INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2019, VOL. 65, NO.2 , PP. 287-292
Manuscript received August 15, 2018; revised April, 2019. DOI: 10.24425/ijet.2019.126312

Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation

De Rosal Ignatius Moses Setiadi

***Abstract*—This research proposes a method to enhance the payload message by embedding messages on the dilated edge areas by the Least Significant Bit (LSB) method. To add security aspects to messages, messages are not embedded directly on the LSB but encrypted with XOR operations with Most Significant Bit (MSB). The experimental results of the test in this study showed that the dilation process to some extent can increase the payload of 18.65% and the average bpp is 1.42 while maintaining the imperceptibilty quality of stego image with an average PSNR value of about 47 dB, SSIM is 0.9977 and MSE is 1.13.**

***Keywords*—Edge, Dilation, Image, Payload, Steganography**

I. Introduction

STEGANOGRAPHY is a science that learns about the concealment of data on a cover media. It aims to deceive someone so as not to know that in a cover media embedded data or secret messages. This technique is mostly done to secure the transmission of secret messaging through the public network [1]. Cover media is a container that is used to hide the data. Cover media can be image, audio, video, or text [2] [3]. The image is a popular and widely researched media in steganographic science to date. Research on steganography also continues to be done to develop some important aspects are imperceptibility, payload, and security [4]. The increased payload is an aspect which is quite widely studied. The number of payloads embedded in the media covers greatly affect to the quality of imperceptibility. This becomes a research challenge to increase payload without excessive side effects on other aspects.

Steganography on digital images is done with various methods that are divided into two main domains, namely spatial domain and frequency domain [5]. In the frequency domain is often used transformations such as Cosine, Wavelete, and Fourier. While the spatial domain method that is widely used is Least Significant Bit (LSB) and Pixel Value Differencing (PVD). LSB is becoming a very popular method in the spastial domain and is continuing to be studied to date [1] [4] [6] [7] [8]. LSB is a very simple method and has advantages that have a good aspect imperceptibility, but this method will become very weak and predictable if done traditionally. In some studies such as [1] [9] [10] [11] the LSB method is combined with encryption methods such as Chaotic Map, AES, DES, or OTP to improve security aspects. Where the encryption method is done on the message before it is embedded in the cover image. Where the encryption method is done on the message before it is embedded in the cover image. In this way the imperceptibility and security aspects can be met, but how to increase the payload of messages?

One way to increase the payload of messages while maintaining the imperceptibility aspect is to use edge detection on the cover image, as did the research [2] [4] [7] [12]. The cover image edge area is an area where messages can be embedded with a larger capacity than a smooth area. This is because the edge area gives more tolerance to changes in pixel values. In smooth areas, changes in pixel values will be more easily detected by human vision [2] [4]. Getting the edge area can be done with an edge detector like Canny, Sobel, and Prewitt [2] [4] [7]. The use of edge detection can also improve the security aspects of messages because the way embedding is not done in sequence [11].

The Canny edge detector produces a more optimal edge area due to the minimal error rate. Another plus is to provide standardized localization solutions and complex mathematical calculations. The Canny edge detector has also been widely applied to various image processing algorithms that require edge detection [13] [14] such as image segmentation and recognition. At the image segmentation stage, edge area dilation techniques are often used to thicken the edge area so that it appears wider and clearer [15]. This technique is inspiring this research to be able to explore the edge area even further. Wider edge areas can be utilized to increase the payload of messages to be embedded. So this study further analyzes the performance of dilation techniques on the edge area to increase message payload while maintaining the quality of imperceptibility in the stego image. To improve message security, prior to embedding in LSB, messages are encrypted with XOR operations against the most significant bits (MSB) [16]. The proposed method is measured by the quality of imperceptibility using MSE, PSNR, and SSIM. The number of payload messages that can be embedded is measured using bits per pixel (bpp). While the message extracting process is measured by the character error rate (CER).

