Journal of Physics: Conference Series **1528** (2020) 012038 doi:10.1088/1742-6596/1528/1/012038

A comparison of joint reversible data hiding methods in encrypted remote sensing satellite images

Ali Syahputra Nasution* and Gunawan Wibisono

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, 16424, Jakarta, Indonesia

*ali.syahputra@ui.ac.id

Abstract. The distribution of remote sensing satellite data from the National Remote Sensing Data Bank (BDPJN) of the National Institute of Aeronautics and Space (LAPAN) to users via the internet requires security so that it is not used illegally by unauthorized parties. Encryption and reversible data hiding are two effective and popular privacy protection and confidential communication solutions. With encryption, data is randomized so it can't be read. Whereas with reversible data hiding, the receiver can extract hidden data and restore the original image without distortion. In this paper, some remote sensing satellite images are used as input in the simulation that is analyzed and compared based on the three methods of joint reversible data hiding in encrypted images, i.e. Zhang's work, Hong's work, and Fatema's work. The experimental results show that Hong's et al. method reveals the best performance of the three methods. For example, when the block size is 8x8, the bit error rate (BER) of the SPOT-6 test image of Hong's et al. method was 12.06%, which is slightly lower than the 14.01% Zhang's method and 11.89% Fatema's et al. method. Likewise, the quality of remote sensing satellite image (image_spot6) recovery represented by the peak signal to noise ratio (PSNR) of Hong's et al. method is 49.96 dB, which is quite higher than the 48.26 dB of Zhang's method and 48.98 dB of Fatema's et al. method.

1. Introduction

The development of internet technology, not only makes it easier to transmit various media/files such as images, pictures, audio, and video but also makes it easier for unauthorized parties to copy and distribute these files without paying appropriate compensation to the content owner [1]. Therefore, problems arise as to how the media can be protected from unauthorized use or operation.

Three basic security requirements that must be met to obtain a secure image transmission are confidentiality, authenticity, and integrity [2]. Encryption and data hiding are two effective and popular ways of protecting the privacy and confidential communications. Encryption techniques convert plaintext content into unreadable chipper text. Data hiding techniques embed secret messages or bits of information into cover media such as images, images, audio or video by making a few modifications. In areas such as medical and military applications, two very important things to consider are encrypting the image before data hiding and restoring the original image correctly after data extraction. If the receiver can recover the original cover image after extracting hidden information without distortion, then this is called reversible data hiding.

Currently, there are many researchers interested in conducting research related to reversible data hiding in encrypted images (RDHEI) [3-12]. There are three roles in the RDHEI scheme, namely,

content owner, data hiding, and receiver. According to when the embedding space for additional data is created, the existing RDHEI method can be classified into two categories: ‘‘vacating room before encryption (VRBE)” [13] and “vacating room after encryption (VRAE)” [3]. The VRAE method can then be divided into two categories: the joint method [3-7] and the separable method [8-12]. In the joint RDHEI method, as shown in Figure 1, embedded data can only be extracted after image decryption. In other words, additional data must be extracted from the plaintext domain, so that the main content is disclosed after data extraction.

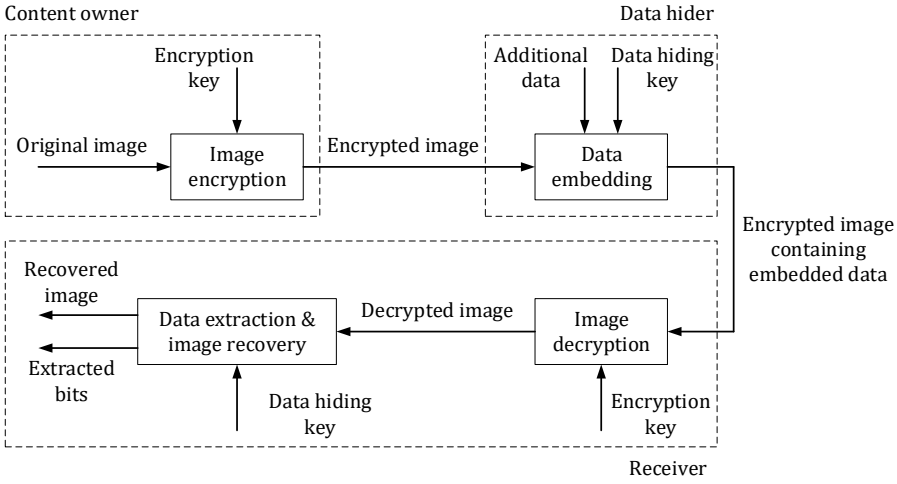

Figure 1. Joint reversible data hiding scheme on encrypted images [3].

