BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **18**, No 2
Sofia • 2018 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2018-0029

An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection

De Rosal Ignatius Moses Setiadi[1], *Jumanto Jumanto*[2]

[1]*Department of Informatics Engineering, Dian Nuswantoro University, Semarang 50131, Indonesia*
[2]*Department of Humanities, Dian Nuswantoro University, Semarang 50131, Indonesia*
E-mails: moses@dsn.dinus.ac.id ilhamj@dsn.dinus.ac.id

***Abstract*:** *The Internet is a public network with many issues of data transfer security. Steganography is a data transmission security technique that is done by hiding the message in a container media, such as an image. The media certainly has its limited payload to accommodate the embedded data. This paper proposes a method for increasing the payload of secret messages in an image. The edge area is used to accommodate more message bits because the image edge area can better tolerate pixel value changes. In this research paper, Canny and Sobel detectors are combined to get a wider edge area. This two-detector combined method provides a larger edge area for greater payload of messages while maintaining imperceptibility of stego-images.*

***Keywords*:** *Image steganography, LSB, Hybrid edge detection, Canny, Sobel.*

1. Introduction

The Internet is a public network which is accessible to everyone from various circles. Lots of activities are done by users there in the virtual world, one of which is sending messages [1]. Internet technology is developing more sophisticated, faster and cheaper modes, which are also accessible to users of mobile devices. This makes the number of internet users to increase from year to year. Security issues then rise, such as digital message theft [2, 3]. Various methods such as steganography, watermarking, secret sharing cryptography, and digital signatures, have consequently been introduced to address the problem [4-6].

Steganography is a technique for hiding digital messages into other digital media, such as images, audio, video, and others so that the messages can be disguised and not directly visible to the human vision. There are two kinds of steganography by domain, i.e., spatial domain and frequency domain [7]. Least Significant Bit (LSB) is a popular method in spatial domains [8]. LSB is not a new method. However, this method has many advantages, such as simple algorithm and the quality of imperceptibility of relatively good stego-image [6, 9]. This makes the LSB still open for more development and further research.

Steganography has several important aspects, such as imperceptibility and message capacity, that can be embedded [10]. Researches on steganography have concentrated on improving both aspects, e.g., studies [1, 11-13]. The studies propose the insertion of secret messages on the edge area of images based on the LSB method to improve the aspect of imperceptibility. This is due to higher sensitivity of the human eyes to changes in the smooth area than those in the image edge area [1, 14].

Each image has a different edge area which determines the number of messages that can be embedded. The more edges there are, the more messages can be embedded. There are many proposed popular edge detection algorithms, among others are the detections of the Sobel and Canny edges [10]. Each image edge detection method has its own advantages, and the results of each edge detection algorithm are different from one another [15]. In this research, two image edge detection methods are combined to provide a better edge area so that the area can be used as a place to embed a larger number of messages.

2. The state of the art

Yang et al. [1] proposed a steganographic LSB method using PVD and edge detection to obtain a large embedding capacity while maintaining the stego-image quality. In this study, the image is divided by segmentation using edge detection, so the image is divided into two areas, i.e., the edge area and smooth area. The edge area embeds more messages than the smooth area. This is because the edge image area can provide more tolerance to changes in the value of the pixel. This study has obtained the value of Peak Signal-to-Noise Ratio (PSNR) more than 33 dB with a message capacity of more than 80,000 bits. The cover image employed is a grayscale image with size of 512×512.

Goodarzi, Zaeim and Shahabi [16] combine two edge detection methods, i.e., Canny edge detection and Fuzzy logic edge detection. The result is a hybrid edge detection. Canny edge detection has obtained 6046 pixels of edge on the image flax, while Fuzzy detector 6323 pixels. When the two edge detections are combined, a 6849-pixel edge has been obtained. With more edge pixels, more message capacity can be embedded. In the baboon image of embedded message with 0.54 bpp (bits per pixel), a PSNR of 52.7 dB is obtained.

Singla and Juneja [17] suggest a steganography using adaptive 1-4-8 LSB on the image edge area. The edge detection method used is a hybrid method Canny detector and Fuzzy detector. The method has also incorporated the AES algorithm to encrypt messages before embedment. The cover image used is the RGB image, with a message embedded at 6 bits on the edge area and 2 bits on the smooth area. This method has obtained a PSNR value of 46.68 dB on the Lena image.

Bai et al. [11] also propose a steganographic LSB technique on the edge area. In the study, the pixels in the cover image are classified into two parts, i.e. edge pixels and non-edge pixels. The classification is done by using three types of edge detectors, namely Canny, Sobel, and Fuzzy. At the edge pixels, more secret bits are pinned by LSB substitution method. The experimental result has shown that the Fuzzy detector has the largest payload, while the Sobel detector has the smallest payload. On the

other hand, the Sobel detector has obtained the highest PSNR value among other detectors.

Kalra and Chhokar [15] propose a combination of Canny and Sobel edge detections to perform an image edge detection. This is done because the detections of Canny and Sobel have their respective advantages. Combining these two methods results in a more complex edge detection and a larger edge areas.

Based on related researches discussed above, the proposed method in this research combines Canny and Sobel edge detections to increase the capacity that can be embedded on the cover and the imperceptibility of the secret messages.

