An Improved 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, The University of Indonesia, Kampus Baru UI, 16424 Depok, Jakarta, Indonesia
ali.syahputra@ui.ac.id

Abstract. Data protection security is very necessary when distributing high resolution remote sensing satellite images from LAPAN to users via electronic media. Reversible data hiding and encryption are two very useful methods for protecting privacy and data security. This paper proposes an increase in the method of joint reversible data hiding on remote sensing satellite images based on the algorithm of Zhang's work, Hong et al.'s work, and Fatema et al.'s work. To evaluate the smoothness of the blocks, a modification of the fluctuation calculation function is presented. The experimental results show that the modified calculation function gives better estimation results. Then, the proposed method gives a lower extracted bit error rate and the visual quality of the image from the proposed method is better than the three references. For example, when the block size is 8×8, the extracted-bit error rate (EER) of the SPOT-6 test image of the proposed modified function was 8.40%, which is quite lower than the 14.14% EER of Zhang's function, 9.62% EER of Hong et al.'s function and 11.87% EER of Fatema's et al.'s method. Likewise, the quality of SPOT-6 image recovery represented by the peak signal-to-noise ratio (PSNR) of proposed modified function is 50.52 dB, which is slightly higher than the 48.23 dB PSNR of Zhang's function, 49.93 dB PSNR of Hong et al.'s function and 49.00 dB PSNR of Fatema's et al.'s function.

Keywords: Encrypted remote sensing satellite images · Joint reversible data hiding · Fluctuation function · EER · PSNR

1 Introduction

Data hiding and encryption are a combination of two approaches to privacy protection and data security that are popular this time. 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. Nowadays, joint reversible data hiding in encrypted images (RDHEI) is desired property where the cover image is encrypted by the content owner before forwarding it to the data hider for embedding data. Then, the receiver side can extract hidden additional information and recover the original cover image without loss

M. Hernes et al. (Eds.): ICCCI 2020, CCIS 1287, pp. 252–263, 2020.
https://doi.org/10.1007/978-3-030-63119-2_21

or distortion. In the joint RDHEI method, as shown in Fig. 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.

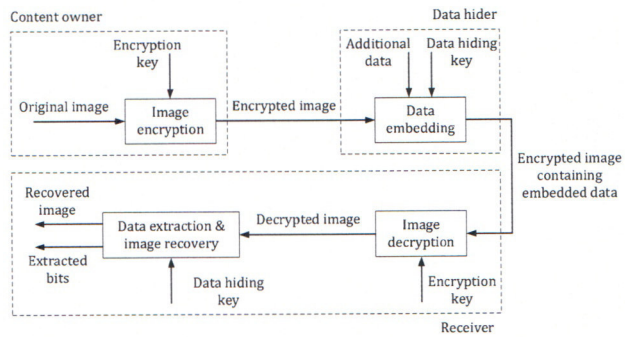


Fig. 1. Joint reversible data hiding scheme on encrypted images [3].

Some of the high-resolution remote sensing images such as SPOT-6, SPOT-7 and Pleiades 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 joint reversible data hiding techniques in high-resolution remote sensing satellite images is very useful for preserving privacy and data security when distributed over the internet network (electronic media). This activity also supports the role of LAPAN in Act Number 21 of 2013 concerning Space [1] and in Government Regulation Number 11 of 2018 regarding Procedures for Organizing Remote Sensing Activities [2] 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.

In recent years, there have been presented several methods of RDHEI, and can be classified into two categories. The first is to find space for confidential data after encrypting the image, referred to as the Vacating Room After Encryption (VRAE) [3–15]. The second is to reserve the amount of space needed for confidential data in a reversible manner before encrypting images. The additional data is hidden into the reserved space after encryption. This is referred to as 'Reserving Room Before Encryption' (RRBE) [16, 17].