Some of the high-resolution remote sensing imageries in Table 1, are commercial and are limited by licensing in terms of data usage, where remote sensing satellite imageries are widely used by users/stakeholders to obtain information about natural resources, disasters, spatial planning. Therefore, the application of encryption and reversible data hiding techniques in high-resolution remote sensing satellite images is very useful for maintaining data security when distributed over the internet network (electronic media). This activity supports the role of LAPAN in Act Number 21 of 2013 concerning Space [14] and in Government Regulation Number 11 of 2018 regarding Procedures for Organizing Remote Sensing Activities [15] where LAPAN is required to collect, store, process, and distribute data through the National Remote Sensing Data Bank (BDPJN) as a remote sensing data network node in the spatial data network system national.

Table 1. Some high-resolution remote sensing satellites.

Satellites	Spatial Resolution (m)	
	Multispectral	Panchromatic
SPOT 6	6	1.5
SPOT 7	6	1.5
PLEIADES	2.8	0.7

The objective of the research is to implement a simulation in MATLAB, to analyze and to compare joint reversible data hiding methods in encrypted remote sensing satellite images based on Zhang’s work [3], Hong’s et al. work [4], and Fatema’s et al. work [7]. The algorithm will be implemented in the MATLAB language. Satellite imageries will be used to test the program. This simulation will analyze bit error rate (BER) and also peak signal to noise ratio (PSNR) of recovered image quality.

2. Method

The research methodology, as shown in the Figure 2, consists of 4 stages, namely satellite image encryption, data embedding, image decryption, data extraction, and image recovery. In the sender side,

to begin image encryption phase, original satellite image is loaded and resize it into a size of 512 x 512 pixels. Then, the color image is extracted into individual red, green, blue channels. After that, the original satellite image is encrypted by an encryption key by applying bitwise exclusive-or (XOR). Let I is an 8-bit uncompressed cover image of size 512 x 512.

In data embedding stage, the block size value (s) is assumed. Then, the data hider segments the encrypted image into several non-overlapping blocks sized by s x s. Next, generate the data message to embed in the encrypted image by considering a matric of 0 and 1. Get two sets S0 and S1 using the data hiding key. If data hiding key values at the pixel position is 0, then it goes into set S0 otherwise set S1. If the additional bit to be embedded is '0' in each block of red channel image, flip the three least significant bits (LSB) of each encrypted pixel in set S0 and pixel in set S1 is not changed. On the other hand, If the additional bit to be embedded is '1', flip the three LSB of each encrypted pixel in set S1 and pixel in set S0 is unchanged. After that, the resultant of red, green, blue channels is combined to get the encrypted image with additional data.

In the receiver side, to begin image decryption phase, after receiving the encrypted image with additional data, the receiver decrypts it with a decryption key by applying bitwise XOR. In the data extraction and image recovery phase, the decrypted image with additional data is decomposed into red, green, blue channels. Then, the decrypted red channel image is segmented into several non-overlapping blocks sized by s x s. Next, each pixel in each block is divided into two sets newS0 and newS1 in the same way. If data hiding key values at the pixel position is 0, then it goes into set newS0, otherwise set newS1. Flip 3 LSB in set newS0 and newS1 to get two set S00 and S11. After that, make two set H0 and H1. If data hiding key values at the pixel position is '0', then set S00 and newS0 goes into set H0 and H1, respectively. Otherwise set newS1 and S11 go into set H0 and H1, respectively. After that, calculate fluctuation H0 and H1 to determine which one is the original image by following equation:

- Fluctuation calculation of Zhang's method [3]

$$f_Z = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4}\right| \quad (1)$$

- Fluctuation calculation of Hong's et al. method [4]

$$f_H = \sum_{u=1}^{s}\sum_{v=1}^{s-1}\left|p_{u,v} - p_{u,v-1}\right| + \sum_{u=1}^{s-1}\sum_{v=1}^{s}\left|p_{u,v} - p_{u+1,v}\right| \quad (2)$$