3. Theory of LSB steganography and image edge detector

3.1. LSB steganography

Steganography is a method used to hide data in a file with the intention to deceive the human vision system. LSB is a method in the highly popular spatial domain used in steganography. LSB is applied in a way to modify the smallest bit value of image pixels by changing them directly [6, 9]. LSB is traditionally done by changing the smallest bit values in a sequential order. When there is an image pixel value {250, 120, 80, 175} and there is a message with a value of 10, then the steps taken to insert the message are as follows:

1. First, convert the pixel values of images and messages into bit numbers
   Cover {250: 1111101**0** | 120: 0111110**0** | 80: 0101000**0** | 175: 1010111**1**},
   Message {10: 1010}.
2. Next, change the smallest bit of image pixel value with each bit value of the message.
   Thus, the Stego's bits becomes {1111101**1** | 0111110**0** | 0101000**1** | 0101110**0**}.
3. Finally re-convert pixel image bit value into decimal number.
   The decimal value of Stego-pixels becomes {**251** | 120 | **81** | **174**}.

A steganography research using LSB method is very simple, so this method is also very predictable and unsafe anymore. But until now this method is still being investigated to improve the image quality and safety. This is due to the advantages possessed by LSB in good imperceptibility quality, so the human sensory system cannot detect small changes that occur. Therefore, to improve the quality, payload, and security of message insertion, LSB is combined with several methods, such as insertion in edge areas [12, 16], cryptographic techniques, adaptive and dynamic LSB [14], and so forth.

3.2. Canny edge detector

Canny is one of the popular edge detection algorithms, which was invented by John Canny [18] in 1986. Canny edge detection has the advantage of being able to detect the edge of the original image with a small error tie so as to obtain the edge of the optimal image. This detector has been widely used in various image processing algorithms that require edge detection. Performance of edge detection is highly dependent on the threshold value used [19]. This makes it very popular and widely used because it successfully provides standardized localization solutions and

complex mathematical calculations to collect smoothing filters. Canny can also reduce many inputs to a certain edge [20].

3.3. Sobel edge detector

Sobel is one of the popular edge detection operators [21], like Canny. The two advantages of this algorithm are that it obtains an effect to reduce random noise in the image and that it gives off lighter and brighter-looking edge elements [22]. The Sobel operator is a partial derivative of $f(x, y)$ where x = 3 and y = 3, which technically can compute the gradient of the image intensity. If there is an image (I), then we use the horizontal T_x and vertical T_y templates to convolve the image to get the edge area, with T_x and T_y:

(1) $$T_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix},$$

(2) $$T_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}.$$

4. The proposed method

Based on the background previously presented, this study proposes a steganographic method based on edge detection. The edge detection used is a combination of Canny and Sobel edge detections. The method being proposed is divided into three main processes, i.e., a process to generate hybrid edge detections, a process of embedding messages, and a process of extracting messages. The following describes the three processes of the method being proposed into details.

4.1. The process to generate hybrid edge detections

The idea of this proposed hybrid edge detection is simple, i.e., using an OR-operation to combine Canny and Sobel edge detections. The first step is done by reading the cover image, and then conducting an edge detection one after the other (Canny or Sobel first, and then the other). The result of Canny edge detection is saved at the variable C_{ea}, while that of Sobel edge detection at the variable S_{ea}. The result of edge detection is a binary number, with 1 as edge area and 0 as non-edge area. The second step is done by conducting an OR-operation on both edge detection results to obtain a hybrid edge detection:

(3) $$\mathrm{CS}_{\mathrm{ea}} = C_{\mathrm{ea}} \parallel S_{\mathrm{ea}},$$

where the obtained $\mathrm{CS}_{\mathrm{ea}}$ is a variable for saving the combination of the two edge detections. Fig. 1 shows an example of combining the two edge detections on the Lena image.