II. LSB Image Steganography and Edge Detector

A. LSB Image Steganografi

LSB is one of the steganographic methods used in image spatial domains. This method has long been used and is still very popular to date. The simple way is to read the image pixel value, where the pixel value of the image has a range of values of 8 bits or if the decimal has a value of 0-255. Typically, the decimal value is converted to a bit value, so the smallest bit value is obtained. The smallest bit value will be changed in value based

De Rosal Ignatius Moses Setiadi is with the Department of Informatics Engineering, Dian Nuswantoro University, Indonesia, (e-mail: moses@dsn.dinus.ac.id).

on the message bit. Then it can be concluded that by default 1 pixel image can only hold 1 bit message. Figure 1 is a typical example of how messages are inserted into the LSB method.

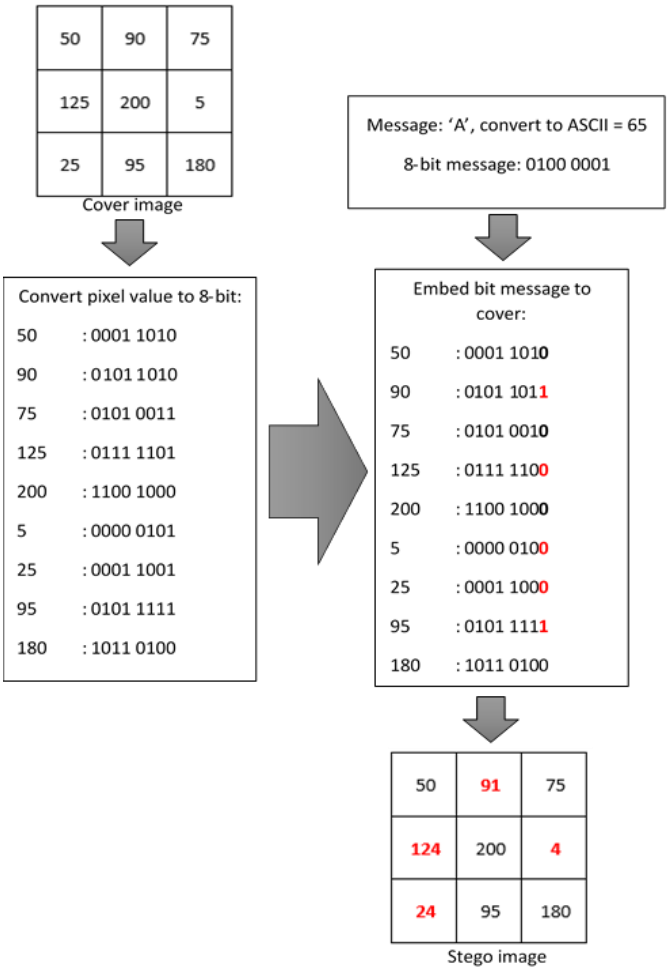

Fig. 1. Sample Implementation LSB Image Steganography (Traditional method)

Based on Figure 1 it can be seen that from 9 pixels cover image only 4 pixels change value, and change value with a maximum difference is 1. It might happen if message bit equal to last bit cover then pixel value cover completely unchanged. This is what makes the imperceptibility aspect of the LSB technique so good and the human eye can not detect changes in pixel values directly. But this method is so simple and very easy to guess, this method also has a maximum payload of 1 bit per pixel when the maximum embedding per pixel is only 1 bit. Then this method still needs to be developed further to increase message payload and security.

B. Image Edge Detector

There are many methods of edge detection on the image, some of which are widely used are Canny, Sobel and Prewitt [2] [4] [7]. Each detector has its own advantages and disadvantages, so the edge area produced by each method is different. Image edge areas are used for various things in image processing. Such as image segmentation, image recognition, morphological pre-processing, and even can be utilized in image steganography. In the steganography theory of the image, it is said that the edge image area has a greater tolerance to the change in pixel value. This is because the difference in pixel values between neighbors is significant so that changes in pixel values more than one can maintain the quality of imperceptibilility. This theory has been widely proven in several image steganography studies based edge area. In some studies, there is a rule that if the value of the message allows being stored in the edge area then the message is sufficiently encountered in the edge area only. But if not then the rest can be pinned on other areas with certain rules [2] [4]. Disadvantages of Image-based steganography of the edge area make the selection of a cover image to be limited because the cover image should use the image that has many edge areas. Edge detector used also affects the number of edge areas. From some popular edge detector imagery, the Canny detector produces a more optimal edge area and has a larger area than the Sobel and Prewitt detectors. Thus, the number of edge areas produced by the Canny detector is superior and can increase the payload of messages. Figure 2 shows the edge area produced by Canny, Sobel and Prewitt detectors on Lena's image, where Canny has a number of edge areas that are far superior to both detectors.