- Fluctuation calculation of Fatema's et al. method [7]

$$f_F = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v} - p_{u-1,v}\right| + \left|p_{u,v} - p_{u+1,v}\right| + \left|p_{u,v} - p_{u,v-1}\right| + \left|p_{u,v} - p_{u,v+1}\right| \quad (3)$$

Hereinafter, combine the red channel with the green and blue channels to give the recovered original image. Finally, Calculate BER by comparing each pixel from the original matric data message with a recovered data message and PSNR [12] to measure the quality of the final recovered image.

$$PSNR(I_o I_m) = 10\ x\ \log_{10}\frac{255^2}{MSE} \quad (4)$$

$$MSE = \frac{1}{M\ x\ N}\sum_{x=1}^{M}\sum_{y=1}^{N}[I_o(x,y) - I_m(x,y)]^2 \quad (5)$$

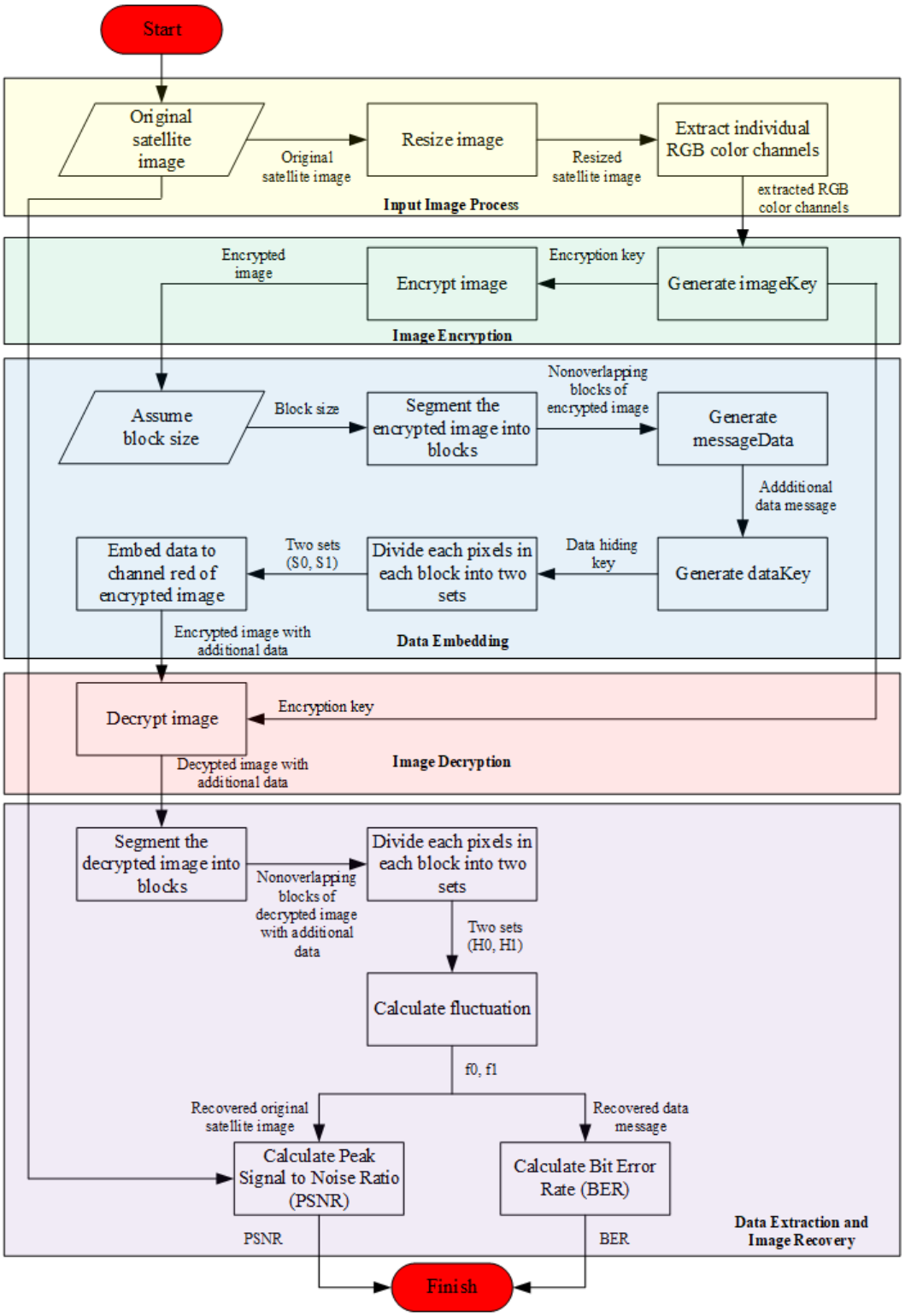

Figure 2. Research methodology.