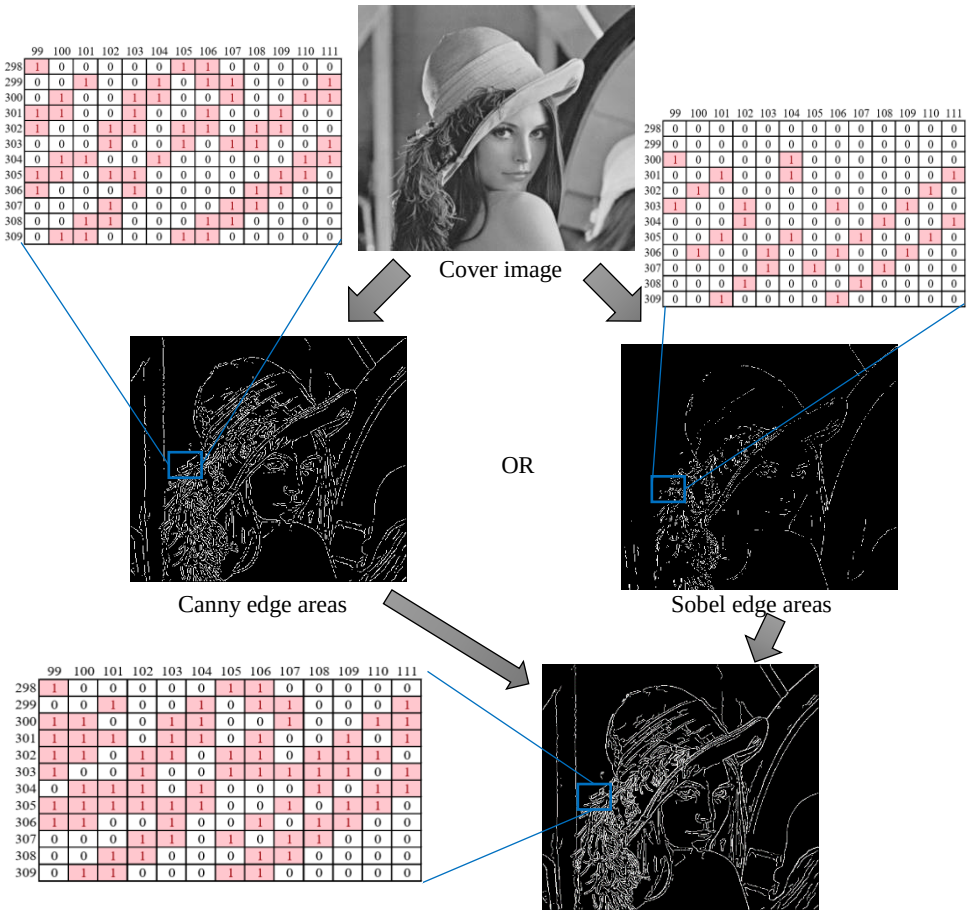

Fig. 1. Process to generate hybrid edge detections

4.2. The process of embedding secret messages

In this process, the secret message is embedded in the cover edge area of the cover image by first altering the message in binary. The secret message has a special character that is used as the final sign of the message. Fig. 2 illustrates the steps in this embedding process.

Here are the details of the steps of the embedding process as shown in Fig. 2.

Read cover image.

Perform edge detection with the Canny method and Sobel method, then save each edge area of each method.

Do a combination of the edge area of a Sobel and a Canny using the OR-operation, so that the image edge area is based on a combination of Canny and Sobel detections with the formula (3). Save the area for use in the extraction process.

Read the secret message, then add one special character at the end of the message.

Change the secret message to binary form according to ASCII.

Reshape binary messages in vector form.

Check the large message. If enough messages to enter to the edge area then the priority message is entered into the edge area. If not enough, then the rest of the message is entered into the smooth area.

Embed the secret message into the smallest bit of the image edge pixel cover with the LSB replacement method.

Get the stego-image.

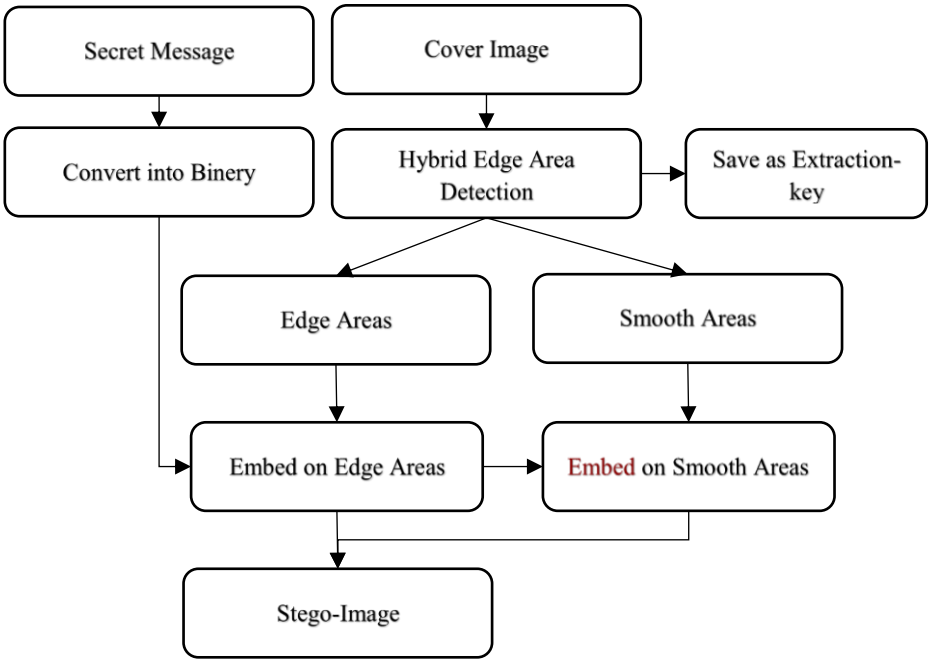

Fig. 2. Phase of embedding secret messages

4.3. The process of extracting secret messages

This process is the stage for obtaining a message extraction. In order to obtain a perfect extraction, the extraction process must use the hybrid edge detectors. Fig. 3 illustrates the extraction process in the proposed method.

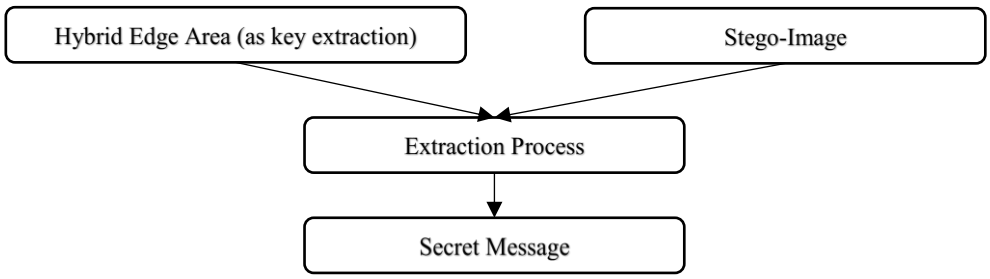

Fig. 3. Phase of extracting secret messages

Here are the details of the steps of the embedding phase as shown in Fig. 3.

1. Read stego-image.

2. Read hybrid edge area as a key of extraction.
3. Perform the extraction process by converting each pixel into binary form.
4. Get the smallest bits sequentially from the first edge area through the last smooth area.
5. Combine each of the eight smallest bits of each pixel into a character.
6. Repeat the iteration to get special characters that become the final signs of the messages.
7. Get secret message extraction.

