IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 21, 2020, accepted December 1, 2020, date of publication December 7, 2020,
date of current version December 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3042971

Hybrid Reversible Data Hiding in Encrypted Satellite Images Using Fluctuation Modification Extraction and Reed-Solomon Code Embedding

GUNAWAN WIBISONO[1], (Member, IEEE), ALI SYAHPUTRA NASUTION[1], TEGUH FIRMANSYAH[2], (Member, IEEE), AND ANTON SATRIA PRABUWONO[3], (Senior Member, IEEE)

[1]Department of Electrical Engineering, Universitas Indonesia, Depok 16424, Indonesia
[2]Department of Electrical Engineering, Universitas Sultan Ageng Tirtayasa, Cilegon 42435, Indonesia
[3]Department of Information Technology, Faculty of Computing and Information Technology Rabigh, King Abdulaziz University, Rabigh 21911, Saudi Arabia

Corresponding author: Gunawan Wibisono (gunawan@eng.ui.ac.id)

This work was supported by Ministry of Research and Technology/National Research and Innovation Agency through the Grants for Applied Research 2020 under Contract NKB-297/UN2.RST/HKP.05.00/2020, then revised by addendum under Grant NKB-2896/UN2.RST/HKP.05.00/2020.

ABSTRACT In conventional hybrid reversible data hiding in encrypted images (RDHEI), the error-free extracted-bit rate condition in recovered images cannot be fully achieved (reversible) as the block size decreases because of the fluctuation function used, which cannot reduce the bit error, as indicated by the high extracted-bit error rate (EER) and low peak signal-to-noise ratio (PSNR). Therefore, this work proposes improving the accuracy of hybrid RDHEI performance for remote sensing satellite images by modifying the fluctuation function in the data extraction process with and without the Reed-Solomon (RS) codes in the data embedding process. The proposed fluctuation function takes the absolute difference in the actual value of two adjacent pixels in horizontal and vertical pixels. The modified fluctuation function algorithm in the extraction process both with and without RS codes in the embedding data process is derived, and performance results are obtained through simulations of SPOT-6, SPOT-7, and Pleiades-1A satellite images. The simulation results show that the proposed hybrid RDHEI algorithm with modification of the fluctuation function without an RS encoder can achieve error-free extracted-bit and maximum PSNR (infinity) values at a block size of 18 x 18 for SPOT-6 and SPOT-7 test images, as well as a block size of 20 x 20 for the Pleiades-1A test image. It is proven that the proposed hybrid RDHEI succeeds in reducing the minimum block size from reference systems. In addition, it can also be seen that the proposed hybrid RDHEI with modification of the fluctuation function and RS coding in data embedding can reduce the minimum block size to achieve error-free extracted bits to 9 x 9 for SPOT-6 and SPOT-7 test images and 10 x 10 for the Pleiades-1A test image.

INDEX TERMS Hybrid reversible data hiding, encryption, remote sensing satellite images, Reed-Solomon (RS) codes, extracted-bit error rate, peak signal-to-noise ratio.

I. INTRODUCTION

Encryption and reversible data hiding are two powerful data security techniques that protect privacy and confidentiality in communication [1]. Encryption techniques transform plaintext content into illegible ciphertext. The reversible data hiding (RDH) technique embeds secret messages or bits of information into the cover media such as images, audio or video by making some modifications and can restore the original cover image without distortion after extracting the hidden information. Adopting the reversible data hiding technique became an impressive strategy. Shaik and Thanikaiselvan [2] evaluated integer wavelet transforms such as Haar, 5/3, 2/6, 9/7-M, 2/10, 5/11-C, 5/11-A, 6/14, 13/7-T, 13/7-C and 9/7-F using a generalized threshold-based histogram shifting technique. The proposed method achieved better embedding capacity and stegoimage quality compared to state-of-the-art RDH techniques. Benhfid *et al.* [3] applied

The associate editor coordinating the review of this manuscript and approving it for publication was Shiqi Wang.

a reversible steganography system based on interpolation by linear box splines on a three-directional mesh. The proposed work surpassed the literature in hiding capacity with an equivalent level of imperceptibility. Maniriho and Ahmad [4] improved information hiding implemented based on difference expansion and modulus functions. The proposed scheme achieved better results with respect to the embedding rate and peak signal-to-noise ratio (PSNR) than existing methods. Sahu and Swain [5] proposed two improved reversible data hiding-based approaches: (1) improved dual image-based least significant bit (LSB) matching with reversibility and (2) n-rightmost bit replacement (n-RBR) and modified pixel value differencing (MPVD). The proposed technique improved the PSNR, embedding capacity (EC), and structural similarity index (SSIM) compared to existing approaches. Setiadi [6] proposed a combination of the hybrid detector (Canny and Sobel) based on 3-bit MSB and a dilation process to increase the payload capacity of messages. The proposed technique succeeded in improving imperceptibility quality and increasing embedding capacity.

Several studies related to RDH in encrypted images (RDHEI) have been proposed [7]–[28]. The RDHEI methods can be classified into the following two categories: hybrid methods [7]–[19] and separable methods [20]–[28]. In the hybrid RDHEI, data extraction and image recovery are performed together. The hybrid RDHEI scheme was first introduced by Zhang [7], where encrypted images were divided into nonoverlapping blocks and data extraction and image recovery were carried out based on fluctuations in image blocks. In Zhang's scheme [7], the fluctuation function for data extraction and image recovery involves an average value of four neighboring pixels but does not include block boundary pixels; therefore, there are some extracted-bit errors and smaller block sizes that are not completely reversible. Hong *et al.* [8] improved Zhang's scheme [7] by proposing a new fluctuation function that exploits the sum of absolute pixel differences, involves two neighboring pixels and includes boundary pixels from each block. The scheme proposed by Hong *et al.* [8] produces an extracted-bit error rate (EER) that is smaller than Zhang's scheme [7]; however, the proposed scheme is not completely reversible for smaller block sizes. Li *et al.* [9] presented a new system of random diffusion strategies that were applied for embedding and accurate predictions to measure fluctuation. Wu and Sun [10] proposed a different hybrid and separable RDHEI system based on prediction errors. However, the visual quality of the decrypted image is less satisfactory. Qian *et al.* [11] presented a reversible data hiding framework for encrypted JPEG bitstreams where secret message bits are coded with error control coding (ECC) of a low-density parity check (LDPC) and embedded into encrypted bitstreams by modifying the embedded bits according to the AC coefficient. However, embedding capacity variations are needed where only 750 bits are used. Liao and Shu [12] further enhanced [7] and [8] by developing a new fluctuation function that uses two, three, or four neighboring pixels based on each pixel location. In addition, data embedding ratios are also considered in this technique. Kim *et al.* [13] improved the performance of the methods of Zhang [7] and Hong *et al.* [8] by introducing lattice patterns for embedding data and modifying the fluctuation function that extracts more information from neighboring pixels. In [14], the work of Li *et al.* [9] was further enhanced by using the full embedding technique. Pan *et al.* [15] proposed a new embedding pattern that considers both border pixels and the spatial correlation of pixels in a block to embed more fluctuations to reduce the error rate further. Fatema *et al.* [16] improved the data extraction accuracy of Zhang's scheme [7] by proposing a new fluctuation function that involves the actual values of the four neighboring pixels to minimize the bit error rate. Smita and Manoj [17] proposed a different scheme using modulo addition encryption and average properties, which provided higher performance than [7] and [8] and full reversibility. In [18], the work of Fatema *et al.* [16] was further enhanced with three fluctuation functions to improve the accuracy of data extraction, but the computational complexity was higher. Overall, the reported hybrid method cannot obtain error-free extracted bits when using high embedding loads (small block sizes).

For the separable RDHEI method, data extraction and image decryption can be separated so that embedded bit extraction is perfectly guaranteed where the data hider compresses the LSB from the encrypted image by emptying space for embedding additional bits. Recipients who have data hiding keys can extract additional data without any errors, while recipients who have encryption keys may decrypt the received data to gain an image identical to the original. If data hiding and encryption keys are available, the recipients can retrieve additional data and restore the original image. The separable RDHEI method was first introduced by Zhang [19] and subsequently developed by several researchers [20]–[26]. To obtain the recovered image without any errors, two methods of RDHEI methodology with reservation room before encryption (RRBE) were proposed [27], [28]. Although both of these methods [27], [28] significantly increase embedding capacity and reversibility, freeing space for data embedding by content owners is not possible because RDHEI always requires content owners to do nothing except image encryption, and data embedding is performed by a data hider.

In hybrid RDHEI methods [7]–[18], many errors occur in the extracted bits, especially when the embedding load is high. To obtain better performance on the hybrid RDHEI scheme, some researchers [29], [30] developed a data embedding scheme using Reed-Solomon (RS) codes. Embedding techniques using RS codes exploit the ability to correct burst errors (sequential incorrect bits received) so that the extraction of incorrect bits can be minimized. In [29], [30], the RS code is generated and gives a low extracted-bit error rate (EER) value. However, the optimal RS code was not determined, namely, the RS code that has a low EER, maximum PSNR, and coding gain $\geq$1. High coding gain increases the security of the image being transmitted because more bits are embedded into the image.

In the reference hybrid RDHEI method [7], [8], [16], the number of error extracted bits, reversibility and visual quality of the recovered image are not good, especially when the embedding load is high. The method of Hong *et al.* [8] gave better EER and PSNR performance compared to Zhang's method [7] and that of Fatema *et al.* [16]. However, the performance of EER and PSNR worsens with shrinking block size.

In this article, two hybrid RDHEI schemes are proposed for remote sensing satellite images. First, the hybrid RDHEI system is proposed and analyzed by modifying the fluctuation function without an RS code. The proposed fluctuation function is used by taking the absolute difference in the actual value of two adjacent pixels in horizontal and vertical pixels. Furthermore, the development of a hybrid RDHEI system is proposed with fluctuation modification and embedded schemes using optimal RS codes. The proposed method can reduce the number of bit errors extracted and increase the reversibility and visual quality of the restored satellite images. This research will increase the security of remote sensing satellite image distributions to users when satellite images are distributed via the internet. Data security techniques, including encryption and RDH, are applied to refuse the use of images by unauthorized users.

The remainder of this article is organized as follows. The proposed system model based on a hybrid RDH scheme with a modified fluctuation function including image encryption, data embedding, hybrid data extraction, and image recovery is described in the first part of Section II. Moreover, the proposed hybrid RDHEI scheme in remote sensing satellite images with modified fluctuation functions and RS code embedding including codeword embedding, hybrid codeword extraction, and image recovery is explained in the second part of Section II. Moreover, the experimental results and analysis are explained in Section III. Section IV provides concluding remarks.

II. SYSTEM MODEL

In this article, high-resolution remote sensing satellite images of SPOT-6, SPOT-7, and Pleiades-1A are used as test images. The SPOT-6 and SPOT-7 images have four multispectral channels with a spatial resolution of 6 meters and one panchromatic channel with a spatial resolution of 1.5 meters [31], [32]. Pleiades-1A imagery has four multispectral channels with a spatial resolution of 2 meters and one panchromatic channel with a spatial resolution of 0.5 meters [33]. Figure 1 shows one scene sample from each SPOT-6, SPOT-7, and Pleiades-1A test image with composite bands 3, 2, and 1 (RGB).