The implementation is created in MATLAB. The images used to test the software, as shown in Figures 3, 4, and 5 are some standard processing high-resolution satellite images, i.e. SPOT-6, SPOT-7, and Pleiades-1A, that has been resized to 512 x 512 where each pixel is represented by 8 bits. The input satellite images can be seen in Figures 2, 3, and 4. The three joint reversible data hiding in

encrypted image algorithms of Zhang [3], Hong et al. [4], and Fatema et al. [7] are compared here with various block size. In this research, two important performance parameters will be analyzed:

- Bit Error Rate (BER); this parameter shows the ratio of unrecovered bits to the total number of embedded bits.
- PSNR (Peak Signal to Noise Ratio); this parameter is to show the differences between the original image and the recovered original image.

Figure 3. SPOT-6 image (image_spot6).

Figure 4. SPOT-7 image (image_spot7).

Figure 5. Pleiades-1A image (image_pleiades1A).

3. Results and Discussion

The complete results are shown in Tables 2, 3 and 4. The contents of the table are block size (s), total message (bit), incorrect message (bit), BER, and PSNR of the three compared methods. Table 1 is a summary result for the SPOT-6 original image of the three different algorithms. Table 2 is a summary result for the SPOT-7 original image of the three different algorithms. Table 3 is a summary result for the Pleiades-1A original image of the three different algorithms.

Table 2. Complete joint RDHEI results of the SPOT-6 image.

Images	Block Size (s)	Total Message (bit)	Zhang [3]			Hong et al. [4]			Fatema et al. [7]		
			Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)
SPOT6_ 20180509.tif	2	65536	32878	50,17	42,6747	26155	39,91	43,8105	32862	50,14	42,6722
	4	16384	5855	35,74	44,1922	4405	26,89	45,4557	5261	32,11	44,6679
	6	7225	1747	24,18	45,9324	1219	16,87	47,5219	1488	20,6	46,6266
	8	4096	574	14,01	48,2690	391	9,55	49,9670	487	11,89	48,9897
	10	2601	234	9	50,2080	145	5,57	52,3283	170	6,54	51,6338
	12	1764	81	4,59	53,2514	63	3,57	54,3403	74	4,2	53,6643
	14	1296	31	2,39	56,0852	20	1,54	57,9739	25	1,93	56,9538
	16	1024	10	0,98	59,8211	5	0,49	62,8806	9	0,88	60,3121
	18	784	3	0,38	64,1041	1	0,13	68,7957	2	0,26	65,9001
	20	625	0	0	Inf	0	0	Inf	0	0	Inf
	22	529	1	0,19	66,9692	2	0,38	64,0236	1	0,19	67,0305
	24	441	0	0	Inf	0	0	Inf	0	0	Inf
	26	361	0	0	Inf	0	0	Inf	0	0	Inf
	28	324	0	0	Inf	0	0	Inf	0	0	Inf
	30	289	0	0	Inf	0	0	Inf	0	0	Inf
	32	256	0	0	Inf	0	0	Inf	0	0	Inf

Table 3. Complete joint RDHEI results of the SPOT-7 image.