5. Experimental result and analysis

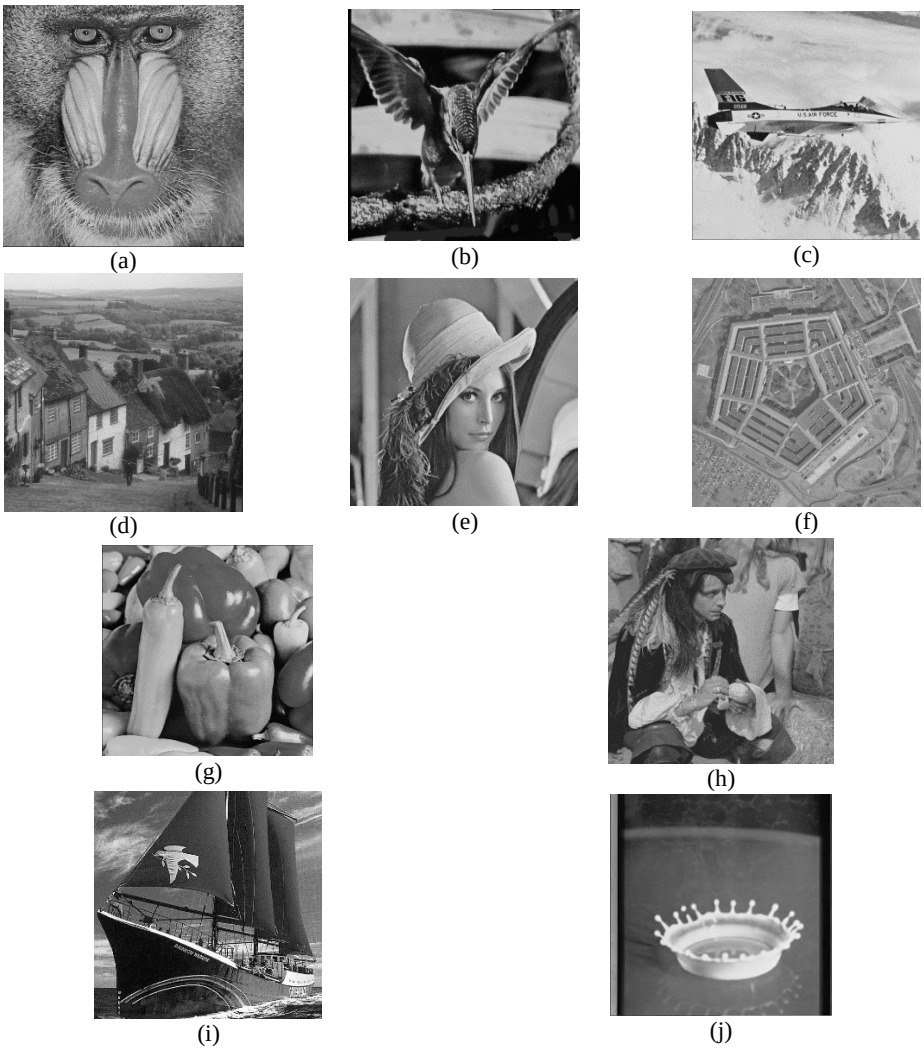

Fig. 4. Cover images used {baboon (a); bird (b); f16 (c); goldhill (d); lena (e); Pentagon (f); peppers (g); pirate (h); ship (i); splash (j)}

This experiment conducts a trial test, on 10 grayscale images standard with size 512×512 pixels as cover image and text as messages to be embedded. Each cover image analyzes and compares the payload capacity of messages that can be embedded in the image edge area. Fig. 4 shows 10 cover images used in this test.