A. PROPOSED HYBRID RDH SCHEME WITH MODIFIED FLUCTUATION FUNCTION

The proposed schematic flowchart is shown in Figure 2 and consists of the following three stages: image encryption, data embedding, hybrid data extraction and image recovery. In the satellite image encryption phase, by using an encryption key, the image owner encrypts the original satellite image to produce the encrypted satellite image. Then, in the data hiding phase, the data hider embeds additional information bits into the encrypted satellite image using the data hiding key without knowing its original content. In the hybrid phase of data extraction and image recovery, with encrypted images containing additional information bits, the recipient first decrypts the image using the encryption key, and the decrypted version is similar to the original satellite image. In accordance with the data hiding key, the receiver may further extract embedded information bits and recover the original satellite image from the decrypted version with the help of the fluctuation function.

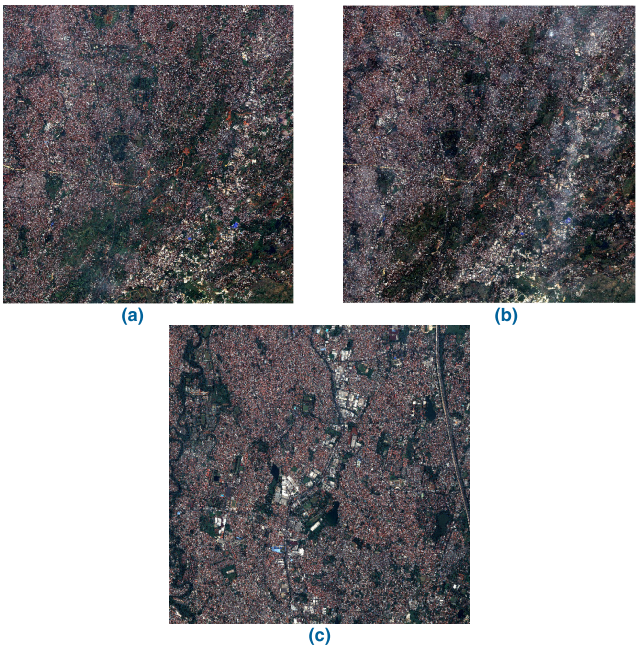

FIGURE 1. Test images (a) SPOT-6; (B) SPOT-7; (c) Pleiades-1A.

1) IMAGE ENCRYPTION

On the content owner side, to start the image encryption phase, the original satellite image is opened and resized to an MxN pixel size. Then, the color satellite image is extracted into each of the red, green and blue channels. After that, the original satellite image is encrypted with an encryption key by applying a bitwise exclusive-or (XOR). Let P be an 8-bit cover satellite image of size MxN, and $p_{i,j}$ is the pixel value located at (i, j), where $0 \leq i < M$ and $0 \leq j < N$. Assuming pixel value, $p_{i,j}$, ranges from 0 to 255, which can be represented by 8 bits $p^0_{i,j}, p^1_{i,j}, p^2_{i,j}, \ldots, p^7_{i,j}$. Encrypted pixel $C_{i,j}$ can be expressed [7] as

$$C_{i,j} = \sum_{l=0}^{7} C^l_{i,j} \, x \, 2^l \tag{1}$$

where

$$C^l_{i,j} = p^l_{i,j} \oplus r^l_{i,j}, \quad l = 0, 1, \ldots, 7$$
$$p^l_{i,j} = \left\lfloor \frac{p_{i,j}}{2^l} \right\rfloor mod 2, \quad l = 0, 1, \ldots, 7$$

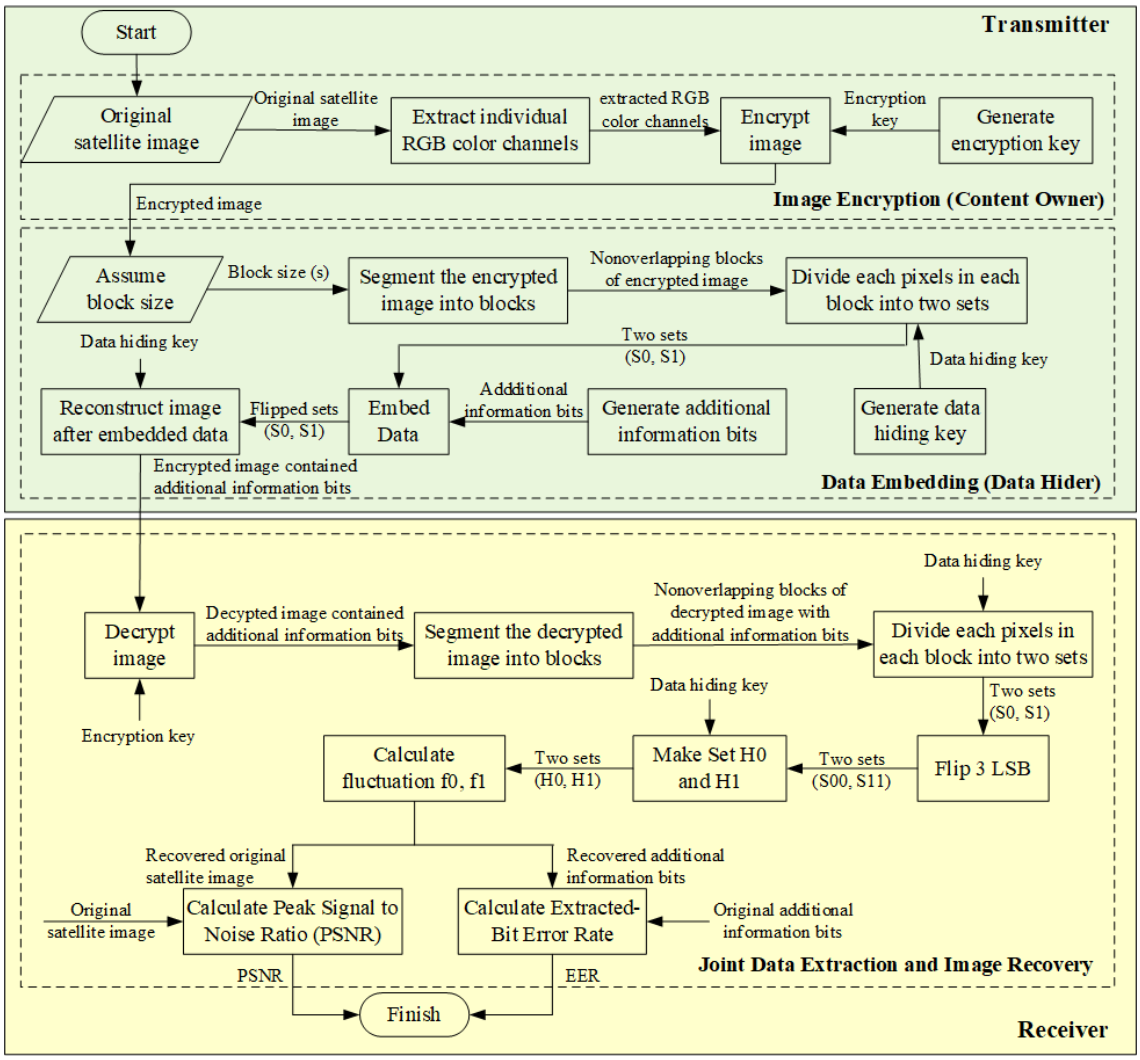

FIGURE 2. Proposed hybrid RDH scheme in remote sensing satellite images with fluctuation function modification.

2) DATA EMBEDDING

Step 1: It is assumed that the block size is $s \times s$. Then, the encrypted satellite image is segmented into some non-overlapping blocks of size $s \times s$. One bit of information can be hidden in a block. $\lfloor \frac{M}{s} \rfloor \times \lfloor \frac{N}{s} \rfloor$ is used for data embedding, where $\lfloor . \rfloor$ is the floor function.

Step 2: Information bits are generated for embedding into encrypted images by considering matrices 0 and 1. Furthermore, each block of pixels is pseudorandomly distributed into two sets, $S0$ and $S1$, according to the data hiding key. If the data hiding key value at the pixel position is 0, then the pixel sets to $S0$; otherwise, it sets to $S1$. The probability that pixels belong to one of the two sets is uniformly distributed.

Step 3: If the information bit to be embedded is '0' in each block of the red channel image, three LSBs of each encrypted pixel are flipped in the S0 set, and the pixel in the S1 set is not changed. Otherwise, if the message bit to be embedded is '1,' three LSBs of each encrypted pixel in the S1 set are reversed, and the pixels in the $S0$ set are not changed. Assume that g_w becomes a function for flipping w LSB from the encrypted pixels. Thus, the flip function of three LSBs, g_3, is expressed as

$$g_3 = 00000111_{(2)} \tag{2}$$

This process continues until all information bits are embedded. After that, the image is reconstructed to obtain an encrypted image containing additional information bits and is then sent to the receiver.

3) HYBRID DATA EXTRACTION AND IMAGE RECOVERY

After receiving an encrypted satellite image containing additional information bits, the receiver first decrypts the image. To start the image decryption phase, the receiver decrypts the encrypted image $C'_{i,j}$ based on the encryption key. Then, the decrypted pixel that contains additional information bits $p'_{i,j}$

can be declared [12] as

$$q'_{i,j} = \begin{cases} \overline{q_{i,j}} & for\ C'_{i,j} = \overline{C_{i,j}} \\ q_{i,j} & for\ C'_{i,j} = C_{i,j} \end{cases} \quad (3)$$

where $\overline{p_{i,j}}$ is the value obtained by flipping w LSB from pixels $p_{i,j}$. Furthermore, the receiver may extract data and recover the original satellite image from the decrypted image by adopting the following steps:

Step 1: Decrypted images containing additional bits of information are described into red, green and blue channels. Furthermore, the decrypted red channel image is segmented into some nonoverlapping blocks of size $s \times s$ that are identical to the initial embedding data.

Step 2: The pixels of each block are pseudorandomly distributed into two sets, $S0$ and $S1$, in accordance with the data hiding key, as in data embedding. If the data hiding key value at the pixel position is 0, then it is set to $S0$; otherwise, it is set to $S1$.

Step 3: Three LSBs on the $S0$ and $S1$ sets are flipped to obtain two sets of $S00$ and $S11$. After that, two sets of $H0$ and $H1$ are made. If the data hiding key value at the pixel position is '0,' then $S00$ and $S0$ are set into the $H0$ set. Otherwise, $S1$ and $S11$ are set into the $H1$ set.

Step 4: To determine the original image block and extract hidden bits, the fluctuation of $H0$ and $H1$ is calculated using the proposed fluctuation function, which is expressed as

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

where $p_{u,v}$ shows the pixel value at position (u, v) in a block. In the proposed fluctuation function, f_p, upright and horizontal values as well as border pixels are used to calculate distances. In addition, both right and left corner pixels are counted to specify the space from the horizontal axis, and the top and bottom corner pixels are counted to specify the space from the vertical axis. For example, each f_p^0 and f_p^1 value becomes the fluctuation function of the $H0$ and $H1$ blocks. By comparing data extraction f_p^0 and f_p^1, image recovery can be performed. If $f_p^0 < f_p^1$, $H0$ will be the original block, and the "0" bit will be the extracted hidden bit. Otherwise, $H1$ will be the original block, and the "1" bit will be the extracted hidden bit. Finally, the extracted hidden bits are combined to obtain information, while bits and blocks are combined to create the original image.