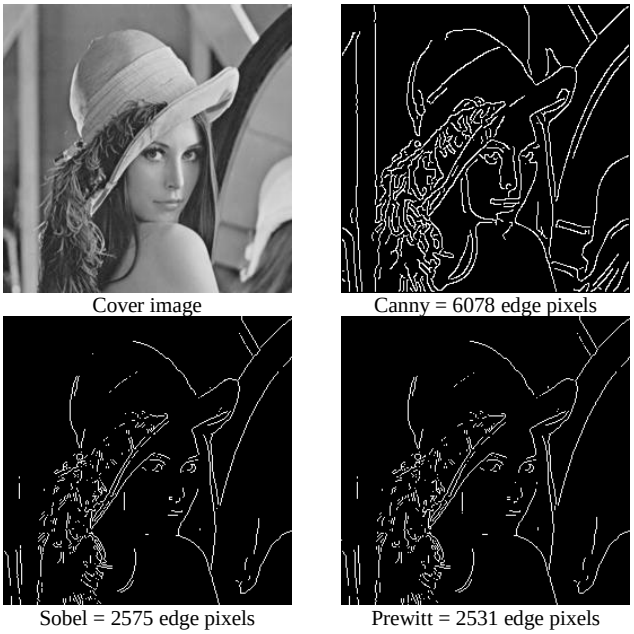

Fig. 2. Cover image with various edge areas

C. Edge Dilation

Edge dilation is widely used in morphological processes aimed at improving the quality of robustness [17]. Basically, the dilation process is performed on binary imagery that aims to enlarge the foreground or white pixel boundary boundary [18], although the dilation process can also be performed on the grayscale image [19]. The dilation process on the edge area of the image makes the image edge area thicker. By default, the dilation process uses a matrix element structure of 3 * 3 size. This process is very useful to clarify the edge of the line when the image so that it can work more optimally [15] [20]. In image steganography based on the edge of the dilation process can be utilized to expand the image edge area. So by utilizing the dilation process can increase the number of edge areas and increase the number of payload messages that can be embedded on the cover image. The binary dilation of A by B is denoted as $A \oplus B$, while the formula for calculating $A \oplus B$ is found in formula (1) [19].

$$A \oplus B = \{z|(\hat{B})_z \cap A \neq \emptyset\} \quad (1)$$

Where $\hat{B}$ is a reflection of the structure of element B on the collection of pixel loop z. The elemental structure reflected overlaps the foregone A when translated into z.

III. PROPOSED METHOD

A. Proposed Embbeding Scheme

In the embedding scheme, requires a cover image and a message to be embedded. Here are the steps for embedding messages:

1. Read the cover image and do two process cover image, first do edge detection and the second process change the cover image into binary form.
2. Perform a dilation on the edge area of the cover image, calculate the number of edge areas and save as the extraction key.
3. Read the text message, then convert it to binary form.
4. Measure text messages, if enough to be embedded in the edge area, pin message on the edge area only, if the message size is larger than the edge area but does not exceed the maximum limit, embed the message with the priority on the edge area and the rest in the smooth area. Where the embedding process is done by XOR operation on the message bit and the MSB value of the insertion coordinates to improve the security.
5. Get the stego image.

As a clearer description can see Figure 3.