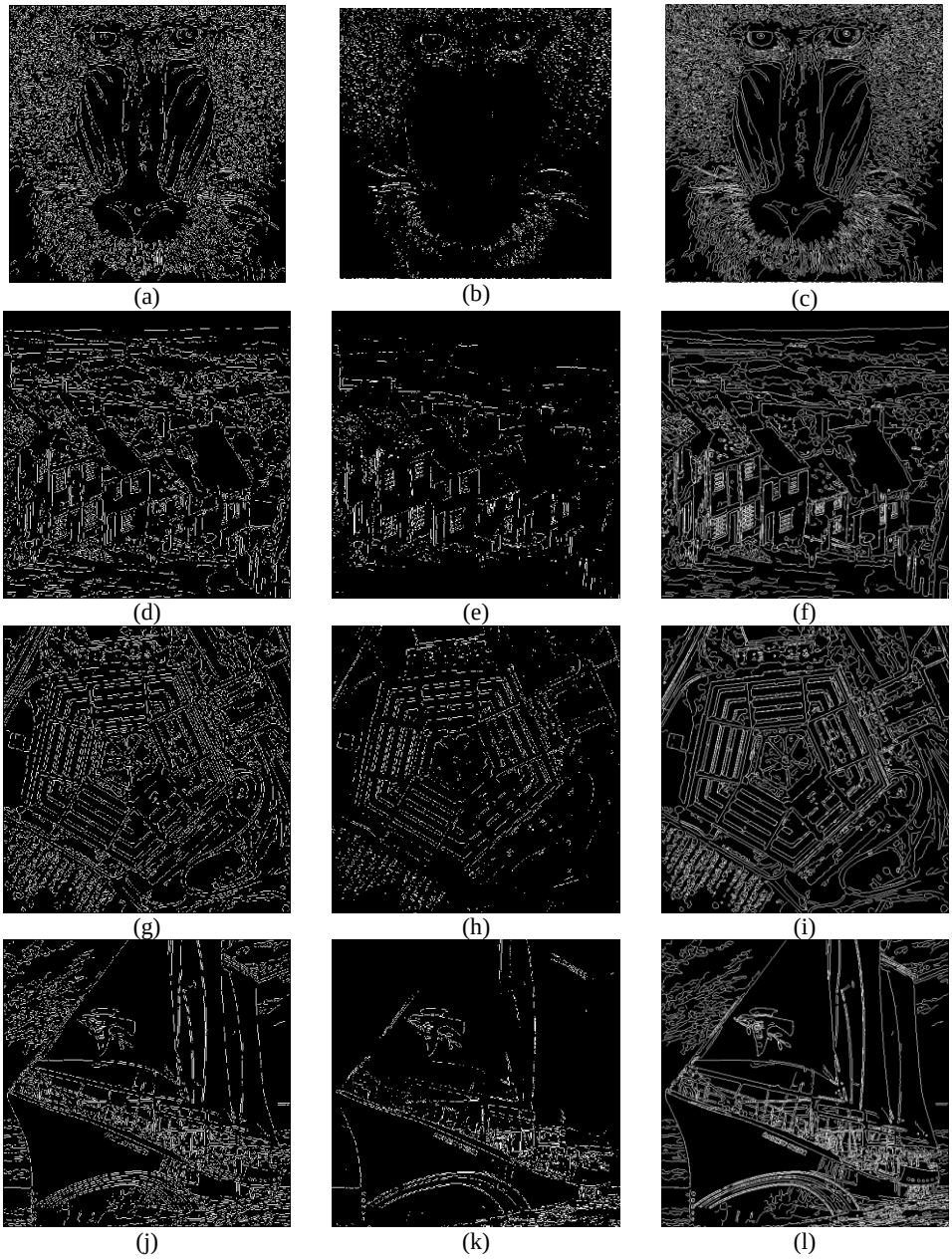

Fig. 5. Edge areas of cover image {Baboon-canny (a); Baboon-Sobel (b); Baboon-hybrid (c); Goldhill-canny (d); Goldhill-Sobel (e); Goldhill-hybrid (f); Pentagon-canny (g); Pentagon-Sobel (h); Pentagon-hybrid (i); Ship-canny (j); Ship-Sobel (k); Ship-hybrid (l)}

Prior to the insertion of secret messages, each cover image does an edge detection with a Sobel, a Canny and hybrid algorithms. This edge area will be used as a container for storing messages. Fig. 5 is a sample of edge detection of the cover image used (baboon.bmp, goldhill.bmp, pentagon.bmp, and ship.bmp).

The edge area shown in Fig. 5 has a significant difference. The edge area obtained from the Canny-Sobel hybrid method has a very clear border. Based on the results of calculations, it is also evident that the entire image of the cover has a bigger number of hybrid Canny-Sobel edge area than the edge area of the Sobel and Canny individually. The details on the results of calculations can be seen in Table 1.

Table 1. Number of edge area pixels based on various edge detections

No	Image	Number of edge area pixels		
		Hybrid	Canny	Sobel
1	baboon	47,187	41,892	12,672
2	bird	21,630	18,452	9,157
3	Lena	21,882	18,427	8,311
4	ship	31,103	26,053	12,554
5	f16	22,322	18,907	9,472
6	Pentagon	35,922	31,415	13,208
7	peppers	20,411	18,056	6,777
8	splash	20,185	19,373	4,284
9	pirate	30,227	26,724	9,512
10	goldhill	32,209	28,098	10,783

As seen in Table 1 the hybrid method has proven to increase the number of image edge areas. The number of image edge areas greatly affects the amount of payload capacity of messages that can be embedded in the image. Study [11], also proves that edge detection with a Sobel algorithm has a smaller payload compared to a Canny, whereas by inserting a message according to the maximum payload, of course, the Sobel algorithm gets the best imperceptibility quality and this has also been proved. In the research, however, there is no trial insertion of messages with the same payload, so we cannot know the quality of imperceptibility with the same payload number of the messages. This study compares the imperceptibility quality of stego-images of the same message payload capacity. The quality of imperceptibility is measured by a PSNR. A PSNR is calculated by the next formula.

$$\text{PSNR} = 10 \log 10 \left(\frac{\max^2}{\sqrt{\sum_{0=0}^{O-1} \sum_{p=0}^{P-1} \sum_{q=0}^{Q-1} \| S_i(o,p,q) - C_i(o,p,q) \|^2}} \right), \quad (4)$$

where max is maximum of pixel intensity, for grayscale image is 255; S_i is stego-image; C_i is cover image; o, p, q are size of image.

There are three different sizes of text messages embedded on each cover image, i.e., 64 bits, 1024 bits, and 8192 bits. Each bit is inserted on each pixel of the cover image contained in the edge area. The measured PSNR values are shown in Figs 6-8.

From the results of PSNR shown in Fig. 6, it appears that the message embedded in the hybrid area of Canny and Sobel has the best value with an average PSNR of 91.46965 dB followed by a Canny with 89.5630 dB and a Sobel with 88.31.48 dB. Fig. 7 also has features similar to Fig. 6, i.e., PSNR excellence that is pinned in the edge area of the hybrid Canny and Sobel. It gets the best value compared to a

detection by a Canny or a Sobel only. The average PSNR on the hybrid algorithm is 78.7471 dB followed by a Canny with 78.1246 dB and a Sobel with 76.3178 dB.