Step 5: The red channel is combined with the green and blue channels to provide the recovered original image. Finally, EER is calculated by comparing each pixel of the original matrix of information bits with the recovered matrix of information bits and PSNR to evaluate the image recovery performance defined [10] by

$$PSNR = 10\, log_{10} \frac{255^2}{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(p_{i,j} - h'_{i,j}\right)^2} \quad (5)$$

where $p_{i,j}$ and $h'_{i,j}$ respectively are original pixel value and modified pixel value.

B. PROPOSED HYBRID RDHEI SCHEME IN REMOTE SENSING SATELLITE IMAGES WITH MODIFIED FLUCTUATION FUNCTIONS AND RS CODE EMBEDDING

The proposed schematic flow diagram is given in Figure 3, which has the following three stages: image encryption, codeword embedding, hybrid codeword extraction and image recovery. The data hider embeds the information bits in the form of RS codeword bits that are generated through the RS encoder process. At the receiver, the estimated value for the inserted codeword bits is extracted using the fluctuation function. Furthermore, hidden data should be restored after the RS decoder. Through the aid of error-correcting capabilities on RS codes, the performance to restore the original satellite image could be improved. The detailed procedure is presented below.

1) CODEWORD EMBEDDING

For an encrypted image, the data hider is not permitted to obtain the content and does not have the right to access it. However, the data hider embeds bits of information into the encrypted satellite image, $C_{i,j}$. The detailed codeword embedding steps are as follows:

Step 1: The block size $s \times s$ is assumed. Then, the encrypted satellite image is segmented into nonoverlapping blocks of size $s \times s$. One bit of information can be hidden in a block. This being said, the maximum number of blocks, J_b, are embedded in an encrypted satellite image as $\lfloor \frac{M}{s} \rfloor x \lfloor \frac{N}{s} \rfloor$, where $\lfloor . \rfloor$ means the floor function.

Step 2: Rate matching and RS encoding processes are performed to produce RS codewords that will be embedded into encrypted satellite images. Generally, RS codes [31] are specified in the Galois field, $GF(2^q)$, where q is a nonnegative integer. Then, the RS code parameter (n, k) with code n length and k data dimension is expressed as $n = 2^q - 1$, $\tau = \lfloor \frac{n-k}{2} \rfloor$, where τ represents the maximum number of symbol errors that can be corrected by the RS decoder. The RS codes rate is expressed as $\frac{k}{n}$. It is recognized that messages and RS codes can be stated as:

$$m(X) = m_0 + m_1 X + \ldots + m_k X^{k-1}$$
$$c(X) = c_0 + c_1 X + \ldots + c_n X^{n-1}$$

where $m(X)$ and $c(X)$ are message polynomials and codeword polynomials, respectively. Polynomial generators are defined as:

$$g(X) = (X - \alpha)\left(X - \alpha^2\right) \ldots \left(X - \alpha^{2\tau}\right) = g_0 + \ldots + g_{2\tau} X^{2\tau}$$

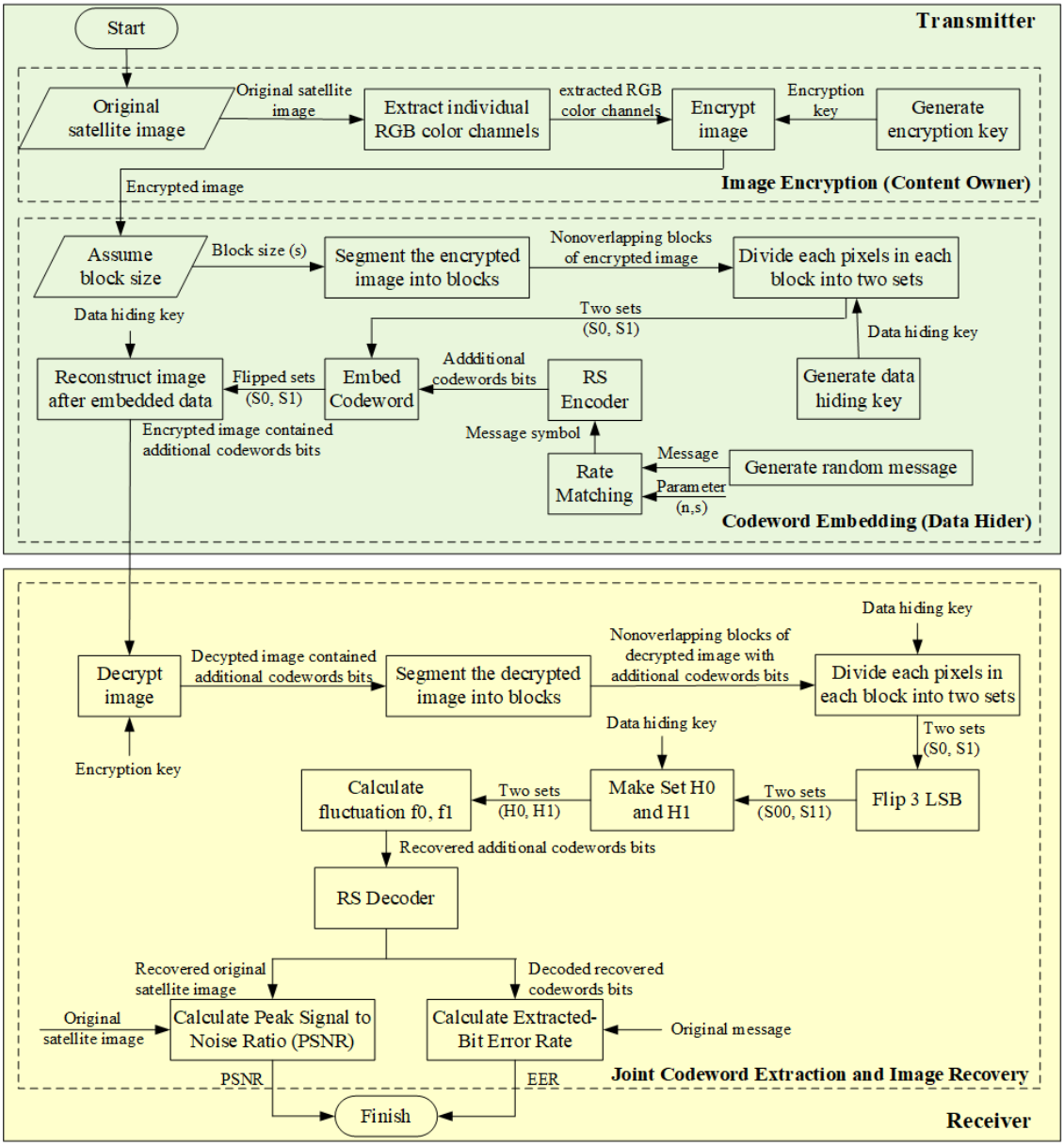

FIGURE 3. Proposed hybrid reversible data hiding scheme in remote sensing satellite images with RS code embedding.

where α is the primitive element $GF\left(2^q\right)$. Systematic encoding of RS codes is expressed [34]-[36] as follows:

$$c\left(X\right) = X^{2\tau} m\left(X\right) + p\left(X\right) \tag{6}$$

where $p\left(X\right)$ is a parity polynomial with a degree $< 2\tau$ and is a residual polynomial when $X^{2\tau} m\left(X\right)$ divided by $g\left(X\right)$.

The maximum number of codewords, J_c, in the encrypted image is $\left\lfloor \frac{J_b}{nq} \right\rfloor$. In the matching of rate, the number of input message bits for the RS encoder, J_{kb}, in the encrypted image is kqJ$_c$. The remaining $J_b - J_{kb}$ bits are zero-padded.

Step 3: By using the RS code codewords, the data hider can insert J_c codewords into the encrypted image. Assume c_a is the a^{th} codeword $\left(c_a\left(0\right), c_a\left(1\right), \ldots, c_a\left(n-1\right)\right)$ *for* $a = 0, 1, \ldots, J_c - 1$, $c_a\left(b\right)$ is an element of $GF\left(2^q\right)$. There is bijection mapping of B between elements in $GF\left(2^q\right)$ and q elements in $GF\left(2\right)$ in accordance with the primitive polynomial $GF\left(2^q\right)$. Hence, binary bits can be defined from the $GF\left(2^q\right)$ element by the B_{F2B} bijection function [30] as

$$B_{F2B} = c_{a,b}\left(0\right), c_{a,b}\left(1\right), \ldots, c_{a,b}\left(q-1\right) \tag{7}$$

where $c_a\left(b\right) \in GF\left(2^q\right)$ for $b = 0, 1, \ldots, n-1$ and $c_{a,b}\left(d\right) \in GF\left(2^q\right)$ for $d = 0, 1, \ldots, q-1$. The mapping of B_C can be applied to the c_a codeword as follows [30]:

$$B_C\left(c_a\right) = \left(B_{F2B}c_a\left(0\right), B_{F2B}c_a\left(1\right), \ldots, B_{F2B}c_a\left(n-1\right)\right) \tag{8}$$

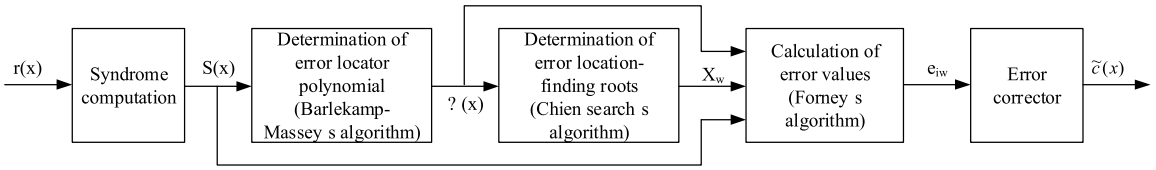

FIGURE 4. Decoding architecture of RS codes.

Then, the combined total of all codeword binary bits, z, can be expressed [30] as:

$$z = \left(B_C\left(c_0\right), B_C\left(c_1\right), \ldots, B_C\left(c_{J_c-1}\right)\right) \tag{9}$$

To employ z to the array block, $y\,(u, v)$, elements from the u^{th} row and the v^{th} column in y mapped from the $\left(u\left\lfloor\frac{M}{s}\right\rfloor + v\right)$ element of z can be declared [30] as:

$$y\,(u, v) = z\left(u\left\lfloor\frac{M}{s}\right\rfloor + v\right) \tag{10}$$

where $0 \leq u < \left\lfloor\frac{M}{s}\right\rfloor$ and $0 \leq v < \left\lfloor\frac{N}{s}\right\rfloor$.

Step 4: In block (u, v), encrypted pixels $\mathrm{C_{i,j}}$, which meet us $\leq i < (u+1)\,s$, $v\,vs \leq j < (v+1)\,s$, are in the same block, where u, v is a positive integer. For each block (u, v), the s^2 pixels are pseudorandomly distributed into two sets, $S_0\,(u, v)$ and $S_1\,(u, v)$, are distributed uniformly according to the data hiding key. $y\,(u, v)$ is embedded into blocks (u, v) by flipping w LSB in the set, which is specified by the codeword bit value. If $y\,(u, v)$ is "0," w LSB of each encrypted pixel in the red channel $\mathrm{S_0}$ (u, v) is flipped. Similarly, if $y\,(u, v)$ is "1," w LSBs of pixels in the red channel $S_1\,(u, v)$ are flipped. The function used to reverse w LSB from encrypted pixels is the same as in equation (4).