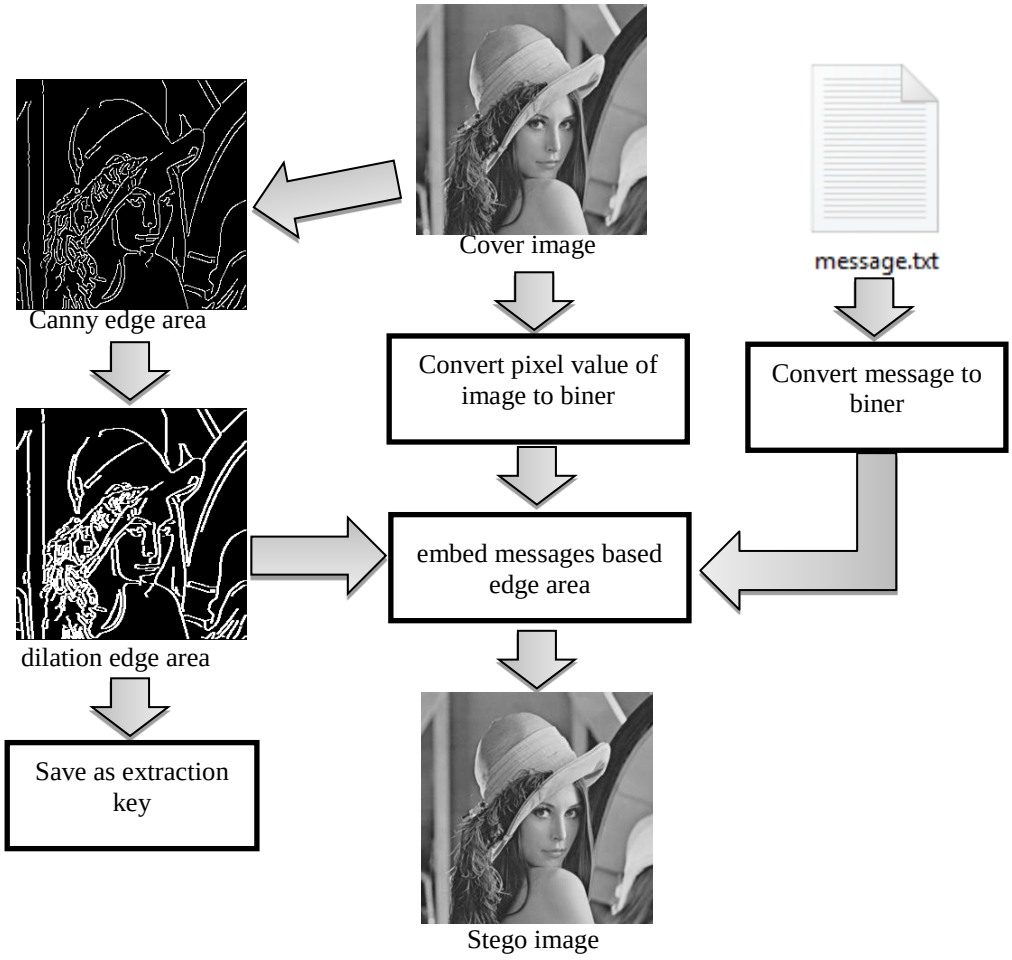

Fig. 3. Proposed embedding LSB Image Steganography method based on dilation edge area

B. Proposed Extraction Scheme

In the extraction scheme, it takes two inputs: stego image and extraction key. The extraction key is the edged edge of the image area. The following is the detailed stage of the extraction process:

1. Read stego image, then change stego image value to binary form.
2. Read the extraction key
3. Take LSB and MSB stego images based on extraction key coordinates.
4. Perform XOR operation on LSB to MSB to get the message.
5. Perform step 4 repeatedly until it finds a sign indicating the end of the message

To see more detail of the proposed extraction process can see Figure 4.