Currently, many researchers have presented several studies related to joint RDHEI. In 2011, Zhang proposed joint RDHEI by dividing the encrypted image into several blocks and extracting the data as well as reproducing the image based on the smoothness of the image block [3]. In Zhang's method, the four pixel borders of each image block were avoided when calculating fluctuations in each block. Furthermore, in 2012, Hong et al. improve Zhang's algorithm by using a new method for calculating the smoothness of image blocks and exploiting side match techniques [4]. Hong et al. take border pixels from each block into the calculation, but only two adjacent pixels are used in evaluating the smoothness of each block. Fatema et al. also improved fluctuation function based

on the Zhang's method by considering the actual value of four adjacent pixels in the calculation of fluctuations to reduce the extracted-bit error rate [10]. Therefore, this paper proposes a modified, more precise function to estimate the complexity of each image block by using two adjacent pixels to reduce extracted-bit error rate and increase peak signal-to-noise ratio of the recovered remote sensing satellite images.

This paper is organized as follows. Section 2, discusses several related studies such as the methods of Zhang [3], Hong et al. [4] and Fatema et al. [10] clearly. Section 3 explains the detailed procedure of the proposed method. Then experimental results and performance comparison with the methods of Zhang, Hong et al., Fatema et al. and proposed modified function is presented in Sect. 4. Conclusions are given in Sect. 5.

2 Related Works

In 2011, joint reversible data hiding in encrypted images was introduced by Zhang by proposing a new algorithm by dividing the image into blocks and using the LSB plane. Then, Hong et al. and Fatema et al. presented improvements in data extraction and image recovery.

In the Zhang method [3], the owner encrypts the image with an exclusive-or bitwise operation. Then the data hider will divide the image into several blocks of size s. After segmenting each block in two parts, he adds additional bits into each block by adopting 3 LSB planes. After sending the encrypted image containing additional data, the receiver will first decrypt it and divide decrypted image containing additional data into blocks of the same size s, then each block will be separated into two sets of the same size and extraction of data/image recovery will be carried out according to fluctuations in Eq. (1) from each block. The Zhang's fluctuation functions are as follows:

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

Where $p_{u,v}$ is the pixel value located at (u, v).

In the Hong et al.'s method [4], they increase data extraction/image recovery based on the Zhang's method. First, they proposed a new function such as Eq. (2) where $p_{u,v}$ is the pixel value located at the position (u, v) of each image block with size s1 x s2 to estimate the smoothness of the block. They consider more pixels so that the extracted-bit error rate is reduced.

$$f_H = \sum_{u=1}^{s_2} \sum_{v=1}^{s_1-1} |p_{u,v} - p_{u,v+1}| + \sum_{u=1}^{s_2-1} \sum_{v=1}^{s_1} |p_{u,v} - p_{u+1,v}| \tag{2}$$

In the Fatema et al.'s method [10], they also improved data extraction/image recovery based on the Zhang's method by proposing new functions such as Eq. (3) where $p_{u,v}$ is the pixel value located at the position (u, v) of each image block with size s. They consider the actual value of four neighbouring pixels in the calculation of fluctuations to reduce the extracted-bit error rate.

$$f_F = \sum_{u=2}^{s-1} \sum_{v=2}^{s-1} |p_{u,v} - p_{u-1,v}| + |p_{u,v} - p_{u+1,v}| + |p_{u,v} - p_{u,v-1}| + |p_{u,v} - p_{u,v+1}| \tag{3}$$

3 Proposed Works

3.1 Modification of Fluctuation Function

The fluctuation function is very important when viewed from previous works. The accuracy of the data extraction is determined by the accuracy of the fluctuation function. In this study, the modification of the fluctuation function is used to calculate the fluctuation value, as shown in Eq. (4). This modified fluctuation function is similar to Hong, but especially when the block size is small, it has more accuracy than the Hong fluctuation function according to empirical results.

$$f_P = \sum_{u=1}^{s}\sum_{v=2}^{s-1}|2 * p_{u,v} - (p_{u,v-1} + p_{u,v+1})| + \sum_{u=2}^{s-1}\sum_{v=1}^{s}|2 * p_{u,v} - (p_{u-1,v} + p_{u+1,v})| \tag{4}$$