Encrypted pixels with attached codeword bits, $C'_{i,j}$, can be stated [30] as:

$$C'_{i,j} = \begin{cases} \overline{C_{i,j}} & for\ i, j \in S0\,(u, v)\ \ and\ y\,(u, v) = 0 \\ \overline{C_{i,j}} & for\ i, j \in S1\,(u, v)\ \ and\ y\,(u, v) = 1 \\ C_{i,j} & others \end{cases} \tag{11}$$

where $\overline{C_{i,j}} = C_{i,j} \oplus g_w$. After that, the red, green, and blue channels are combined again to obtain an encrypted image containing codeword bits.

2) HYBRID CODEWORD EXTRACTION AND IMAGE RECOVERY

After calculating the fluctuation function, the estimated bit codewords are then processed by the RS decoder to detect and correct errors that occur in the codeword bits. The RS decoding algorithm, the Barlekamp-Massey (BM) algorithm, Chien search, and the Forney algorithm [34], [35] are considered in the proposed system. The decoding architecture of RS codes can be seen in Figure 4.

Let r be one of $\hat{c}_a$ for $a = 0, 1, \ldots, J_c - 1$ and $r\,(X)$ be the polynomial look of r. Then, the polynomial $r\,(X)$ can be defined as:

$$r\,(X) = r_0 + r_1 X + r_2 X^2 + \ldots + r_{n-1} X^{n-1}$$

where $\mathrm{r_b}$ is the $GF\,(2^q)$ element for $b = 0, 1, \ldots, n-1$. The obtained polynomial can be considered as the sum of the codeword polynomial sent $c'\,(X)$ and the polynomial error $e\,(X)$ given by:

$$r\,(X) = c'\,(X) + e\,(X)$$

The RS decoder attempts to identify the position and error value up to τ error with the following steps:

a: CALCULATE THE SYNDROME

Syndrome is an evaluation of the received polynomial $r\,(X)$ for each root of the polynomial generator $g\,(X)$. To determine the location and error value, the $\mathrm{S_i}$ syndrome for $j = 1, 2, \ldots, 2\tau$ can be specified [34], [35] as:

$$S_i = c\left(\alpha^j\right) + e\left(\alpha^j\right) = e_0 + e_1\alpha^i + \ldots + e_{n-1}\alpha^{j(n-1)} \tag{12}$$

where α is a primitive element in $GF\,(2^q)$, $(X) = 0$ for $X = \alpha^j$ and $j = 1, 2, \ldots, 2\tau$. The syndrome polynomial is defined [34], [35] as:

$$S\,(X) = S_1 + S_2 X + S_\tau X^{2\tau-1} = \sum_{i=0}^{2\tau-1} S_{i+1} X^i \tag{13}$$

If all syndromes are equal to zero, then there is no codeword change during transmission, and the decoding algorithm for the given data block has been completed.

b: DETERMINE THE ERROR LOCATOR POLYNOMIAL WITH THE BARLEKAMP-MASSEY ALGORITHM

The Berlekamp-Massey algorithm is a computationally effective method for solving key equations in terms of the number of operations in $GF\,(2^q)$. This method is often implemented in software decoders. The polynomial error location $\Lambda\,(X)$ is defined [34], [35] as:

$$\Lambda\,(X) = \Lambda_0 + \Lambda_1 X + \ldots + \Lambda_{t-1} X^{u-1} \tag{14}$$

where w is the amount of errors, and $\mathrm{w} \leq \tau$.

c: SEARCH THE ROOT ERROR EVALUATION POLYNOMIAL

Calculation of the root polynomial with coefficients for $\mathrm{GF}\,(2^9)$ is performed using the Chien search algorithm [34], [35]. The multiplicative inversion of the root polynomial error location $\Lambda\,(X)$ represents the position of the error $\mathrm{i_b}$ in the received polynomial $r\,(X)$.

d: CALCULATE THE ERROR VALUE WITH THE FORNEY ALGORITHM

In the BM algorithm [34], [35], the coefficient of the error location polynomial is determined from (14). Then, the location of the error can be found by solving the roots $\alpha^{i_0}, \alpha^{i_1}, \ldots, \alpha^{i_{u-1}}$ of the polynomial. Forney's method [32], [33] exploits each error spot to determine the appropriate error value. Before calculating the error value, two parameters are needed: polynomial syndrome, $S(X)$, and error locator polynomial. The error evaluator polynomial, $\Omega(X)$, is defined [34], [35] as

$$\Omega(X) = S(X)\,\Lambda(X)\left(modX^{2\tau}\right) \tag{15}$$

The error value, e_{i_w}, is calculated [29], [30] with

$$e_{i_w} = -\frac{\Omega\left(\alpha^{-i_u}\right)}{\Lambda'\left(\alpha^{-i_u}\right)} \tag{16}$$

where $\Lambda'(X)$ is a derivation of (17), and u is from 0 to u-1.

e: CORRECT ERRORS

After knowing the error polynomial, the RS codeword polynomial, $\tilde{c}(X)$, can be determined [34], [35] as:

$$\tilde{c}(X) = r(X) - e(X) \tag{17}$$

After decoding the J_c codewords, the recovered codewords $\tilde{c}_a$ for $a = 0, 1, \ldots, J_c - 1$ are calculated. Systematic RS codes are considered, so the recovered message is obtained by joining kq bits from the recovered codeword.

The image recovery input is codewords $\tilde{c}$, which are recovered, and the pixels are decrypted q'. The recovered codeword bit $\tilde{y}$ is counted, and the recovered $\tilde{c}_a$ codewords are used instead of c_a. After obtaining the decrypted pixels $p'_{i,j}$, the restored pixels $\tilde{h}'_{i,j}$ are defined as:

$$\tilde{h}'_{i,j} = \begin{cases} \overline{q'_{i,j}} & for\ (i,j) \in H0\,(u,v)\ and\ \tilde{y}\,(u,v) = 0 \\ \overline{q'_{i,j}} & for\ (i,j) \in H1\,(u,v)\ and\ \tilde{y}\,(u,v) = 1 \\ q'_{i,j} & others \end{cases}$$

where $\overline{q'_{i,j}} = q'_{i,j} \oplus g_w$, and $\tilde{y}\,(u,v)$ are elements in the u^{th} row and the v^{th} column at $\tilde{y}$.

The red channel is combined with the green and blue channels to provide the restored original satellite image. Furthermore, each pixel of the original codeword bit matrix is compared with the restored codeword bit matrix to calculate EER and PSNR as in equation (5) to evaluate the image recovery performance.

III. RESULTS AND ANALYSIS

In this article, three high-resolution remote sensing satellite test images, namely, SPOT-6, SPOT-7, and Pleiades-1A, are are used. The test image has been resized to 512 × 512 pixels, and each pixel is reflected by 8 bits for efficient processing time. The block size range is from 2 × 2 to 32 × 32. Two performance parameters are analyzed, i.e.,

a. EER is the ratio of incorrect (nonrecoverable) bits to the number of embedded bits.
b. PSNR shows the difference in quality between the original satellite image and the restored original satellite image.

A. PERFORMANCE ANALYSIS OF PROPOSED HYBRID RDH SYSTEM WITH MODIFICATION OF FLUCTUATION FUNCTION

Comparisons of EER and PSNR performances of the recovered image between the proposed modification of the fluctuation function and the functions by Zhang [7], Hong *et al.* [8], and Fatema *et al.* [16] are shown in Figures 5, 6, and 7

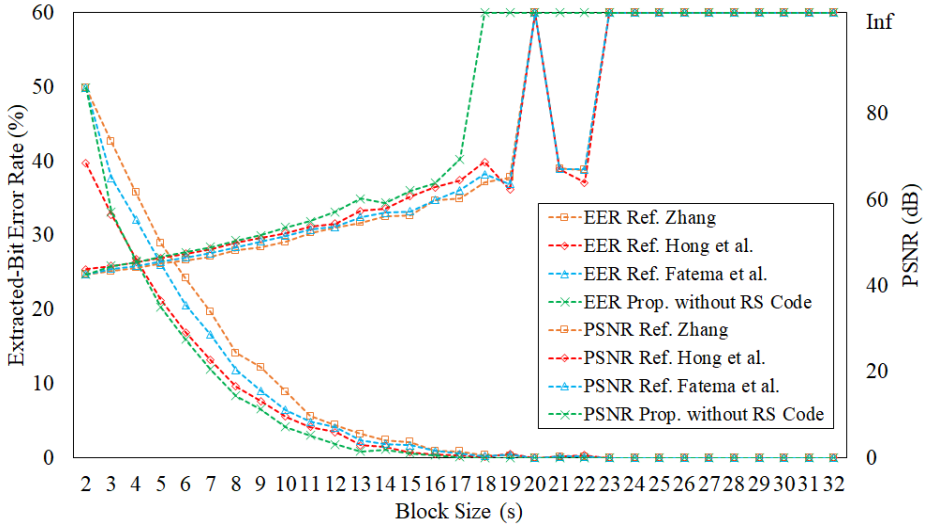

FIGURE 5. Comparison of EER and PSNR of the recovered images in the SPOT-6 test image.

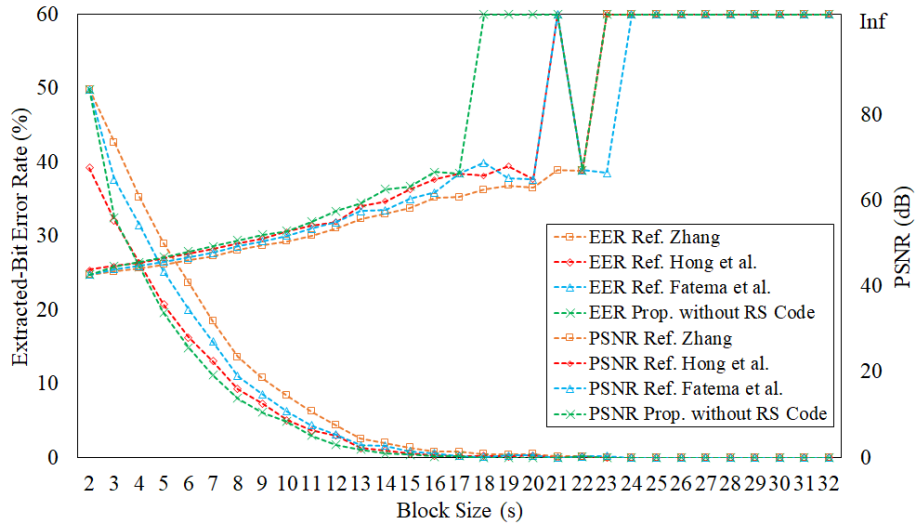

FIGURE 6. Comparison of EER and PSNR of the recovered image in the SPOT-7 test image.