Images	Block Size (s)	Total Message (bit)	Zhang [3]			Hong et al. [4]			Fatema et al. [7]		
			Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)
SPOT7_ 20180508.tif	2	65536	32796	50,04	42,6954	25790	39,35	43,8852	32737	49,95	42,7069
	4	16384	5770	35,22	44,2593	4309	26,3	45,5464	5171	31,56	44,7403
	6	7225	1707	23,63	46,0244	1179	16,32	47,6610	1459	20,19	46,7224
	8	4096	561	13,7	48,3754	383	9,35	50,0493	451	11,01	49,3172
	10	2601	218	8,38	50,5133	132	5,07	52,7408	164	6,31	51,7738
	12	1764	77	4,37	53,5241	52	2,95	55,1967	55	3,12	54,9728
	14	1296	27	2,08	56,6819	13	1	59,8175	21	1,62	57,8020
	16	1024	8	0,78	60,6743	3	0,29	64,9136	6	0,59	61,9054
	18	784	4	0,51	62,5347	3	0,38	63,9767	1	0,13	68,8319
	20	625	3	0,48	63,0009	2	0,32	64,9200	2	0,32	64,9263
	22	529	1	0,19	67,0373	1	0,19	67,0822	1	0,19	67,0822
	24	441	0	0	Inf	0	0	Inf	0	0	Inf
	26	361	0	0	Inf	0	0	Inf	0	0	Inf
	28	324	0	0	Inf	0	0	Inf	0	0	Inf
	30	289	0	0	Inf	0	0	Inf	0	0	Inf
	32	256	0	0	Inf	0	0	Inf	0	0	Inf

Table 4. Complete joint RDHEI results of Pleiades-1A image.

Images	Block Size (s)	Total Message (bit)	Zhang [3]			Hong et al. [4]			Fatema et al. [7]		
			Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)	Incorrect Message (bit)	Bit Error Rate (%)	PSNR (dB)
PHR1A_ 20180501.tif	2	65536	32741	49,96	42,6993	26865	40,99	43,6758	32834	50,1	42,6838
	4	16384	6076	37,08	44,0308	4922	30,04	44,9482	5579	34,05	44,3911
	6	7225	1920	26,57	45,5184	1528	21,15	46,4779	1781	24,65	45,8230
	8	4096	767	18,73	47,0047	570	13,92	48,3056	694	16,94	47,4389
	10	2601	305	11,73	49,0649	218	8,38	50,5123	266	10,23	49,6749
	12	1764	138	7,82	50,9220	95	5,39	52,5114	95	5,39	52,5052
	14	1296	60	4,63	53,2245	33	2,55	55,8577	36	2,78	55,4356
	16	1024	17	1,66	57,5709	12	1,17	58,9439	11	1,07	59,3754
	18	784	11	1,4	58,4245	5	0,64	61,8484	4	0,51	62,8243
	20	625	4	0,64	61,9255	2	0,32	64,8780	2	0,32	65,0549
	22	529	2	0,38	64,1383	0	0	Inf	0	0	Inf
	24	441	0	0	Inf	0	0	Inf	0	0	Inf
	26	361	0	0	Inf	0	0	Inf	0	0	Inf
	28	324	0	0	Inf	0	0	Inf	0	0	Inf
	30	289	0	0	Inf	0	0	Inf	0	0	Inf
	32	256	0	0	Inf	0	0	Inf	0	0	Inf

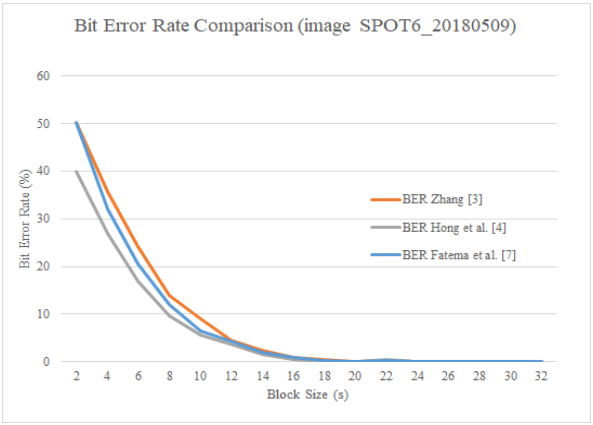

Figure 6. BER comparison of SPOT6 image.

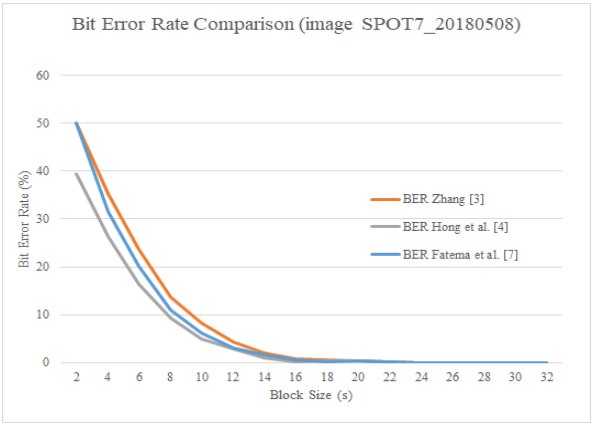

Figure 7. BER comparison of SPOT7 image.