To further reduce the extracted-bit error rate, the fluctuation calculation of the image block can be estimated by calculating the absolute difference in horizontal and vertical neighbouring pixels. Figure 2 shows the distribution of neighbouring pixels from a given pixel. A grid circled in green in different positions means the pixel to be counted, and the colour marked is their neighbouring pixel. Three types of pixels according to their coordinates are shown in the figure. The marked in orange is Zhang's (f_Z) and Fatema et al.'s (f_F) fluctuation function calculation. The marked in blue second class is Hong et al.'s fluctuation function calculation (f_H). The marked in red is the proposed fluctuation function calculation (f_P).

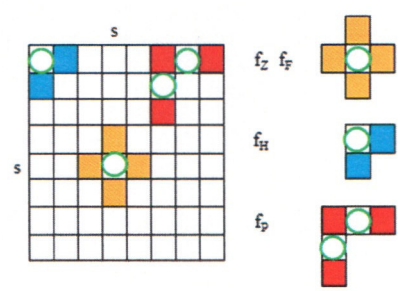


Fig. 2. Distribution of neighbouring pixels of a given pixel.

3.2 Procedures of the Proposed Method

Image Encryption. In the sender side, to begin image encryption phase, the original satellite image is loaded and resize it into a size of MxN 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 P is an 8-bit uncompressed cover image of size MxN, and $p_{i,j}$ is the pixel value located

at (i, j). Assume the pixel values $p_{i,j}$ range from 0 to 255 which can be represented by 8 bits $p^0_{i,j}, p^1_{i,j}, p^2_{i,j}, \ldots, p^7_{i,j}$. So, we have

$$p^k_{i,j} = \left\lfloor \frac{p_{i,j}}{2^k} \right\rfloor \bmod 2, \; k = 1, \; 2, \; \ldots, \; 7 \tag{5}$$

For encrypted images C, encrypted bits $C^k_{i,j}$ can be calculated with the exclusive-or operation as follows:

$$C^k_{i,j} = p^k_{i,j} \oplus r^k_{i,j}, \; k = 1, \; 2, \; \ldots, \; 7 \tag{6}$$

Where $r^k_{i,j}$ is generated by an encryption key using the standard stream cipher. Then $C_{i,j}$ encrypted data can be obtained as follows:

$$C_{i,j} = \sum_{k=0}^{7} C^k_{i,j} \, x \, 2^k \tag{7}$$

Data Embedding. In data embedding stage (see Fig. 3), the block size value s is assumed. Then, the data hider segments the encrypted image into several non-overlapping blocks sized by sxs. Next, generate the data message to embed in the encrypted image by considering a matrix of 0 and 1. Get two sets S_0 and S_1 using the data hiding key. If data hiding key values at the pixel position is 0, then it goes into set S_0 otherwise set S_1. If the bit message 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 S_0 and pixel in set S_1 is not changed. On the other hand, If the bit message to be embedded is '1', flip the three LSB of each encrypted pixel in set S_1 and pixel in set S_0 is unchanged. After that, the resultant of red, green, blue channels is combined to get the encrypted image with additional data.

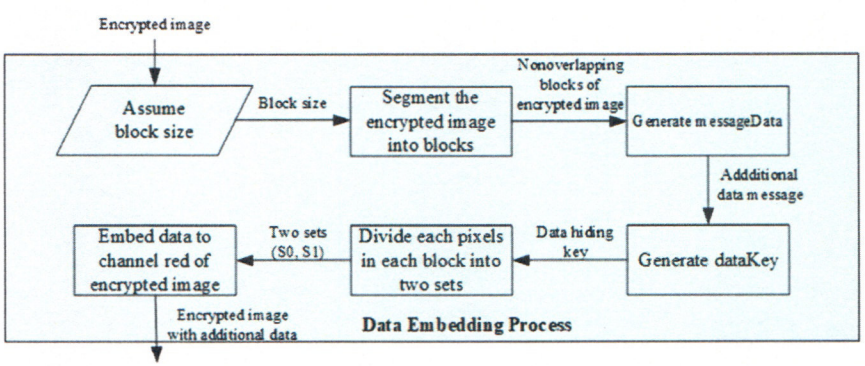


Fig. 3. Data embedding process scheme.