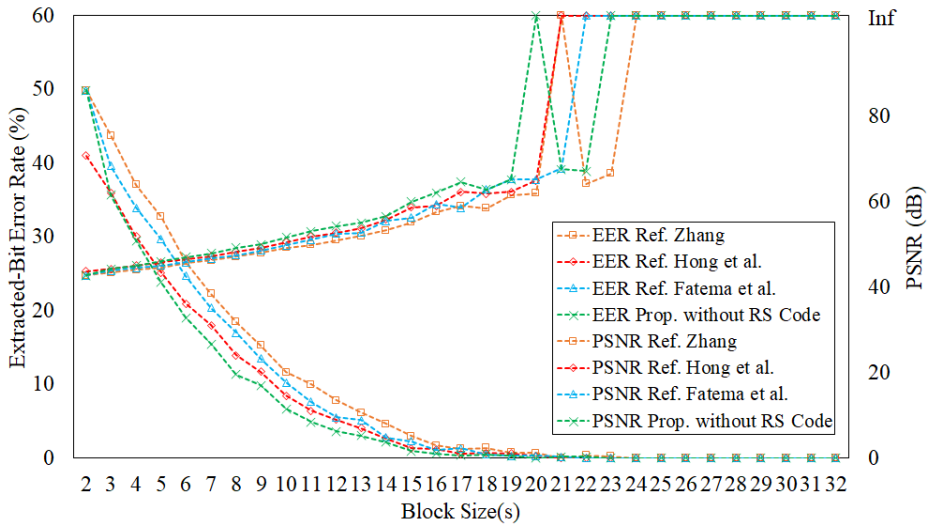

FIGURE 7. Comparison of EER and PSNR of the recovered image in the Pleiades-1A test image.

for the SPOT-6, SPOT-7, and Pleiades-1A test images. Figures 5, 6, and 7 show that the EER performance decreases and PSNR performance increases with increasing block size. It appears that the proposed hybrid RDHEI has a smaller EER and higher PSNR than the methods proposed by Zhang [7], Hong [8], and Fatema [16].

As shown in Figures 6 and 7, there are some anomalies of simulation results in the SPOT-7 and Pleiades-1A test images. In the SPOT-7 test image, when a block size of 22 × 22 occurs, an extracted-bit error of 1 bit occurs in the block position y (3, 12). Based on the fluctuation calculation results, at the position of block y (3, 12), the proposed fluctuation function extracts the wrong information bit, "0," while only the Zhang fluctuation function correctly extracts the embedded information bit into the image, which is bit "1." In the Pleiades-1A test image, when a block size is 21 × 21, there is an extracted-bit error of 1 bit in the block position y (4, 8). Based on the fluctuation calculation, at the position of block y (4, 8), no fluctuation function can extract the information bit that is implanted into the image, that is, the correct bit "1", where all the fluctuation functions extract the wrong information bits, which is bit "0". In addition, with a block size of 22 ×22, there is an extracted-bit error of 1 bit in the block position y (4, 8). Based on the fluctuation calculation, at the position of block y (4, 8), the proposed fluctuation function extracts the wrong information bit, "0," while the Hong and Fatema fluctuation functions correctly extract the information bit embedded into the image, which is bit "1." Table 1 shows the comparison of minimum block sizes, number of embedded message bits, and gain to obtain error-free extracted-bit

TABLE 1. Comparison of minimum block sizes to obtain error-free extracted-bits and maximum PSNR (infinity) in the SPOT-6, SPOT-7, and Pleiades-1A test images

Methods	Minimum block size	Number of message (bits)	Gain (%) to		
			Zhang [7]	Hong et al. [8]	Fatema et al. [16]
SPOT-6					
Zhang [7]	20x20	625	100.00	100.00	100.00
Hong et al. [8]	20x20	625	100.00	100.00	100.00
Fatema et al. [16]	20x20	625	100.00	100.00	100.00
Proposed without RS code	18x18	784	125.44	125.44	125.44
SPOT-7					
Zhang [7]	23x23	484	100.00	84.03	84.03
Hong et al. [8]	21x21	576	119.01	100.00	100.00
Fatema et al. [16]	21x21	576	119.01	100.00	100.00
Proposed without RS code	18x18	784	161.98	136.11	136.11
PLEIADES-1A					
Zhang [7]	21x21	576	100.00	100.00	108.88
Hong et al. [8]	21x21	576	100.00	100.00	108.88
Fatema et al. [16]	22x22	529	91.84	91.84	100.00
Proposed without RS code	20x20	625	108.51	108.51	118.15

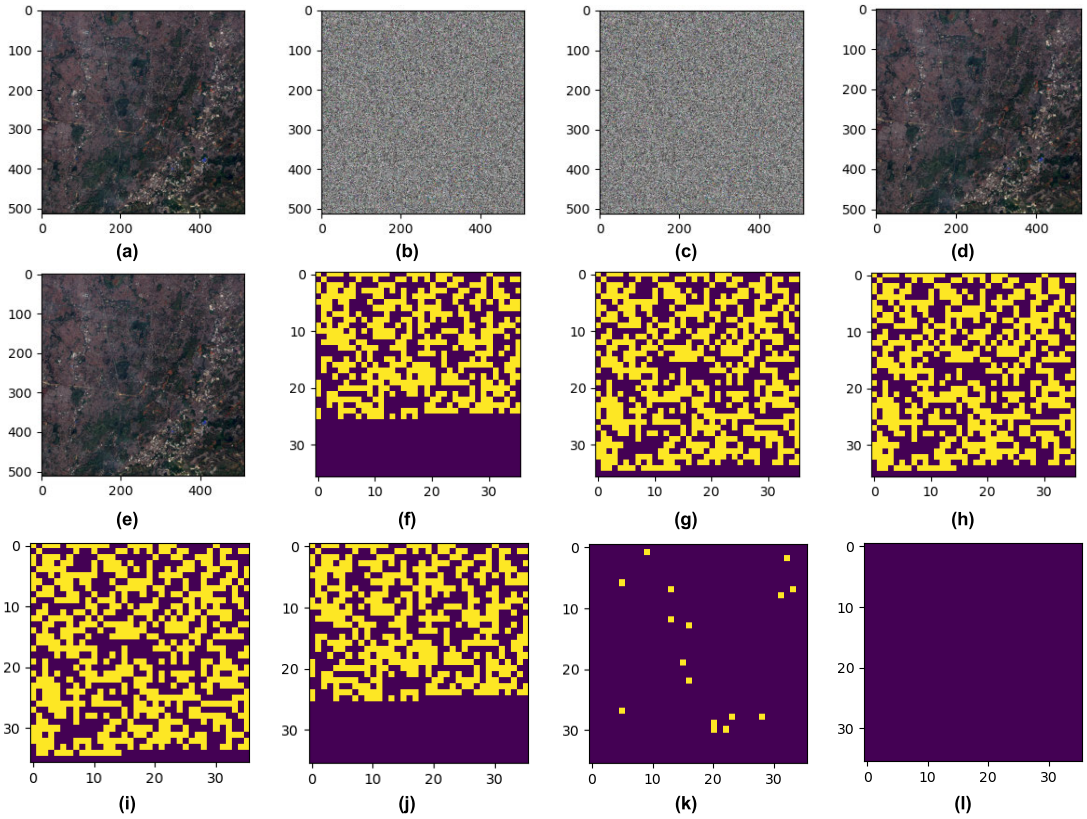

FIGURE 8. Simulation results display of the proposed method by modifying the fluctuation function and RS codes embedding in the SPOT-6 image. (a) original SPOT-6 test image; (b) encrypted image; (c) encrypted image containing data; (d) decrypted image containing data; (e) recovered image after RS decoding; (f) embedded data in the image before RS encoding; (g) embedded codewords in the image after RS encoding; (h) recovered codewords before RS decoding; (i) recovered codewords after RS decoding; (j) recovered data after RS decoding; (k) incorrect extracted bit before RS decoding; (l) incorrect extracted bit after RS decoding.

and maximum PSNR (infinity) between the proposed hybrid RDHEI systems without RS codes and references in the SPOT-6, SPOT-7, and Pleiades-1A test images. Gain is the ratio between the number of bits embedded from a comparison system and the number of bits embedded from the system being compared.

As shown in Table 1, the minimum block size of the proposed system is always smaller, and the number of embedded message bits is always greater than those in [7], [8], and [16] for all satellite images tested. It can be concluded that the hybrid RDHEI system with modification of the fluctuation function succeeded in improving the minimum block

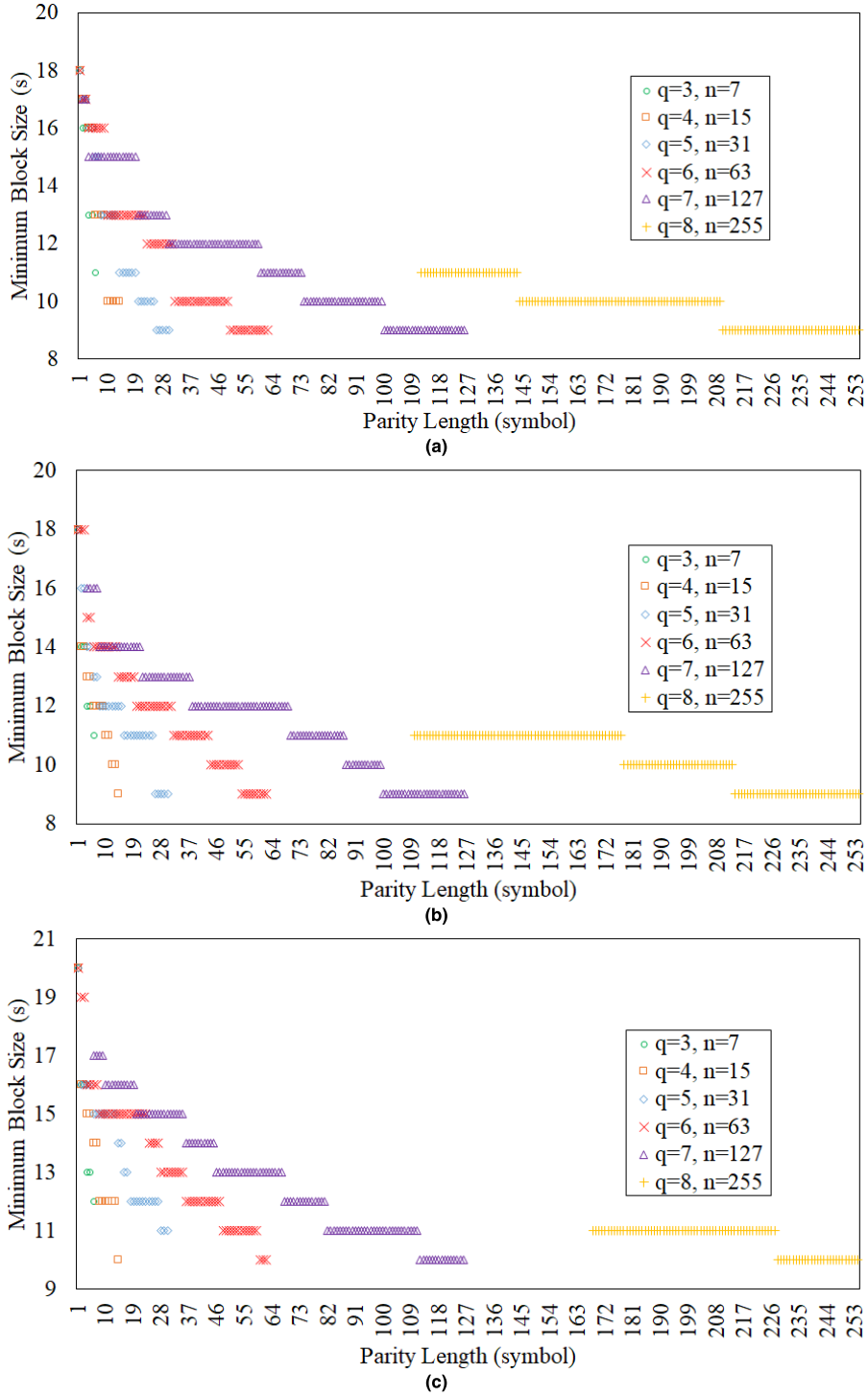

FIGURE 9. Minimum block size to obtain error-free extracted-bits and maximum PSNR (infinity) with the proposed RS codes embedding in satellite test images. (a) SPOT-6; (b) SPOT-7; (c) Pleiades-1A.

size and number of message bits embedded from [7], [8], and [16]. It can also be seen in Table 1 that the proposed hybrid RDHEI system provides a gain $\geq$ 100% because it has more embedded message bits than those in [7], [8], and [16].