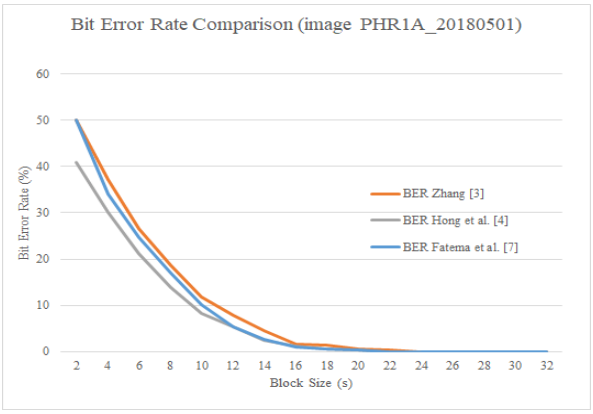

Figure 8. BER comparison of Pleiades-1A image.

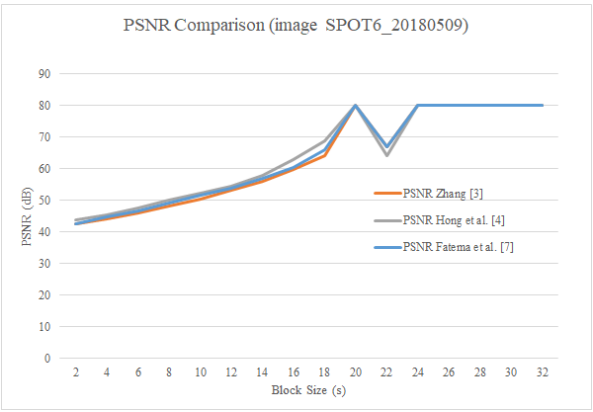

Figure 9. PSNR comparison of SPOT6 image.

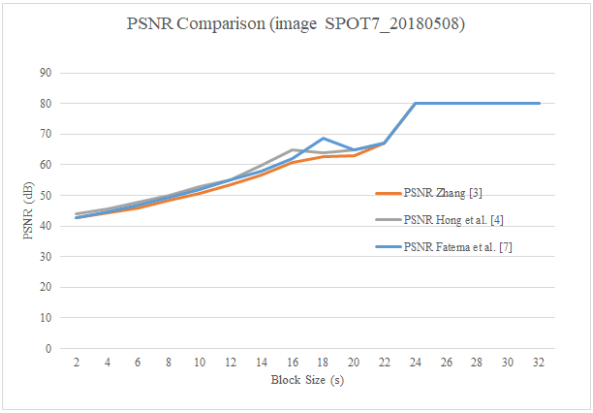

Figure 10. PSNR comparison of SPOT7 image.

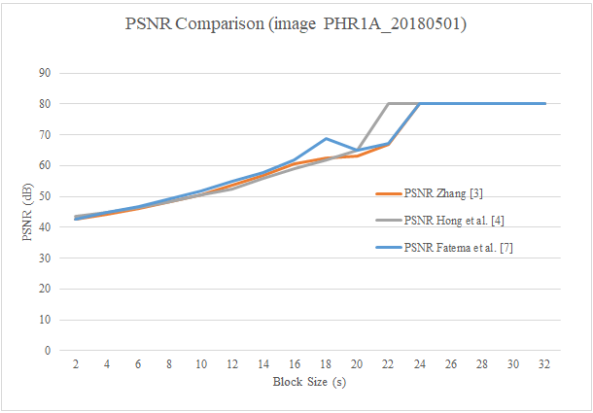

Figure 11. PSNR comparison of Pleiades-1A image.

3.1. Bit Error Rate (BER)

Tables 2 to 4, and Figures 6 to 8 show the bit error rate (%) comparison between the three joint RDHEI methods for test satellite imageries, SPOT-6, SPOT-7, and Pleiades-1A concerning the block size s. Generally, BER and block size are inversely proportional. It can be seen that if more bits are embedded in the encrypted image, the error rate will be higher, otherwise error rate decreases.