Image Decryption. 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 which is similar to image encryption procedures. For flipped encrypted bits $C'^{k}_{i,j}$, the marked decrypted bit can be calculated as follows:

$$C'^{k}_{i,j} \oplus r^{k}_{i,j} = \overline{C^{k}_{i,j}} \oplus r^{k}_{i,j} = \overline{p^{k}_{i,j} \oplus r^{k}_{i,j}} \oplus r^{k}_{i,j} = \overline{p^{k}_{i,j}} \tag{8}$$

In the same block, the bits that have not been flipped without the embedded bits will be the same as the original bits $p^{k}_{i,j}$.

Data Extraction and Image Recovery. 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 *sxs*. Next, each pixel in each block is divided into two sets $newS_0$ and $newS_1$ in the same way. If data hiding key values at the pixel position is 0, then it goes into set $newS_0$, otherwise set $newS_1$. Flip three LSB in set $newS_0$ and $newS_1$ to get two sets S_{00} and S_{11}. After that, make two sets H_0 and H_1. If data hiding key values at the pixel position is '0', then set S_{00} and $newS_0$ goes into set H_0 and H_1, respectively. Otherwise set $newS_1$ and S_{11} go into set H_0 and H_1, respectively. After that, calculate fluctuation H_0 and H_1 to determine which one is the original image.

Hereinafter, combine the red channel with the green and blue channels to give the recovered original image. Finally, calculate EER by comparing each pixel from the original matrix data message with a recovered data message and PSNR [6] to measure the quality of the final recovered image as follows:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(O_{i,j} - M_{i,j}\right)^2} \tag{9}$$

Where $O_{i,j}$ and $M_{i,j}$ are the original pixel values and the modified pixel values, respectively.

4 Results and Discussion

In this paper, three standard processing high-resolution remote sensing satellite images, i.e. SPOT-6, SPOT-7, and Pleiades-1A, as shown in Fig. 4, are considered. The test images have been resized to 512 × 512 where each pixel is represented by 8 bits. The range of the block size is from two to 32. In this research, two important performance parameters will be analyzed:

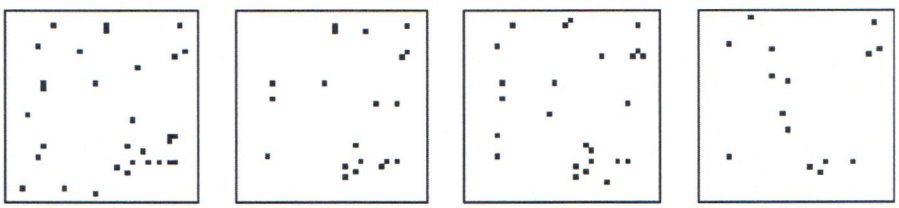
- Extracted-bit error rate (EER); this parameter shows the ratio of unrecovered bits to the total number of embedded bits.
- Peak signal-to-noise ratio (PSNR); this parameter is to show the differences between the original image and the recovered original image.

To compare the proposed joint data hiding method with the referenced methods, the error pattern of the data hiding system is shown in Fig. 5. For a SPOT-6 image and s = 14, error positions of Zhang's function [3], Hong's function [4], Fatema's function [10],

(a) (b) (c)

Fig. 4. Simulation test images. (a) SPOT-6; (b) SPOT-7; (c) Pleiades-1A.

and the proposed system with fluctuation functions in Eq. (4) are shown in (a), (b), (c) and (d) in Fig. 5, respectively. The small black square in a large square in Fig. 4 denotes *sxs* error pixels in a SPOT-6 image. From Fig. 5a to 5d, the recovery performance of the system with the proposed fluctuation functions in Eq. (4) is better than the ones of Zhang's method [3], Hong's method [4], and Fatema's method [10].