B. PERFORMANCE ANALYSIS OF THE PROPOSED HYBRID RDHEI SYSTEM WITH MODIFICATION OF FLUCTUATION FUNCTIONS AND RS CODES EMBEDDING SCHEME

In this section, simulation results from the hybrid RDHEI system for remote sensing satellite images using

TABLE 2. Minimum block size to obtain error-free extracted-bits with several methods for testing SPOT-6 image

Methods	Rate	Minimum block size	Number of messages (bits)	Gain (%) to									
				Zhang [7]	Hong et al. [8]	Fatema et al. [16]	Taesoo et al. with RS(15,7) [29]	Taesoo et al. with RS(31,21) [29]	Sunghwan with RS (15,11) [30]	Sunghwan with RS (15,7) [30]	Sunghwan with RS (31,23) [30]	Sunghwan with RS (31,15) [30]	Proposed without RS code
SPOT-6 Remote Sensing Test Image													
Zhang [7]	1	20x20	625	100.00	100.00	100.00	148.81	142.05	183.82	89.29	126.26	87.41	79.72
Hong et al. [8]	1	20x20	625	100.00	100.00	100.00	148.81	142.05	183.82	89.29	126.26	87.41	79.72
Fatema et al. [16]	1	20x20	625	100.00	100.00	100.00	148.81	142.05	183.82	89.29	126.26	87.41	79.72
Taesoo et al. with RS(15,7) [29]	0.47	14x14	420	67.20	67.20	67.20	100.00	95.45	123.53	60.00	84.85	58.74	53.57
Taesoo et al. with RS(31,21) [29]	0.68	14x14	440	70.40	70.40	70.40	104.76	100.00	129.41	62.86	88.89	61.54	56.12
Sunghwan with RS(15,11) [30]	0.73	16x16	340	54.40	54.40	54.40	80.95	77.27	100.00	48.57	68.69	47.55	43.37
Sunghwan with RS(15,7) [30]	0.47	11x11	700	112.00	112.00	112.00	166.67	159.09	205.88	100.00	141.41	97.90	89.29
Sunghwan with RS(31,23) [30]	0.74	13x13	495	79.20	79.20	79.20	117.86	112.50	145.59	70.71	100.00	69.23	63.14
Sunghwan with RS(31,15) [30]	0.48	11x11	715	114.40	114.40	114.40	170.24	162.50	210.29	102.14	144.44	100.00	91.20
Proposed without RS code	1	18x18	784	125.44	125.44	125.44	186.67	178.18	230.59	158.38	109.65	109.65	100.00
Proposed + RS (7, 1)	0.14	11x11	300	48.00	48.00	48.00	71.42	68.18	88.23	42.86	60.61	41.96	38.27
Proposed + RS(15,5)	0.33	10x10	860	137.60	137.60	137.60	204.76	195.45	252.94	122.86	173.74	120.28	109.69
Proposed + RS(31,11)	0.35	10x10	880	140.80	140.80	140.80	209.52	200.00	252.94	125.71	177.78	123.08	112.24
Proposed + RS (31, 5)	0.16	9x9	500	80.00	80.00	80.00	119.05	113.64	147.06	71.43	101.01	69.93	63.78
Proposed + RS(63,31)	0.49	10x10	1116	178.56	178.56	178.56	265.71	253.64	328.24	159.43	225.45	156.08	142.35
Proposed + RS(63,13)	0.21	9x9	624	99.84	99.84	99.84	148.57	141.82	183.53	89.14	126.06	87.27	79.59
Proposed + RS(127,67)	0.53	11x11	938	150.08	150.08	150.08	223.33	213.18	275.88	134.00	189.49	131.19	119.64
Proposed + RS(127,27)	0.21	9x9	567	90.72	90.72	90.72	135.00	128.86	166.76	81.00	114.55	79.30	72.32
Proposed + RS(255,111)	0.44	10x10	888	142.08	142.08	142.08	211.43	201.82	261.18	126.86	179.39	124.20	113.27
Proposed + RS(255,45)	0.18	9x9	360	57.60	57.60	57.60	85.71	81.82	105.88	51.43	72.73	50.35	45.92

RS embedding schemes are discussed. On the sender's side, as shown in Figure 8 (a), the original SPOT-6 test image is encrypted to produce an encrypted image, as shown in Figure 8 (b). Then, by using RS code (31, 23), 1,296 bits consisting of 1,240 codeword bits +54 padding bits are embedded into the encrypted image using a 14 x 14 block size to produce an encrypted image containing the information bits shown in Figure 8 (c).

On the receiving side, encrypted images containing information bits are received and decrypted to produce decrypted images containing information bits, as shown in Figure 8 (d). Finally, the hidden bits are extracted, and the original SPOT-6 image is recovered from the decrypted image containing information bits, as shown in Figure 8 (e).

Generated message data before RS encoding are shown in Figure 8 (f). Codeword data after RS encoding are shown in Figure 8 (g). Recovered codeword data before RS decoding are shown in Figure 8 (h). Recovered data codewords after RS decoding are shown in Figure 8 (i). Recovered message data after RS decoding are shown in Figure 8 (j).

Extraction of incorrect bits before RS decoding is shown in Figure 8 (k). Alternatively, the extraction of incorrect bits after RS decoding is shown in Figure 8 (l). Figures 9 (a), (b), and (c) show the simulation results of the

TABLE 3. Minimum block size to obtain error-free extracted-bits with several methods for testing SPOT-7 image

Methods	Rate	Minimum block size	Number of messages (bits)	Gain (%) to									
				Zhang [7]	Hong et al. [8]	Fatema et al. [16]	Taesoo et al. with RS (15,7) [29]	Taesoo et al. with RS (31,21) [29]	Sunghwan with RS (15,11) [30]	Sunghwan with RS (15,7) [30]	Sunghwan with RS (31,23) [30]	Sunghwan with RS (31,15) [30]	Proposed without RS code
SPOT-7 Remote Sensing Test Image													
Zhang [7]	1	23x23	484	100.00	84.03	84.03	96.80	110.00	96.80	83.45	80.00	67.69	61.73
Hong et al. [8]	1	21x21	576	119.01	100.00	100.00	115.20	130.91	115.20	99.31	95.21	80.56	73.47
Fatema et al. [16]	1	21x21	576	119.01	100.00	100.00	115.20	130.91	115.20	99.31	95.21	80.56	73.47
Taesoo et al. with RS(15,7) [29]	0.47	13x13	500	103.31	86.81	86.81	100.00	113.64	100.00	86.21	82.64	69.93	63.78
Taesoo et al. with RS(31,21) [29]	0.68	14x14	440	90.90	76.39	76.39	88.00	100.00	88.00	75.86	72.73	61.54	56.12
Sunghwan with RS(15,11) [30]	0.73	13x13	500	103.31	86.81	86.81	100.00	113.64	100.00	86.21	82.64	69.93	63.78
Sunghwan with RS(15,7) [30]	0.47	12x12	580	119.84	100.69	100.69	116.00	131.82	116.00	100.00	95.87	81.12	73.98
Sunghwan with RS(31,23) [30]	0.74	12x12	605	125.00	105.03	105.03	121.00	137.50	121.00	104.31	100.00	84.62	77.17
Sunghwan with RS(31,15) [30]	0.48	11x11	715	147.73	124.13	124.13	143.00	162.50	143.00	123.76	118.18	100.00	91.20
Proposed without RS code	1	18x18	784	161.98	136.11	136.11	156.80	178.18	156.80	135.17	129.59	109.65	100.00
Proposed + RS(7,5)	0.71	14x14	915	189.05	158.85	158.85	183.00	207.95	183.00	157.76	151.24	127.97	116.71
Proposed + RS(7,1)	0.14	11x11	300	61.98	52.08	52.08	60.00	68.18	60.00	51.72	49.59	41.96	38.27
Proposed + RS(15,9)	0.60	12x12	1044	215.70	181.25	181.25	208.80	237.27	208.80	180.00	172.56	146.01	133.16
Proposed + RS(15,1)	0.07	9x9	208	42.97	36.11	36.11	41.60	47.27	41.60	35.86	34.38	29.09	26.53
Proposed + RS(31,15)	0.48	11x11	975	201.45	169.27	169.27	195.00	221.59	195.00	168.10	161.16	136.36	124.36
Proposed + RS(31,5)	0.16	9x9	500	103.31	86.81	86.81	100.00	113.64	100.00	86.21	82.64	69.93	63.78
Proposed + RS(63,31)	0.49	11x11	930	192.15	161.46	161.46	186.00	211.36	186.00	160.34	153.72	130.07	118.62
Proposed + RS(63,9)	0.14	9x9	432	89.26	75.00	75.00	86.40	98.18	86.40	74.48	71.40	60.42	55.10
Proposed + RS(127,57)	0.45	11x11	938	193.80	162.85	162.85	187.60	213.18	187.60	161.72	155.04	131.19	119.64
Proposed + RS(127,27)	0.21	9x9	567	117.15	98.44	98.44	113.40	128.86	113.40	97.76	93.72	79.30	72.32
Proposed + RS(255,145)	0.57	11x11	1160	239.67	201.39	201.39	232.00	263.64	232.00	200.00	191.74	162.24	147.96
Proposed + RS(255,41)	0.16	9x9	328	67.77	56.94	56.94	65.60	74.55	65.60	56.55	54.21	45.87	41.84

proposed system with RS codes embedded in the SPOT-6, SPOT-7, and Pleiades-1A test images, respectively.

RS code characteristics ranging from $3 \leq$ GF power (q) ≤ 8 or from $7 \leq$ RS codes length (n) ≤ 255 are simulated to determine the minimum block size to obtain the error-free extracted-bit and maximum PSNR (infinity) of the recovered image. It can be seen in Figures 9 (a), (b), and (c) that the minimum block size will be smaller when using the parity symbol size that becomes longer for the same gf codeword length. This is because the RS code correction capability is also increasing. In addition, with the same parity length, the minimum block size is obtained when using the smallest length of codewords or GF power.