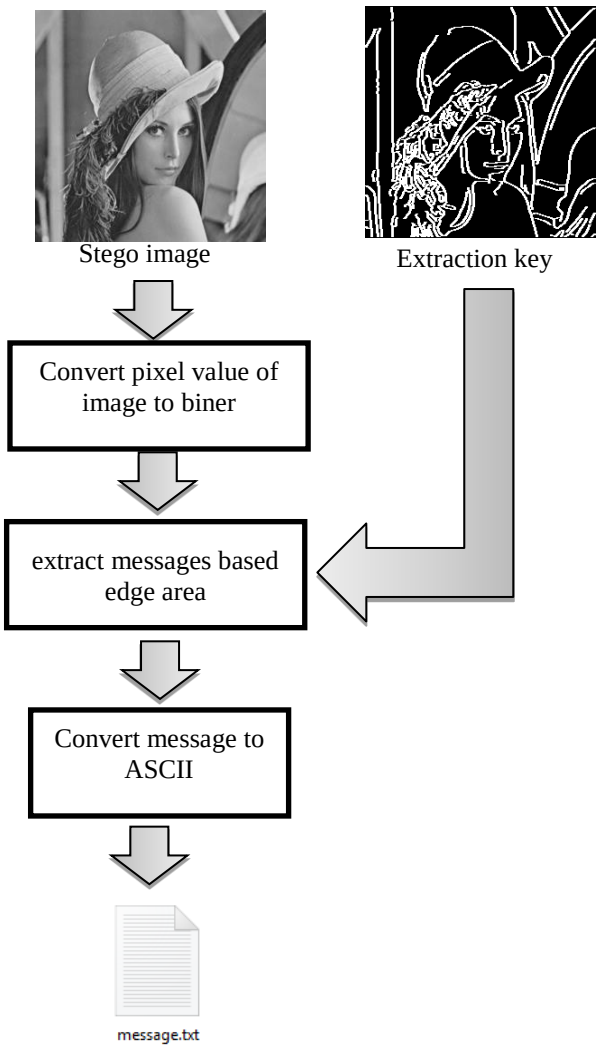

Fig. 4. Proposed extracting LSB Image Steganography method based on dilation edge area

IV. Experimental and Results

This stage is tested against the proposed method, it should be emphasized again that the contribution tested in this research is the addition of image payload while maintaining imperceptibility aspect as well as improving security aspect with XOR operation.

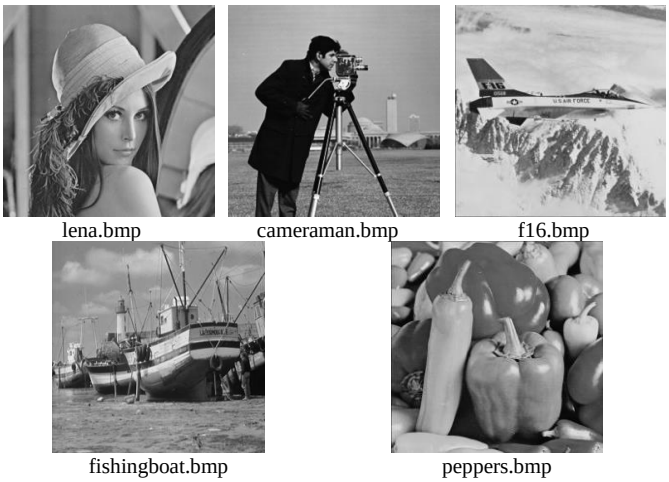

Fig. 5. Cover Image used

The cover image used in this study is a standard test image with a grayscale type of 256 * 256, as shown in Figure 5. Furthermore, all cover images are edge detection process followed by a dilation process at the edge area. Figure 6 shows the edge detection samples and the widening results.

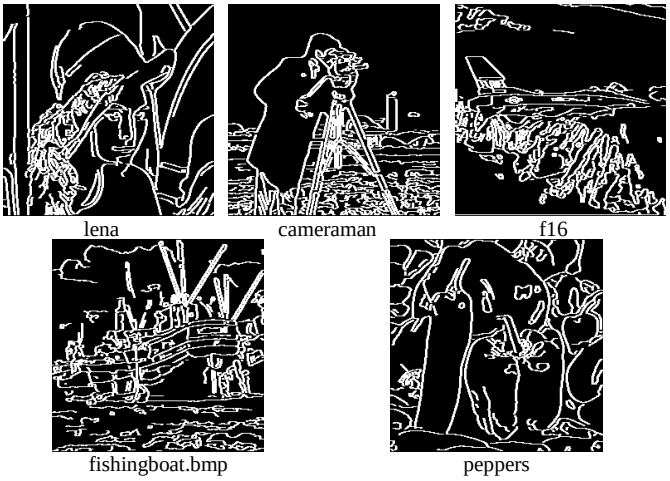

Fig. 6. Cover Image used

After obtaining the dilated edge area, then save it for the extraction process. The maximum message size embedded in the cover image is by pinning a 2-bits on the edge area and 1-bit in the smooth area. The edge area will be prioritized to embed the message first, if any remaining then pinned on the fine area. Table I shows the calculation of the number of tepid areas and the maximum size of embedded messages.