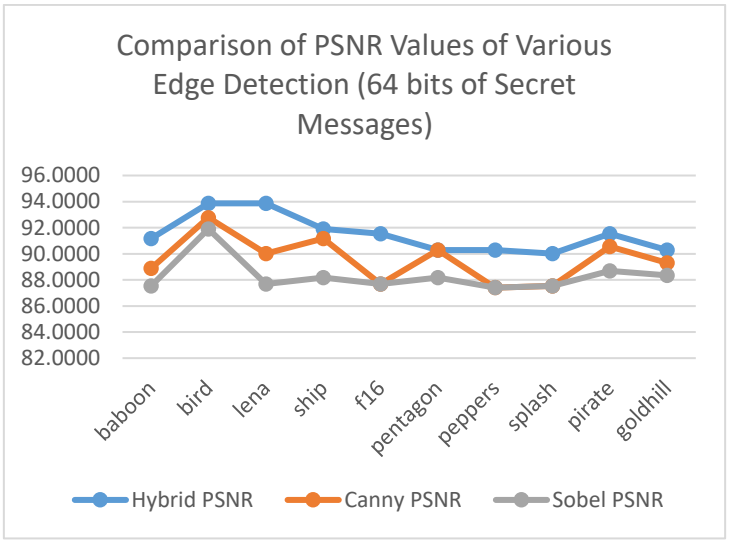

Fig. 6. Comparison of PSNR values of various edge detections for 64 bits of secret messages embedded

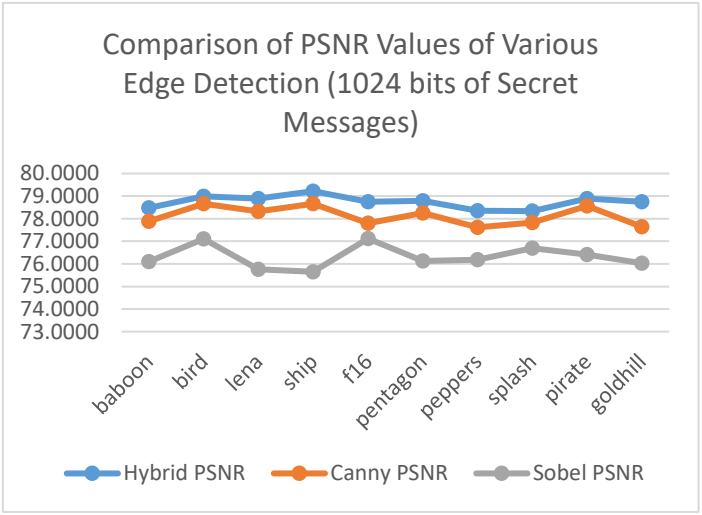

Fig. 7. Comparison of PSNR values of various edge detections for 1024 bits of secret messages embedded

The chart in Fig. 8 also shows the advantages of the proposed method in which the PSNR stego-image with the hybrid method looks superior with an average value of 69.336 dB, while detections by a Canny obtains 69.0735 dB and by a Sobel 67.4548 dB. This proves that the aspect of imperceptibility with the hybrid method is superior to the others. The payload aspect is also measured in units of bits per pixel (bpp). Formula (5) is the bpp formula used in this study.

(5) $$\text{bpp} = \frac{\text{max bits of secret message}}{A \times B},$$

with A and B as the height and width of the cover image

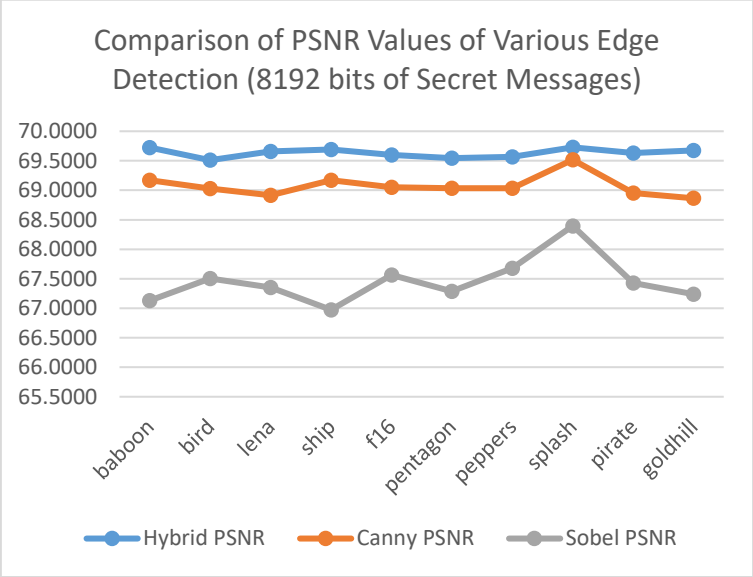

Fig. 8. Comparison of PSNR values of various edge detections for 8192 bits of secret messages embedded

The test results above are received by inserting a maximum of two smallest bits in the edge area and one small bit in the smooth area. Table 2 shows that the use of the hybrid edge detection method can increase the payload of embedded messages. This can be evidently seen from the average value of a higher bit per pixel (bpp) and PSNR in the category. The experiment also tests two kinds of hybrid techniques, i.e., the hybrid *x*-*y*-*z* and the hybrid *x*-*y*. The difference is that, the edge area (*y*) of the hybrid *x*-*y* method embeds a 2-bit message, while the smooth area (*x*) embeds a 1-bit message. In the hybrid method *x*-*y*-*z*, 3 bits embed a message in the area of intersecting edges (*z*), 2 bits at the edges of the area that do not intersect (*y*), and 1 bit in the smooth areas (*x*). The values of *x*, *y*, and *z* here are variables that can be changed in value according to the need. The greater value is entered, the greater the value of bpp is. However, the value of PSNR in this method is getting smaller. Table 3 shows the maximum of payload capacity, the number of bits per pixels, and the PSNR averages of the 10 images with different *x*, *y* and *z* values.