Table 2, Table 3, and Table 4 show the comparison of the main results between the proposed system and RS codes with the reference functions from Zhang [7], Hong *et al.* [8], Fatema *et al.* [16], Kim and Kim [29], Sunghwan [30], and the proposed modification function without RS codes to obtain error-free extracted-bit and maximum PSNR (infinity) in the SPOT-6, SPOT-7, and Pleiades-1A test images, respectively. The minimum block size of the proposed system is always smaller than that of the reference system or the proposed

TABLE 4. Minimum block size to obtain error-free extracted-bits with several methods for testing Pleiades-1A image

Methods	Rate	Minimum block size	Number of messages (bits)	Gain (%) to									
				Zhang [7]	Hong et al. [8]	Fatema et al. [16]	Taesoo et al. with RS (15,7) [29]	Taesoo et al. with RS (31,21) [29]	Sunghwan with RS (15,11) [30]	Sunghwan with RS (15,7) [30]	Sunghwan with RS (31,23) [30]	Sunghwan with RS (31,15) [30]	Proposed without RS code
Pleiades-1A Remote Sensing Test Image													
Zhang [7]	1	21x21	576	100.00	100.00	108.88	169.41	174.55	151.58	99.31	149.61	116.36	92.16
Hong et al. [8]	1	21x21	576	100.00	100.00	108.88	169.41	174.55	151.58	99.31	149.61	116.36	92.16
Fatema et al. [16]	1	22x22	529	91.84	91.84	100.00	155.59	160.30	139.21	91.21	137.40	106.87	84.64
Taesoo et al. with RS(15,7) [29]	0.47	16x16	340	59.03	59.03	64.27	100.00	103.03	89.47	58.62	88.31	68.69	43.37
Taesoo et al. with RS(31,21) [29]	0.68	16x16	330	57.29	57.29	62.38	97.05	100.00	86.84	56.90	85.71	66.67	42.09
Sunghwan with RS(15,11) [30]	0.73	15x15	380	65.97	65.97	71.83	111.76	115.15	100.00	65.52	98.70	76.77	48.47
Sunghwan with RS(15,7) [30]	0.47	12x12	580	100.69	100.69	109.64	170.59	175.76	152.63	100.00	150.65	117.17	73.98
Sunghwan with RS(31,23) [30]	0.74	15x15	385	66.84	66.84	72.78	113.24	116.67	101.16	66.38	100.00	77.78	49.11
Sunghwan with RS(31,15) [30]	0.48	13x13	495	85.94	85.94	93.57	145.59	150.00	85.34	128.57	128.57	100.00	63.14
Proposed without RS code	1	18x18	784	125.44	125.44	125.44	230.59	237.58	206.32	135.17	203.64	158.38	100.00
Proposed + RS(7,3)	0.43	13x13	648	112.50	112.50	122.50	190.59	196.36	170.53	111.72	168.31	130.91	103.68
Proposed + RS(7,1)	0.14	12x12	252	43.75	43.75	47.64	74.18	76.36	66.32	43.45	65.45	50.91	40.32
Proposed + RS(15, 7)	0.46	12x12	812	140.97	140.97	153.49	238.82	246.06	213.68	140.00	210.91	164.04	129.92
Proposed + RS (15,1)	0.07	10x10	172	29.86	29.86	32.51	238.82	52.12	45.26	29.66	44.68	34.75	27.52
Proposed + RS(31,13)	0.42	12x12	715	124.13	124.13	135.16	210.29	216.67	188.16	123.27	185.71	144.44	114.40
Proposed + RS (31,3)	0.10	11x11	195	33.85	33.85	36.86	57.35	59.09	51.32	33.62	50.65	39.39	31.20
Proposed + RS(63,27)	0.43	12x12	648	112.50	112.50	122.50	190.59	196.36	170.53	111.72	168.31	130.91	103.68
Proposed + RS(63,3)	0.05	10x10	108	18.75	18.75	20.42	31.76	32.73	28.42	18.62	28.05	21.81	17.28
Proposed + RS(127, 45)	0.35	11x11	630	109.38	109.38	119.09	185.29	190.91	165.79	108.62	163.64	127.27	100.80
Proposed + RS(127, 15)	0.12	10x10	210	36.46	36.46	39.70	61.76	63.64	55.26	36.21	54.55	42.42	33.60
Proposed + RS(255, 87)	0.34	11x11	696	120.83	120.83	131.57	204.71	210.91	183.16	120.00	180.78	140.61	111.36
Proposed + RS(255, 27)	0.11	10x10	216	37.50	37.50	40.83	63.53	65.45	56.84	37.24	56.10	43.64	34.56

system without RS codes. The minimum block size that can be achieved in the SPOT-6 and SPOT-7 test images is 9 x 9, while in Pleiades-1A, it is 10 x 10.

However the number of bits embedded in the proposed hybrid RDHEI with modification of the fluctuation function and RS code is lower than that in the proposed hybrid RDHEI with modification of the fluctuation function without the RS code. It shows the proposed RDHEI hybrid with modification of the fluctuation function and RS code, which has a minimum block size of 1 or 2 levels lower than the minimum block size but has a gain greater than 100%. Gain is the ratio of the number of bits embedded by the proposed RDHEI system with the RS code to the proposed RDHEI system without the RS codes.

To investigate the performance of the proposed system with RS codes, some characteristics of optimal RS codes, namely, RS codes that provide the minimum block size and the largest number of message bits of each codeword symbol length, are simulated on each test image. For SPOT-6 test images, there are five RS codes used in the simulation: RS (15, 5), RS (31, 11), RS (63, 31), RS (127, 67), and RS (255, 111). For SPOT-7 test images, there are six RS codes used in the simulation, namely, RS (7, 5), RS (15, 9), RS (31, 15), RS (63, 31), RS (127, 57), and RS (255, 145). For the Pleiades-1A test

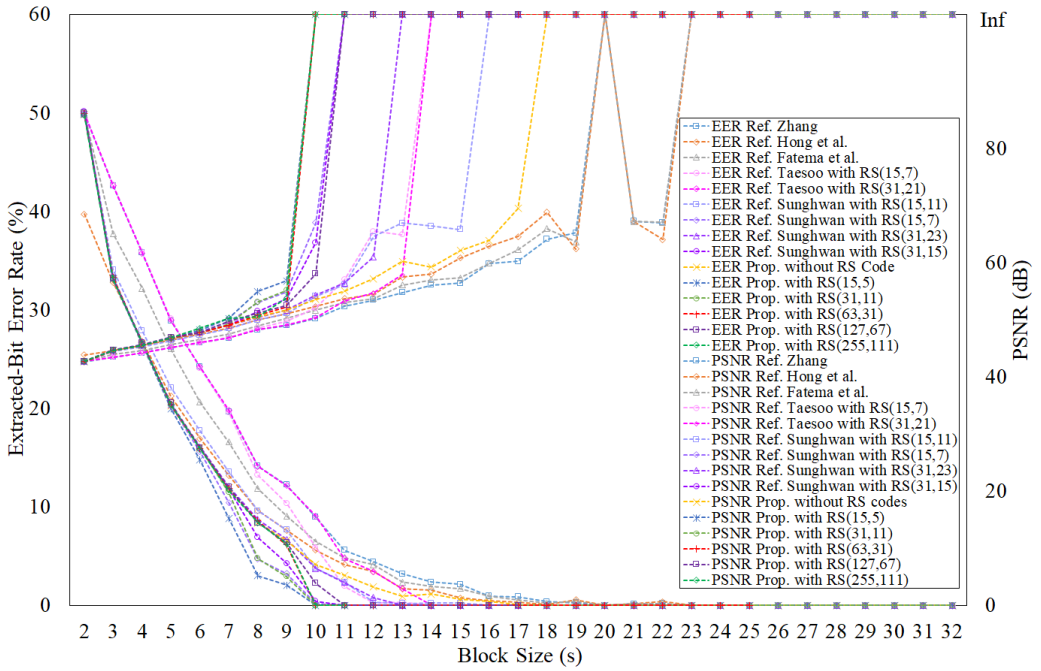

FIGURE 10. Comparison of EER and PSNR performance of the recovered image between the proposed system and the RS codes with the proposed system without RS codes and the three reference systems in the SPOT-6 test image.

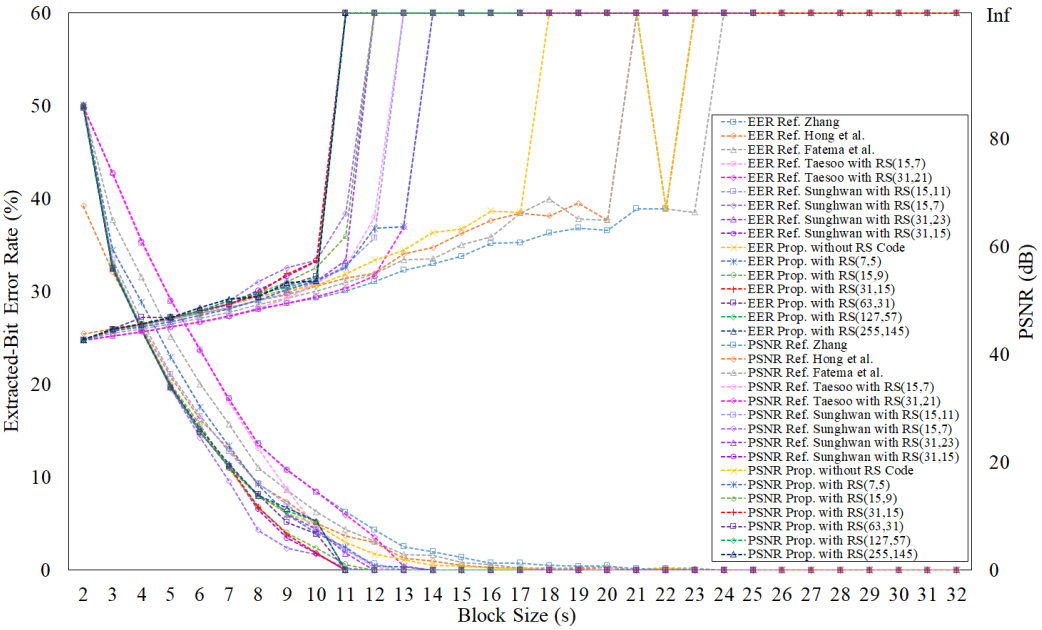

FIGURE 11. Comparison of EER and PSNR performance of the recovered image between the proposed system and the RS codes with the proposed system without RS codes and the three reference systems in the SPOT-7 test image.

image, there are six RS codes used in the simulation, namely, RS (7, 3), RS (15, 7), RS (31, 13), RS (63, 27), RS (127, 45), and RS (255, 87). The EER and PSNR performance of the recovered images from the reference system, the proposed system without RS codes and the proposed system with RS codes for each SPOT-6, SPOT-7, and Pleiades-1A test image are shown in Figures 10-12.