TABLE I
Number of Edge Area and Maximum Message every Image

Image	Number of edge pixels using Dilation	Number of edge pixels without Dilation	Maximum Message (using dilation) in bit
lena	14487	6077	94510
cameraman	13448	6476	92432
f16	12536	6196	90608
fishingboat	15724	7767	96984
peppers	12543	5662	90622

Prior to the insertion process, the message encryption process is done to improve the security. Encryption is done by XOR operation on message bit and MSB. The results of this XOR operation are embedded in the LSB. As an illustration of the encryption process as well as embedding the message as follows:

Message =’A’, convert to ASCII = 65, ASCII to biner = 1000 0001

If there is a cover image pixel with values 50, 25, 66, 120, 75, 88, 65, and 128 then the pixels will be converted to binary numbers as follows:

50 =0011 0010, MSB=0, LSB=0, 1st bit message =1
25 =0001 1001, MSB=0, LSB=1, 2nd bit message =0
66 =0100 0010, MSB=0, LSB=0, 3rd bit message =0
120 =0111 0111, MSB=0, LSB=1, 4th bit message =0
75 =0100 1011, MSB=0, LSB=1, 5th bit message =0
160 =1010 0000, MSB=1, LSB=0, 6th bit message =0
65 =0100 0001, MSB=0, LSB=1, 7th bit message =0
128 =1000 0000, MSB=1, LSB=0, 8th bit message =1

Encryption using XOR Operation = MSB XOR bit message
LSB 1st pixel = 0 XOR 1 = 1
LSB 2nd pixel = 0 XOR 0 = 1
LSB 3rd pixel = 0 XOR 0 = 1
LSB 4th pixel = 0 XOR 0 = 1
LSB 5th pixel = 0 XOR 0 = 1
LSB 6th pixel = 1 XOR 0 = 1
LSB 7th pixel = 0 XOR 0 = 1
LSB 8th pixel = 1 XOR 1 = 0

The original binary message is 1000 0001 encrypted to 1111 1110, then the encrypted message is pinned on the cover image so that the stego image with pixel value is: 51, 25, 67, 120, 75, 161, 65, 128.

The experiments carried out in this study were by embedding text messages with the size of 512 bytes or 4096 bits, 1024 bytes or 8192 bits, 2048 bytes or 16384 bits, and the maximum size of messages that could be embedded in the cover image. To measure imperceptibility quality, we used a mean square error (MSE) measurement tool which can be calculated by formula (1), peak signal to noise ratio (PSNR) which can be calculated by formula (2), and structural similarity index (SSIM) can be calculated with the formula (3).

$$MSE = \sum_{m=0}^{M}\sum_{n=0}^{N}\|c(m,n) - s(m,n)\| \quad (1)$$

$$PSNR = 10\ log_{10}\left(\frac{255^2}{\sqrt{MSE}}\right) \quad (2)$$

Where:
m, n = the number of rows and columns
c = cover image
s = stego image

$$SSIM\ (C,S) = \frac{(2\mu_C\mu_S + \gamma_1)(2\sigma_{CS} + \gamma_2)}{(\mu_C^2 + \mu_S^2 + \gamma_1)(\sigma_C^2 + \sigma_S^2 + \gamma_2)} \quad (3)$$

Where :
C is a cover image
S is a stego image
μ_C and μ_S is mean of the C and S images
σ_{CS} is the image covariance C against S
σ_C^2 is a variant of image C
σ_S^2 is a variant of image S
$\gamma_1=(k_1L)^2$ and $\gamma_2=(k_2L)^2$
L is a dynamic range of the image(2^{bit}-1)with the default valuek_1=0.01 dan k_2=0.03

The edge of the area dilation process can make a smooth area may be regarded as the edge of the area, thus reducing the quality of stego image imperceptibility. To prove that the use of dilation on edge areas can increase the payload of messages without affecting imperceptibility quality in Table II, Table III, and Table IV compared to MSE, PSNR, and SSIM values of message embedding on edge areas with and without dilation.

Based on the experimental results shown by Table II it appears that insertion without dilation and with dilation has the same mean MSE and SSIM values if rounded three digits behind the coma and has only a margin of less than 0.1 dB for PSNR. While in Table III and Table IV, it appears that insertion with dilation is better when viewed from all measuring instruments. This is due to the edge area owned by the proposed method is much bigger even more than double, so the rest of the messages pinned to the fine area is much less. This makes the message imperceptibility better.