Tables 2 and 3 show the parameter values of *x*, *y*, and *z*, with the maximal values recommended for the Hybrid *x*-*y*, i.e., x=4 and y=3. A bigger parameter value will significantly affect the quality of a stego-image, but this is not recommended here. Insertion of a message is done by an iteration adjusted to the parameter value. Here, the first iteration is inserted in the smallest bit at the edge area, and the second iteration is in the second smallest bit at the edge area. The third iteration is inserted in the smallest bit at the smooth area. The fourth iteration is inserted in the third smallest bit at the edge area, and the fifth iteration is in the second smallest bit at the

smooth area. This process is done throughout all the messages until they are all inserted. Meanwhile, for the Hybrid *x-y-z*, the recommended parameter values are *x*=5, *y*=4, and *z*=3. The insertion technique is the same as that for the Hybrid *x-y*. The difference is that priority of insertion starts from the edge area cut of the two edge detections, and then the edge area outside the cut area, and then the smooth area. The extraction process needs a key, i.e., the edge area of the cover image which has been saved in the message insertion process. The default reading of messages starts from the smallest bit at the edge area through the smooth area. Steps of extraction are to be adjusted to the insertion process. Table 4 shows the message extraction results of the stego-images employed.

Table 2. Bit per pixel (bpp) and PSNR values in various edge detections

No	Image	Hybrid *x-y-z*		Hybrid *x-y*		Canny		Sobel	
		bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR
1	baboon	1.20815	46.5772	1.18000	47.9508	1.15981	48.2161	1.0483	50.0277
2	bird	1.10532	47.4977	1.08251	49.3007	1.07039	49.5578	1.0349	50.2977
3	Lena	1.10200	48.0815	1.08347	49.3833	1.07029	49.6165	1.0317	50.4003
4	ship	1.14727	46.5429	1.11865	48.2682	1.09938	48.5748	1.0479	49.4372
5	f16	1.10826	47.8227	1.08515	49.3379	1.07212	49.5680	1.0361	50.2746
6	Pentagon	1.17022	46.7560	1.13703	48.5241	1.11984	48.7805	1.0504	49.9861
7	peppers	1.09473	48.2425	1.07786	49.4588	1.06888	49.6219	1.0259	50.4933
8	splash	1.09024	48.5170	1.07700	49.4951	1.07390	49.5527	1.0163	50.7357
9	pirate	1.13823	47.4815	1.11531	48.8892	1.10194	49.1012	1.0363	50.2952
10	goldhill	1.14832	47.2629	1.12287	48.7516	1.10718	48.9956	1.0411	50.1926
Average		1.13127	47.4782	1.10798	48.9360	1.09437	49.1585	1.03689	50.2140

Table 3. Average max capacity, bit per pixel (bpp), and PSNR values in hybrid edge detections from all images

Method	Max capacity, bits	bpp	PSNR, dB
x-y-z (*x*=4, *y*=3, *z*=2)	558700.7	2.1312738	40.03984
x-y (*x*=3, *y*=2)	552595.8	2.1079859	41.07054
x-y-z (*x*=5, *y*=4, *z*=3)	820844.7	3.1312738	33.96991
x-y (*x*=4, *y*=3)	814739.8	3.1079859	34.32479

A steganography research seeks for a method which is effective in enhancing significant aspects of steganography, i.e., security, payload capacity, and imperceptibility quality. However, a perfect message extraction should also be considered in the enhancement process. This research has proposed a method for a perfect message extraction, as shown in Table 4. Information can be maintained through a perfect message extraction. Otherwise, missing information, if any, can change the meaning of a hidden message.

Table 4. Extraction results with sample messages from all images

Image	Message	Message length	Message extraction	Note
Baboon	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Bird	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Lena	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Ship	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
f16	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Pentagon	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Peppers	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Splash	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Pirate	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted
Goldhill	My Name is …… Indonesia	104 bits	My Name is …… Indonesia	Successfully extracted
	The Internet is …system	30928 bits	The Internet is …system	Successfully extracted

6. Conclusion

The edge area of the image is an insensitive part of the pixel value change. It is used in the science of steganography on the image. Inserting message bits in the edge area also serves as an alternative solution to improve the security of message insertion. We have come to the conclusion that these two advantages can be obtained when we apply steganographic techniques. The experiment conducted in this study has proven

that the edge area detected by combining the two methods, i.e., a Canny and a Sobel can significantly expand and, therefore, the payload capacity of messages that can be inserted in the edge area increases. The experiment has also proven that inserting messages on the hybrid edge area with the same payload message is better than the case of the Canny edge area or the Sobel edge area. The average number of bpp with the 10 images also shows that with the proposed hybrid method, the number of bits of messages is bigger than that with only one edge detection method. The value of PSNR obtained is also high. The experiment has obtained 1.13127 bits per pixel and a PSNR of 47.4782 dB through the hybrid *x-y-z* method, with the value $x = 1$ bit, $y = 2$ bits, and $z = 3$ bits. The *x-y* hybrid method can pin 1.10798 bits per pixel with a PSNR of 48.9360 dB. The *x-y-z* value here can be adjusted to the payload capacity of the message, but it is still advisable to keep the PSNR value above 30 dB for good stego-image quality. This way, the image cannot be detected or perceived by the human visual system.

