sarkar. "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", *International Journal of Computer Science and Security (IJCSS)*, Volume (4), Issue (6), 2011, p.561-570.

[4] G.Kaur, A.Kochhar, "A Steganography Implementation based on LSB & DCT", *International Journal for Science and Emerging Technologies with Latest Trends*, 4(1), 2012, 35-41, ISSN No.(Online):2250-3641.

[5] A.Verma, R.Nolkha, A.Singh, G.Jaiswal, "Implementation of Image Steganography using 2-Level DWT Technique", *International Journal of Computer Science and Business Informatics*, ISSN:1694-2108, Vol.1, No.1, May 2013.

[6] K.B.Raja, C.R.Chowdary, K.R.Venugopal, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", *IEEE ICISIP,* pp. 170-176, Dec. 2005.

[7] S.Sarreshtedari, M.Ghotbi, S. Ghaemmaghami, 2009. On the Effect of Spatial to Compressed Domains Transformation in LSB-based Image Steganography, Sharif University of Technology, Tehran, Iran.

[8] R.Hovančák, P.Foriš, D.Levický., 2006. Steganography Based On DWT Transform. *Department of Electronics and Multimedia Telecommunications, Technical University of Košice,* Park Komenského 13, 041 20 Košice, Slovak Republic.

[9] A.G. Bors, I.Pitas, "Image Watermarking using DCT Domain Constraints", *Proceeding of Image Processing,* International Conference on 16-19 Sep 1996, Volume: 3, page(s): 231-234, Lausanne, Switzerland.

[10] N.F.Johnson, S.C.Katzenbeisser., "A Survey of Steganographic Techniques", in S.C.Katzenbeisser, F.Petitcolas (Eds.): Information Hiding, *Artech House,* Norwood, MA., 2000, pp 43–78.

[11] R.Chandramouli, N.Memon, "Analysis of LSB Image Steganography Techniques", *IEEE International Conference on Image Processing*, vol. 3, 2001, pp. 1019–1022.

[12] N.N.EL-Emam., "Hiding a Large Amount of Data with High Security Using Steganography Algorithm", *Journal of ComputerScience* 3 (4):223-232, 2007, ISSN 1549-3636.

[13] http://www.itacs.uow.edu.au, *digital watermarking tutorial, Date :12-10-2008, 09.15 wib .*

[14] Hmood, A.K., Z. M. Kasirun, Hamid A. Jalab, Gazi Mahabubul Alam, A. A. Zaidan, and B.B. Zaidan. 2010. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. *International Journal of the Physical Sciences,* August, 2010, Vol. 5, Issue 7, pp. 1054-1062.