(a) (b) (c) (d)

Fig. 5. Incorrect extracted-bit pattern of Zhang's method [3], Hong's method [4], Fatema's method [10], and proposed method in the SPOT-6 image for s = 14. (a) f_Z in (1); (b) f_H in (2); (c) f_F in (3), (d) f_P in (4).

In Fig. 6 to Fig. 8, the EER dan PSNR of image recovery performances of the referenced functions and proposed function are shown according to the block size of *s* when SPOT-6, SPOT-7 and Pleiades-1A images in Fig. 4 are considered. The 'Ref. Zhang [3] ', 'Ref. Hong et al. [4] ', and Ref. Fatema et al. [10] in these figures denote EERs for Zhang's function in (1), Hong's function in (2), and Fatema's function in (3) respectively. The 'Proposed Function' in these figures denotes for EERs for the proposed fluctuation functions in (4). The 'Inf' in these figures denotes infinite PSNR. Infinite PSNR cannot be illustrated in these figures. However, for convenience, it is located at 103.4 dB. For all test images, the EER of proposed function slightly lower than the other three references functions as the block size decreases. Likewise, the PSNR of proposed function is slightly higher than the other three references functions as the block size decreases.

In SPOT-6 test image, as shown in Fig. 6, when 4096 bits are embedded (s = 8 × 8), the EER of the proposed function is 8.4% which is 5.74% lower than Zhang's function of 14.14%, 1.22% lower than Hong's function of 9.62%, and 3.47% lower than Fatema et al.'s function of 11.87%. Likewise, when 4096 bits are embedded (s = 8 × 8), the PSNR of the proposed function is 50.52 dB which is 2.29 dB higher than Zhang's function of 48.23 dB, 0.59 dB higher than Hong's function of 49.93 dB, and 1.52 dB higher than Fatema et al.'s function of 49.00 dB. By using at least 784 bits (s = 18 × 18),

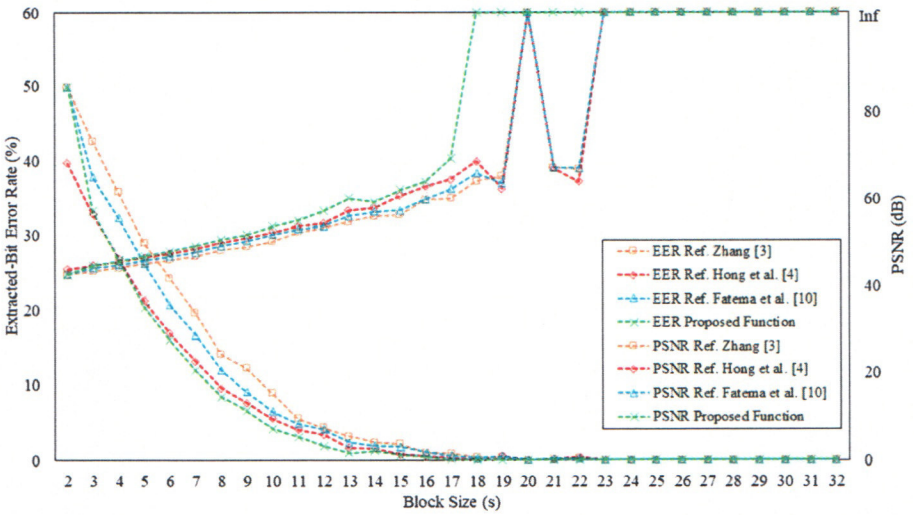


Fig. 6. EER and PSNR image recovery performances comparison of referenced and proposed function for the SPOT-6 test image.

error-free extracted bits and complete reversibility (PSNR = infinity) can be achieved by the proposed function meanwhile at least 625 bits ($s = 20 \times 20$), error-free extracted bits and infinite PSNR can be achieved by the three references.