For all test images, as shown in Figure 6 to 8, the BER of Hong's et al. method [4] slightly lower than the other two methods. On SPOT-6 test image, when 4096 bits are embedded (s=8), the BER for Hong et al. [4] method is 9.55% which is 4.46% lower than Zhang [3] method of 14.01%, and 2.34% lower than Fatema et al. [7] methods of 11.89%. By using at least 625 bits (s=22), error-free extracted bits can be achieved for the three algorithms. On SPOT-7 test image, when 4096 bits are embedded (s=8), the BER for Hong et al. [4] method is 9.35% which is 3.72% lower than Zhang [3] method of 13.07%, and 1.66% lower than Fatema et al. [7] methods of 11.01%. By using at least 441 bits (s=24), error-free extracted bits can be achieved for all three algorithms. On Pleiades-1A test image, when 4096 bits are embedded (s=8), the BER for Hong et al. [4] method is 13.92% which is 4.81% lower than Zhang [3] method of 18.73%, and 3.02% lower than Fatema et al. [7] methods of 16.94%. By using at least 625 bits (s=22), error-free extracted bits can be achieved for Hong et al. [3] and Fatema et al. [7] methods, but at least 441 bits (s=24) for Zhang [3] method. The error-free extracted bit can be seen in Figure 12.

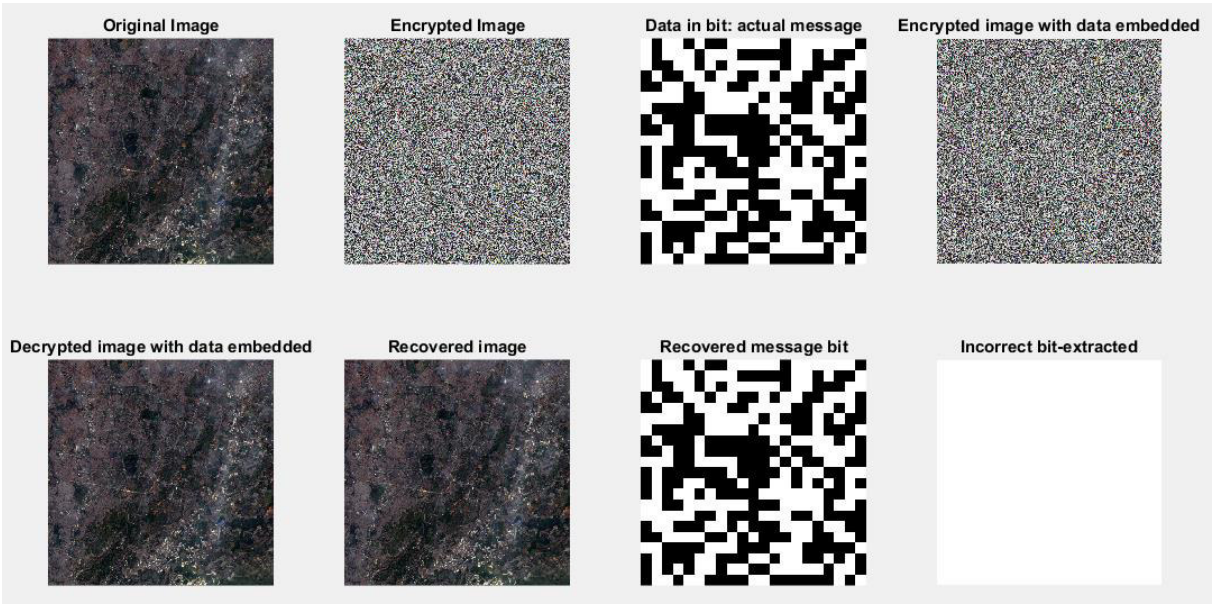

Figure 12. Display the result of the error-free extracted bit when block size s=24.

3.2. Peak Signal to Noise Ratio (PSNR)

Tables 2 to 4, and Figures 9 to 11 show the PSNR (dB) comparison between the three joint RDHEI methods for test satellite imageries, SPOT-6, SPOT-7, and Pleiades-1A concerning the block size s. Generally, PSNR and block size are inversely proportional. It can be seen that if more bits are embedded in the encrypted image, the PSNR will be lower, otherwise, PSNR increases.