References

1. Yang, C.-H., C.-Y. Weng, S.-J. Wang, H.-M. Sun. Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems. – IEEE Transactions on Information Forensics and Security, Vol. **3**, 2008, No 3, pp. 488-497.
2. Verma, M., R. Rani. Significant Secret Image Sharing Scheme Based on Boolean Operation. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 2, pp. 134-150.
3. Setiadi, D. R. I. M., T. Sutojo, E. H. Rachmawanto, C. A. Sari. Fast and Efficient Image Watermarking Algorithm Using Discrete Tchebichef Transform. – In: International Conference on Cyber and IT Service Management (CITSM'17), Denpasar, 2017.
4. Nag, A., S. Biswas, D. Sarkar, Partha. Secret Image Sharing Scheme Based on a Boolean Operation. – Cybernetics and Iformation Technologies, Vol. **14**, 2014, No 2, pp. 98-113.
5. Ardy, R. D., O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, E. H. Rachmawanto. Digital Image Signature Using Triple Protection Cryptosystem (RSA, Vigenere, and MD5). – In: International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS'17), Yogyakarta, 2017.
6. Setiadi, D. R. I. M., H. A. Santoso, E. H. Rachmawanto, C. A. Sari. An Improved Message Capacity and Security Using Divide and Modulus Function in Spatial Domain Steganography. – In: International Conference on Information and Communications Technology (ICOIACT'18), Yogyakarta, 2018.
7. Setyono, A., D. R. I. M. Setiadi, Muljono. StegoCrypt Method Using Wavelet Transform and One-Time Pad for Secret Image Delivery. – In: International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE'17), Semarang, 2017.
8. Zhu, Z., T. Zhang, P. Zhu, B. Wan, X. Hou. Steganalysis of AE-LSB Steganography Based on Pixel Value Differencing. – In: International Conference on Natural Computation (ICNC'13), Shenyang, 2013.
9. Astuti, Y. P., D. R. I. M. Setiadi, E. H. Rachmawanto, 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'18), Yogyakarta, 2018.
10. Singla, D., M. Juneja. An Analysis of Edge Based Image Steganography Techniques in Spatial Domain. – In: Recent Advances in Engineering and Computational Sciences (RAECS'14), Chandigarh, 2014.
11. Bai, J., C.-C. Chang, T.-S. Nguyen, C. Zhu, Y. Liu. A High Payload Steganographic Algorithm Based on Edge Detection. – Displays, Vol. **46**, 2017, No 1, pp. 42-51.

12. I s l a m, S., M. R. M o d i, P. G u p t a. Edge-Based Image Steganography. – EURASIP Journal on Information Security, Vol. **2014**, 2014, No 1.
13. I r a w a n, C., D. R. I. M. S e t i a d i, C. A. S a r i, E. H. R a c h m a w a n t o. Hiding and Securing Message on Edge Areas of Image Using LSB Steganography and OTP Encryption. – In: International Conference on Informatics and Computational Sciences (ICICoS'17), Semarang, 2017.
14. M o h a m e d, M. H., N. M. A L-A i d r o o s, M. A. B a m a t r a f. A Combined Image Steganography Technique Based on Edge Concept & Dynamic LSB. – International Journal of Engineering Research & Technology (IJERT), Vol. **1**, 2012, No 8, pp. 1-7.
15. K a l r a, A., R. L. C h h o k a r. A Hybrid Approach Using Sobel and Canny Operator for Digital Image Edge Detection. – In: International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE'16), Ghaziabad, 2016.
16. G o o d a r z i, M. H., A. Z a e i m, A. S. S h a h a b i. Convergence between Fuzzy Logic and Steganography for High Payload Data Embedding and More Security. – In: International Conference on Telecommunication Systems, Services, and Applications (TSSA'11), Bali, 2011.
17. S i n g l a, D., D. M. J u n e j a. New Information Hiding Technique Using Features of Image. – Journal of Emerging Technologies in Web Intelligence, Vol. **6**, 2014, No 2, pp. 237-242.
18. C a n n y, J. A Computational Approach to Edge Detection. – IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. **PAMI-8**, 1986, No 6, pp. 679-698.
19. N i k o l i c, M., E. T u b a, M. T u b a. Edge Detection in Medical Ultrasound Images Using Adjusted Canny Edge Detection Algorithm. – In: Telecommunications Forum (TELFOR'16), Belgrade, 2016.
20. K a u r, P., B. K a u r. 2-D Geometric Shape Recognition Using Canny Edge Detection Technique. – In: International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016 .
21. J i n-Y u, Z., C. Y a n, H. X i a n-X i a n g. Edge Detection of Images Based on Improved Sobel Operator and Genetic Algorithms. – In: International Conference on Image Analysis and Signal Processing, Linhai, 2009.
22. G a o, W., X. Z h a n g, L. Y a n g, H. L i u. An Improved Sobel Edge Detection. – In: IEEE International Conference on Computer Science and Information Technology (ICCSIT'10), Chengdu, 2010.

Received 05.11.2017; Second Version 08.05.2018; Accepted 21.05.2018