In SPOT-7 test image, as shown in Fig. 7, when 4096 bits are embedded ($s = 8 \times 8$), the EER of the proposed function is 8.01% which is 5.61% lower than Zhang's function of 13.62%, 1.29% lower than Hong's function of 9.3%, and 3.03% lower than Fatema et al.'s function of 11.04%. Likewise, when 4096 bits are embedded ($s = 8 \times 8$), the PSNR of the proposed function is 50.74 dB which is 2.35 dB higher than Zhang's function of 48.39 dB, 0.67 dB higher than Hong's function of 50.07 dB, and 1.44 dB higher than Fatema et al.'s function of 49.30 dB. By using at least 784 bits ($s = 18 \times 18$), error-free extracted bits and complete reversibility (PSNR = infinity) can be achieved by the proposed function meanwhile at least 576 bits ($s = 21 \times 21$), error-free extracted bits and infinite PSNR can be achieved by Hong and Fatema, and at least 484 bits ($s = 23 \times 23$), error-free extracted bits and infinite PSNR can be achieved by Zhang.

In Pleiades-1A test image, as shown in Fig. 8, when 4096 bits are embedded ($s = 8 \times 8$), the EER of the proposed function is 11.35% which is 7.13% lower than Zhang's function of 18.48%, 2.59% lower than Hong's function of 13.94%, and 5.67% lower than Fatema et al.'s function of 17.02%. Likewise, when 4096 bits are embedded ($s = 8$), the PSNR of the proposed method is 49.20 dB which is 2.15 dB higher than Zhang's function of 47.05 dB, 0.91 dB higher than Hong's function of 48.29 dB, and 1.79 dB higher than Fatema et al.'s function of 47.41 dB. By using at least 625 bits ($s = 20 \times 20$), error-free extracted bits and complete reversibility (PSNR = infinity) can be achieved by the proposed function meanwhile at least 576 bits ($s = 21 \times 21$), error-free extracted bits and infinite PSNR can be achieved by Zhang and Hong, and at least 529 bits ($s = 22 \times 22$), error-free extracted bits and infinite PSNR can be achieved by Fatema.

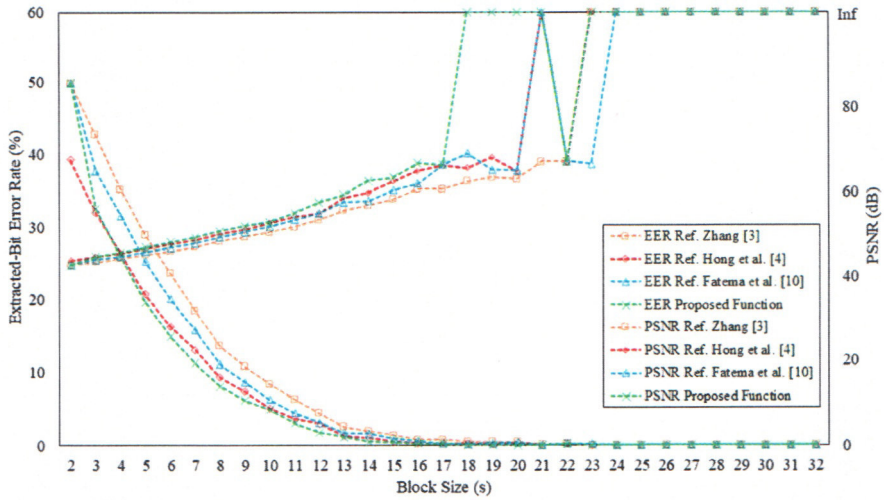


Fig. 7. EER and PSNR image recovery performances comparison of referenced and proposed function for the SPOT-7 test image.