TABLE II
RESULTS MSE, PSNR, AND SSIM FROM EMBEDDING 512 BYTES MESSAGE

Image	With Edge Area Dilation			Without Edge Area Dilation		
	MSE	PSNR	SSIM	MSE	PSNR	SSI
lena	0.015	66.388	1.0000	0.016	66.210	1.00
cameraman	0.015	66.265	0.9999	0.015	66.331	0.99
f16	0.017	65.807	1.0000	0.017	65.949	1.00
fishingboat	0.016	65.973	0.9999	0.016	66.034	0.99
peppers	0.015	66.283	1.0000	0.015	66.419	1.00
Average	0.016	66.143	1.0000	0.016	66.189	1.00

TABLE III
RESULTS MSE, PSNR, AND SSIM FROM EMBEDDING 1024 BYTES MESSAGE

Image	With Edge Area Dilation			Without Edge Area Dilation		
	MSE	PSNR	SSIM	MSE	PSNR	SSI
lena	0.030	63.364	0.9999	0.046	61.480	0.99
cameraman	0.031	63.229	0.9999	0.043	61.790	0.99
f16	0.033	62.957	0.9999	0.047	61.448	0.99
fishingboat	0.032	63.049	0.9999	0.036	62.607	0.99
peppers	0.031	63.242	0.9999	0.049	61.271	0.99
Average	0.031	63.168	0.9999	0.044	61.719	0.99

TABLE IV
RESULTS MSE, PSNR, AND SSIM FROM EMBEDDING 2048 BYTES MESSAGE

Image	With Edge Area Dilation			Without Edge Area Dilation		
	MSE	PSNR	SSIM	MSE	PSNR	SSI
lena	0.077	59.256	0.9998	0.099	58.167	0.99
cameraman	0.085	58.831	0.9996	0.106	57.876	0.99
f16	0.096	58.289	0.9998	0.109	57.752	0.99
fishingboat	0.070	59.669	0.9998	0.122	57.275	0.99
peppers	0.087	58.741	0.9997	0.097	58.284	0.99
Average	0.083	58.957	0.9997	0.107	57.871	0.99

Based on the payload measurements using bits per pixel (bpp) written in formula (4), the maximum message that can be accommodated in the proposed method also has a substantial difference compared to the method without dilation. To see the maximum bpp measurement results by embedding 2-bits on the edge area and 1-bit in the fine area can be seen in table V.

$$bpp = \frac{maximum\ bits\ of\ message}{M \times N} \quad (4)$$

TABLE V
BPP OF MAXIMUM MESSAGE TO EMBED

Image	With Edge Area Dilation	Without Edge Area Dilation
lena	1.44211	1.18546
cameraman	1.41040	1.19763
f16	1.38257	1.18909
fishingboat	1.47986	1.23703
peppers	1.38278	1.17279
Average	1.41954	1.19640

Table V proves that the maximum number of embedded bits has an average difference of 0.2 bpp or the maximum number of message messages that can be embedded increases by 18.65%, with the results of MSE, PSNR and SSIM values averaging 1.13, 47.59 dB, and 0.9977. This value can still be

categorized as having a very good imperceptibility aspect because the PSNR result is above 40 dB and the SSIM value is near perfect [21].

A steganographic method would be useless if message extraction could not work perfectly [4]. In the message extraction test, this method is measured using the character error rate (CER). CER serves to measure the number of characters wrong message after extraction message [22]. CER can be calculated using formula (5) and the result of the calculation is shown in Table VI.

$$CER = \frac{number\ of\ characters\ error}{message\ length} \quad (5)$$

TABLE VI
CER OF EXTRACTION MESSAGE RESULTS

Image	Message Length (in byte)			
	512	1024	2048	Max Message
lena	0	0	0	0
cameraman	0	0	0	0
f16	0	0	0	0
fishingboat	0	0	0	0
peppers	0	0	0	0
Average	0	0	0	0

The result of the CER calculation shown in table VI is entirely 0, this means that the message extraction process can be done perfectly.