For all test images, as shown in Figure 7 to 11, the PSNR of Hong's et al. method [4] slightly higher than the other two methods. On SPOT-6 test image, when 4096 bits are embedded (s=8), the PSNR for Hong et al. [4] method is 49.96 dB which is 1.68 dB higher than Zhang [3] method of 48.26 dB, and 0.98 dB higher than Fatema et al. [7] methods of 48.98 dB. By using at least 625 bits (s=22), complete reversibility (PSNR = infinity) can be provided for the three algorithms. On SPOT-7 test image, when 4096 bits are embedded (s=8), the PSNR for Hong et al. [4] method is 50.04 dB which is 1.67 dB higher than Zhang [3] method of 48.37 dB, and 0.73 dB higher than Fatema et al. [7] methods of 49.31 dB. By using at least 441 bits (s=24), complete reversibility can be achieved for all three algorithms. On Pleiades-1A test image, when 4096 bits are embedded (s=8), the PSNR for Hong et al. [4] method is 48.30 dB which is 1.3 dB higher than Zhang [3] method of 47.00 dB, and 0.87 dB higher than Fatema et al. [7] methods of 47.43 dB. By using at least 625 bits (s=22), complete reversibility can be achieved for Hong et al. [3] and Fatema et al. [7] methods, but at least 441 bits (s=24) for Zhang [3] method.

4. Conclusion

All methods used for joint reversible data hiding in encrypted remote sensing satellite images have been simulated in this research. Compare to Zhang [3] and Fatema et al. [7], Hong et al. [4] method has better performance for most all test images of various block sizes by applying side match technique and performing descending order of the absolute smoothness difference between two candidate blocks in extraction and recovery of blocks which can reduce error extracted bit.

Acknowledgment

The authors would like to thank Universitas Indonesia for funding through Hibah PIT9 Universitas Indonesia (UI), under contract No. NKB-0058/UN2.R3.1/HKP.05.00/2019.

References

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information *hiding*-a survey," in *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062-1078, July 1999.

[2] N. Kittawi and A. Al-Haj, "*Reversible data hiding* in encrypted images," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 808-813.

[3] X. Zhang, "*Reversible data hiding* in Encrypted Image," in *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255-258, April 2011.

[4] W. Hong, T. Chen and H. Wu, "An Improved *Reversible data hiding* in Encrypted Images Using Side Match," in *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202, April 2012.

[5] M. Li, D. Xiao, Z. Peng, and H. Nan, "A modified *reversible data hiding* in encrypted images using random diffusion and accu*rate* prediction," *ETRI J*., vol. 36, no. 2, 2014.

[6] X. Wu and W. Sun, "High-capacity *reversible data hiding* in encrypted images by prediction error," *Signal Process*., vol. 104, pp. 387–400, 2014.

[7] F. Khanam, Kyoung-Young Song and Sunghwan Kim, "A modified *reversible data hiding* in encrypted image using enhanced measurement functions," *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, Vienna, 2016, pp. 869-872.

[8] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Secur*., 2012. vol. 7, no. 2, pp. 826–832.

[9] Weiming Zhang, Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted images, Signal Processing," Volume 94, 2014, Pages 118-127, ISSN 0165-1684.

[10] Z. Qian and X. Zhang, "Reversible Data Hiding in Encrypted Images with Distributed Source Encoding," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 4, pp. 636-646, April 2016.

[11] D. Xiao, Y. Xiang, H. Zheng, and Y. Wang, "Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism," *J. Vis. Commun. Image R*., vol. 45, pp. 1-10, 2017.

[12] Qin Chuan, He Zhihong, Luo Xiangyang, and Dong Jing, "Reversible data hiding in encrypted image with separable capability and high embedding capacity," Information Sciences, vol. 465, October 2018, pages 285-304.

[13] K. Ma, W. Zhang, X. Zhao, N. Yu and F. Li, "*Reversible data hiding* in Encrypted Images by Reserving Room Before Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553-562, March 2013.

[14] The Republic of Indonesia, "Law Number 21 the Year 2013 Regarding Space," Ministry of Law and Human Rights of the Republic of Indonesia, Jakarta, 2013.

[15] The Republic of Indonesia, "Government Regulation Number 11 the Year 2018 Regarding Procedures for Organizing Remote Sensing Activities," Ministry of Law and Human Rights of the Republic of Indonesia, Jakarta, 2018.