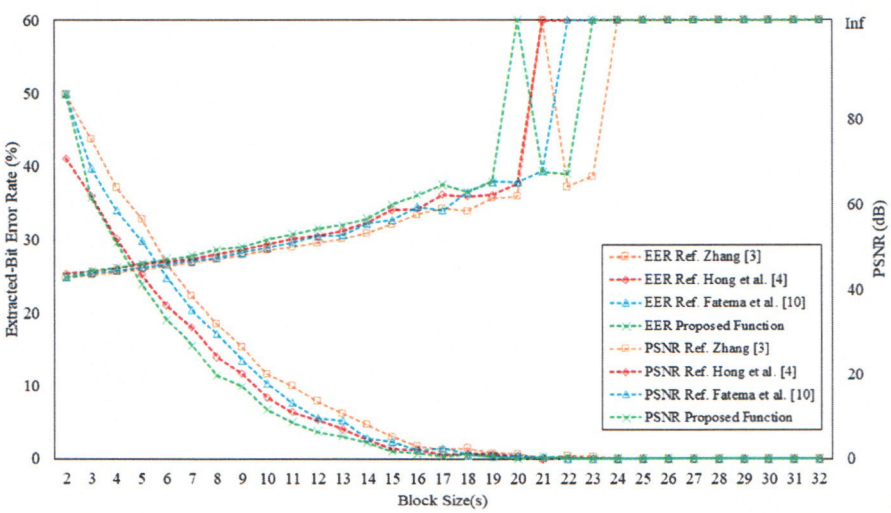


Fig. 8. EER and PSNR image recovery performances comparison of referenced and proposed function for the Pleiades-1A test image.

Table 1 through Table 3 show the comparison of the main results between the modification of the proposed function and the reference function Zhang [3], Hong et al. [4], and Fatema et al. [10] for error-free extracted-bits and infinite PSNR on the SPOT-6, SPOT-7, and Pleiades-1A test images. The "minimum block size (s)" in the Table is the minimum block size (s) that guarantees error-free extracted-bits and maximum PSNR (infinity). "Number of messages (bits)" in the Table is the actual number of bits that can

be embedded that corresponds to the minimum block size (s). The "gain" in the Table states the ratio of the number of message bits of the proposed function to the number of message bits from the three reference functions Zhang, Hong et al., and Fatema et al. and written in percent (%).

Table 1. Comparison of minimum block size (s) to obtain error-free extracted-bits and infinite PSNR between proposed systems with references for SPOT-6 test image.

Methods	Minimum block size (s)	Number of Message (bits)	Gain (%) with Zhang [3]	Gain (%) with Hong et al. [4]	Gain (%) with Fatema et al. [10]
Ref. Zhang [3]	20 × 20	625	–	–	–
Ref. Hong et al. [4]	20 × 20	625	–	–	–
Ref. Fatema et al. [10]	20 × 20	625	–	–	–
Proposed	18 × 18	784	125,44	125,44	125,44

Table 2. Comparison of minimum block size (s) to obtain error-free extracted-bits and infinite PSNR between proposed systems with references for SPOT-7 test image.

Methods	Minimum block size (s)	Number of Message (bits)	Gain (%) with Zhang [3]	Gain (%) with Hong et al. [4]	Gain (%) with Fatema et al. [10]
Ref. Zhang [3]	23 × 23	484	–	–	–
Ref. Hong et al. [4]	21 × 21	576	119,01	–	–
Ref. Fatema et al. [10]	21 × 21	576	119,01	–	–
Proposed	18 × 18	784	161,98	136,11	136,11

As shown in Tables 1 through Table 3, the minimum block size (s) of the proposed system is always smaller than the reference systems. The number of message bits embedded in the proposed system is also greater than the reference system. In Table 1, the number of embedded message bits of the proposed system shows 125.44% greater than the three reference systems in the SPOT-6 test image. In Table 2, the number of embedded message bits of the proposed system shows 161.98% greater than the Zhang reference system, and 136.11% greater than the Hong and Fatema reference system in the SPOT-7 test image. In Table 3, the number of embedded message bits of the proposed

Table 3. Comparison of minimum block size (s) to obtain error-free extracted-bits and infinite PSNR between proposed systems with references for Pleiades-1A test image.