V. CONCLUSION

Based on the experimental results, it is evident that the use of dilation on the edge area may increase the payload of embedded messages by not affecting the imperceptibility quality of stego image. Even on messages that have larger sizes of edge areas without dilation can improve the quality of imperceptibility. Proven with message embedding size 16384 bits value of PSNR superior more than 1dB, as well as the value of SSIM and MSE is superior. This is because the average number of edges with dilation is 13748 pixels while no dilation is 6436 pixels. Thus the message can be embedded more on the edge area and the remaining less embedded in the fine area. Of course this also applies to larger messages. With the maximum payload of messages with an average payload of 1.42 bpp, imperceptibility quality is also included in the exellent category, which is about 1.13 for MSE value, 47.59 dB for PSNR value, and 0.9977 for SSIM value.

REFERENCES

[1] K. M. Kordov and B. Stoyanov, "Least Significant Bit Steganography using Hitzl-Zele Chaotic Map," *International Journal of Electronics and Telecommunications,* vol. 63, no. 4, pp. 417-422, 2017.

[2] S. Islam, M. R. Modi, and P. Gupta, "Edge-based Image Steganography," *EURASIP Journal on Information Security,* vol. 2014, no. 1, 2014.

[3] A. K. Sahu, G. Swain and E. S. Babu, "Digital Image Steganography Using Bit Flipping," *Cybernetics and Information Technologies,* vol. 18, no. 1, pp. 69-80, 2018.

[4] D. R. I. M. Setiadi and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," *Cybernetics and Information Technologies,* vol. 18, no. 2, 2018 in Press.

[5] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 15, no. 4, pp. 1987-1995, 2017.

[6] A. K. Sahu and G. Swain, "An Improved Data Hiding Technique Using Bit Differencing and LSB Matching," *Internetworking Indonesia Journal,* vol. 10, no. 1, pp. 17-21, 2018.

[7] N. Jain, S. Meshram, and S. Dubey, "Image Steganography Using LSB and Edge – Detection Technique," *International Journal of Soft Computing and Engineering,* vol. 2, no. 3, pp. 217-222, 2012.

[8] W. Wang, J. Ye, T. Wang and W. Wang, "Reversible data hiding scheme based on significant-bit-difference expansion," *IET Image Processing,* vol. 11, no. 11, pp. 1002-1014, 2017.

[9] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi and C. A. Sari, "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," in *International Seminar on Application for Technology of Information and Communication (iSemantic)*, Semarang, 2017.

[10] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto and D. R. I. M. Setiadi, "An imperceptible LSB image hiding on edge region using DES encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, Salatiga, 2017.

[11] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and securing message on edge areas of image using LSB steganography and OTP encryption," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[12] W. Luo, F. Huang, and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics And Security,* vol. 5, no. 2, pp. 201-214, 2010.

[13] M. Nikolic, E. Tuba, and M. Tuba, "Edge Detection in Medical Ultrasound Images Using Adjusted Canny Edge Detection Algorithm," in *Telecommunications Forum (TELFOR)*, Belgrade, 2016.

[14] P. Kaur and B. Kaur, "2-D Geometric Shape Recognition using Canny Edge Detection Technique," in *International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016.

[15] E. Ortiz, K. W. Bowyer, and P. J. Flynn, "An optimal strategy for dilation based iris image enrollment," in *IEEE International Joint Conference on Biometrics*, Clearwater, 2014.

[16] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," in *International Conference on Information and Communications Technology (ICOIACT)*, Yogyakarta, 2018.

[17] R. Singh, P. Rawat, and P. Shukla, "Robust medical image authentication using 2-D stationary wavelet transform and edge detection," in *IET International Conference on Biomedical Image and Signal Processing (ICBISP)*, Wuhan, 2017.

[18] R. Mukherjee, A. Pundir, D. Mahato, G. Bhandari and G. J. Saxena, "A robust algorithm for morphological, spatial image-filtering and character feature extraction and mapping employed for vehicle number plate recognition," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2017.

[19] R. C. Gonzalez, R. E. Woods and S. L. Eddins, Digital Image Processing Using Matlab, Gatesmark Publishing, 2009.

[20] T. S. Le, V. N. Tran, and K. Hamamoto, "A robust and flexible license plate detection method," in *International Conference on Advanced Technologies for Communications (ATC)*, Hanoi, 2014.

[21] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Yogyakarta, 2017.

[22] S. Bhattacharyya, S. Mondal, and G. Sanyal, "A Robust Image Steganography using Hadamard Transform," in *International Conference on Information Technology in Signal and Image Processing*, Mumbai, 2013.