Methods	Minimum block size (s)	Number of Message (bits)	Gain (%) with Ref. Zhang [3]	Gain (%) with Hong et al. [4]	Gain (%) with Fatema et al. [10]
Ref. Zhang [3]	21 × 21	576	–	–	108,88
Ref. Hong et al. [4]	21 × 21	576	–	–	108,88
Ref. Fatema et al. [10]	22 × 22	529	–	–	–
Proposed	20 × 20	625	108,51	108,51	118,15

system shows 108.51% greater than the Zhang and Hong reference system, and 118.15% greater than the Fatema reference system in the Pleiades-1A test image.

5 Conclusion

In this paper, based on Zhang [3], Hong et al. [4] and Fatema et al. [10] functions, a modified fluctuation function to measure the smoothness of image block has been proposed. The experimental results show that the modified fluctuation function is more precise and can further reduce the extracted-bit error rate compared to the other three references functions. Furthermore, the visual quality of the recovered remote sensing satellite images, represented by PSNR, is quite higher than the other three references functions. In the future, error control coding can be used in the algorithm in order to improve the performance.

Acknowledgment. The authors would like to thank Universitas Indonesia for funding through PUTI Prosiding Universitas Indonesia (UI), under contract No. NKB-1183/UN2.RST/HKP.05.00/2020.

References

1. 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)
2. 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)
3. Zhang, X.: Reversible data hiding in encrypted Image. IEEE Signal Process. Lett. **18**(4), 255–258 (2011)
4. Hong, W., Chen, T., Wu, H.: An improved reversible data hiding in encrypted images using side match. IEEE Signal Process. Lett. **19**(4), 199–202 (2012)

5. Li, M., Xiao, D., Peng, Z., Nan, H.: A modified reversible data hiding in encrypted images using random diffusion and accurate prediction. ETRI J. **36**(2), 325–328 (2014)
6. Wu, X., Sun, W.: High-capacity reversible data hiding in encrypted images by prediction error. Signal Process. **104**, 387–400 (2014)
7. Liao, X., Shu, C.: Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J. Vis. Commun. Image R. **28**, 21–27 (2015)
8. Kim, Y.S., Kang, K., Lim, D.W.: New reversible data hiding scheme for encrypted images using lattices. Appl. Math. Inf. Sci. **9**(5), 2627–2636 (2015)
9. Pan, Z., Wang, L., Hu, S., Ma, X.: Reversible data hiding in encrypted image using new embedding pattern and multiple judgements. Multimedia Tools Appl. **75**(14), 8595–8607 (2016)
10. Fatema, K., Song, K.Y., Sunghwan, K.: A modified reversible data hiding in encrypted image using enhanced measurement functions. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN) 2016, pp. 869–872, Vienna (2016)
11. Zhang, X.: Separable reversible data hiding in encrypted image. IEEE Trans. Inf. Forensics Secur **7**(2), 826–832 (2012)
12. Zhang, X., Qian, Z., Feng, G., Ren, Y.: Efficient reversible data hiding in encrypted images. J. Bis. Commun. Image Represent. **25**(2), 322–328 (2014)
13. Qian, Z., Zhang, X.: Reversible data hiding in encrypted images with distributed source encoding. IEEE Trans. Circuits Syst. Video Technol. **26**(4), 636–646 (2016)
14. Xiao, D., Xiang, Y., Zheng, H., Wang, Y.: Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism. J. Vis. Commun. Image R. **45**, 1–10 (2017)
15. Chuan, Q., Zhihong, H., Xiangyang, L., Jing, D.: Reversible data hiding in encrypted image with separable capability and high embedding capacity. Inf. Sci. **465**, 285–304 (2018)
16. Ma, K., Zhang, W., Zhao, X., Yu, N., Li, F.: Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. Inf. Forensics Secur. **8**(3), 553–562 (2013)
17. Zhang, W., Ma, K., Yu, N.: Reversibility improved data hiding in encrypted images. Signal Process. **94**, 118–127 (2014). ISSN 0165-1684