Overall, it appears that the performance of the EER and PSNR recovered images from the proposed system with RS codes is better than the reference system as well as from the proposed system without RS codes. The proposed system with RS codes can provide a smaller minimum block size to achieve error-free extracted-bit and maximum PSNR (infinity) than the three reference systems or the proposed

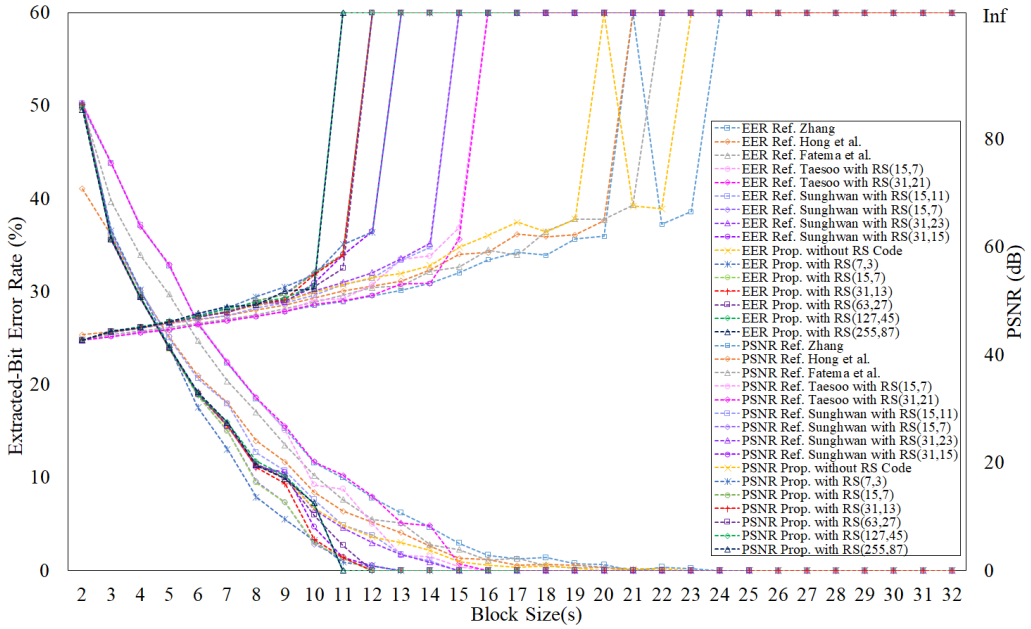

FIGURE 12. Comparison of EER and PSNR performance of the recovered image between the proposed system and the RS codes with the proposed system without RS codes and the three reference systems in the Pleiades-1A test image.

system without RS codes. The proposed system with RS codes can provide a smaller minimum block size to achieve error-free extracted bit and maximum PSNR (infinity) than the reference system or from the proposed system without RS codes.

For the SPOT-6 test image in Figure 10, it is shown that the performance of RS (15, 5), RS (31, 11), RS (63, 31), and RS (255, 111) can provide the minimum block size to obtain an error-free extracted-bit and maximum PSNR (infinity), i.e., block size = 10 x 10. The EER performance of the reference system and the proposed system without RS codes at block size = 10 x 10 is nonzero. Likewise, the PSNR image recovered from the three reference systems and the proposed system without RS codes at block size = 10 x 10 is not infinite. At block sizes smaller than 10 x 10, the proposed system with RS codes gives a lower EER value and a higher PSNR compared to the reference system and the proposed system without RS codes.

For the SPOT-7 test image in Figure 11, it is shown that the performance of RS (31, 15), RS (63, 31), RS (127, 57) and RS (255, 145) can provide the minimum block size needed to obtain an error-free extracted-bit and maximum PSNR (infinity), i.e., block size = 11 x 11. The EER performance of the three reference systems and the proposed system without RS codes at block size = 11 x 11 is not zero. Likewise, the PSNR image recovered from the reference system and the proposed system without RS codes at block size = 11 x 11 is not infinite.

At block sizes smaller than 11 x 11, the proposed system with RS codes gives a lower EER value and a higher PSNR compared to the reference system and the proposed system without RS codes. For the Pleiades-1A test image in Figure 12, it is shown that the performance of RS (127, 45) and RS (255, 87) can provide the minimum block size to obtain an error-free extracted-bit and maximum PSNR (infinity) that is at size block = 11 x 11. The EER performance of the t references system and the proposed system without RS codes at block size = 11 x 11 is not zero.

Likewise, the PSNR image recovered from the reference system and the proposed system without RS codes at block size = 11 x 11 is not infinite. At block sizes smaller than 11 x 11, the proposed system with RS codes gives a lower EER value and a higher PSNR compared to the reference system and the proposed system without RS codes.

As shown in Figures 10, 11, and 12, the proposed hybrid RDHEI with a modification fluctuation function with RS code has succeeded in removing the anomaly of failure and achieves error-free extracted bits that occur on systems without RS codes and reference methods.

IV. CONCLUSION

This study presents a proposed hybrid RDHEI system for remote sensing satellite images with modification of the fluctuation function and RS codes on data embedding for remote sensing satellite test images. The results show that the proposed hybrid RDHEI with the modification of the fluctuation function has a lower EER performance and larger PSNR than existing methods for the same block size. The proposed hybrid RDHEI with modification of the fluctuation function without RS codes can achieve error-free extracted-bit and maximum PSNR (infinity) values when the block size is 18 x 18 for SPOT-6 and SPOT-7 test images, and the block size is 20 x 20 for Pleiades-1A test images. The proposed hybrid RDHEI system with modified fluctuations and

RS code embedding can improve estimation performance better than systems without RS code and reference systems. The proposed system provides error-free extracted-bit and maximum PSNR (infinity) with a smaller block size compared to existing methods and the proposed system without RS codes. For the SPOT-6 test image, a minimum block size of 9 x 9 is obtained, i.e., when using RS (31, 5), RS (63, 13), RS (127, 27), and RS (255, 45). For the SPOT-7 test image, the minimum block size of 9 x 9 is obtained when using RS (15, 1), RS (31, 5), RS (63, 9), RS (127, 27), and RS (255, 41). For the Pleiades-1A test image, a minimum block size of 10 x 10 is obtained when using RS (15, 1), RS (63, 3), RS (127, 15), and RS (255, 27). It was shown that the minimum block size will be smaller when using a longer parity symbol size with the same codeword length or GF power. The proposed hybrid RDHEI with a modification fluctuation function with RS codes succeeded in removing the anomaly of failure and achieves error-free extracted bits that occur on systems without RS code and reference methods. Moreover, there is a suggestion for future works, such as considering all channels to carry additional data and extending the system to correct the error of the covered image.

REFERENCES

[1] N. Kittawi and A. Al-Haj, "Reversible data hiding in encrypted images," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, May 2017, pp. 808–813, doi: 10.1109/ICITECH.2017.8079951.

[2] A. Shaik and V. Thanikaiselvan, "Comparative analysis of integer wavelet transforms in reversible data hiding using thresholdbased histogram modification," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 2018, pp. 1–12, Jun. 2018, doi: 10.1016/j.jksuci.2018.06.001.

[3] A. Benhfid, E. B. Ameur, and Y. Taouil, "Reversible steganographic method based on interpolation by bivariate linear box-spline on the three directional mesh," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 32, no. 7, pp. 850–859, Sep. 2020, doi: 10.1016/j.jksuci.2018.09.016.

[4] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 31, no. 3, pp. 335–347, Jul. 2019, doi: 10.1016/j.jksuci.2018.01.011.

[5] A. K. Sahu, and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 2019, pp. 1–15, Jul. 2019, doi: 10.1016/j.jksuci.2019.07.004.

[6] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 2019, pp. 1–11, Dec. 2019, doi: 10.1016/j.jksuci.2019.12.007.

[7] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011, doi: 10.1109/LSP.2011.2114651.

[8] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012, doi: 10.1109/LSP.2012.2187334.

[9] M. Li, D. Xiao, Z. Peng, and H. Nan, "A modified reversible data hiding in encrypted images using random diffusion and accurate prediction," *ETRI J.*, vol. 36, no. 2, pp. 325–328, Apr. 2014, doi: 10.4218/etrij.14.0213.0449.

[10] X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Process.*, vol. 104, pp. 387–400, Nov. 2014, doi: 10.1016/j.sigpro.2014.04.032.

[11] Z. Qian, X. Zhang, and S. Wang, "Reversible data hiding in encrypted JPEG bitstream," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1486–1491, Aug. 2014, doi: 10.1109/TMM.2014.2316154.

[12] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *J. Vis. Commun. Image Represent.*, vol. 28, pp. 21–27, Apr. 2015, doi: 10.1016/j.jvcir.2014.12.007.

[13] Y. S. Kim, K. Kang, and D. W. Lim, "New reversible data hiding scheme for encrypted images using lattices," in *Appl. Math. Inf. Sci.*, vol. 9, no. 5, pp. 2627–2636, 2015.

[14] M. Li, Y. Zhang, D. Xiao, and A. Kulsoom, "Improved reversible data hiding for encrypted images using full embedding strategy," *Electron. Lett.*, vol. 51, no. 9, pp. 690–691, Apr. 2015, doi: 10.1049/el.2014.4476.

[15] Z. Pan, L. Wang, S. Hu, and X. Ma, "Reversible data hiding in encrypted image using new embedding pattern and multiple judgments," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8595–8607, Jul. 2016, doi: 10.1007/s11042-015-2773-4.

[16] F.-T.-Z. Khanam, K.-Y. Song, and S. Kim, "A modified reversible data hiding in encrypted image using enhanced measurement functions," in *Proc. 8th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Vienna, Austria, Jul. 2016, pp. 869–872.

[17] S. Agrawal and M. Kumar, "Mean value based reversible data hiding in encrypted images," *Optik*, vol. 130, pp. 922–934, Feb. 2017, doi: 10.1016/j.ijleo.2016.11.059.

[18] F.-T.-Z. Khanam and S. Kim, "New fluctuation functions to measure spatial correlation of encrypted images in reversible data hiding," *J. Korean Inst. Commun. Inf. Sci.*, vol. 42, no. 2, pp. 331–337, Feb. 2017.

[19] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012, doi: 10.1109/TIFS.2011.2176120.

[20] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 322–328, Feb. 2014, doi: 10.1016/j.jvcir.2013.11.001.

[21] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," *Sci. World J.*, vol. 2014, pp. 1–8, May 2014, doi: 10.1155/2014/604876.

[22] Z. Qian, X. Zhang, and G. Feng, "Reversible data hiding in encrypted images based on progressive recovery," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1672–1676, Nov. 2016, doi: 10.1109/LSP.2016.2585580.

[23] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016, doi: 10.1109/TCSVT.2015.2418611.

[24] D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," *Signal Process.*, vol. 123, pp. 9–21, Jun. 2016, doi: 10.1016/j.sigpro.2015.12.012.

[25] 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 Represent.*, vol. 45, pp. 1–10, May 2017, doi: 10.1016/j.jvcir.2017.02.001.

[26] C. Qin, Z. He, X. Luo, and J. Dong, "Reversible data hiding in encrypted image with separable capability and high embedding capacity," *Inf. Sci.*, vol. 465, pp. 285–304, Oct. 2018, doi: 10.1016/j.ins.2018.07.021.

[27] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013, doi: 10.1109/TIFS.2013.2248725.

[28] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Process.*, vol. 94, pp. 118–127, Jan. 2014, doi: 10.1016/j.sigpro.2013.06.023.

[29] T. Kim and S. Kim, "Efficient transmission of reversible data hiding in encryption images by using Reed–Solomon codes," in*Proc. 3rd Int. Conf. Future Internet Things Cloud*, Rome, Italy, 2015, pp. 765–769, doi: 10.1109/FiCloud.2015.31.

[30] S. Kim, "Reversible data-hiding systems with modified fluctuation functions and Reed–Solomon codes for encrypted image recovery," *Symmetry*, vol. 9, no. 5, p. 61, Apr. 2017, doi: 10.3390/sym9050061.

[31] SPOT-6 satellite sensor (1.5m). (2013). *Satellite Imaging Corporation, Airbus Defence and Space*. Accessed: Jun. 1, 2020. [Online]. Available: https://www.satimagingcorp.com/satellite-sensors/spot-6/

[32] SPOT-7 Satellite Sensor (1.5m). (2013). *Satellite Imaging Corporation, Airbus Defence and Space*. Accessed: Jun. 1, 2020. [Online]. Available: https://www.satimagingcorp.com/satellite-sensors/spot-7/

[33] Pleiades-1A satellite sensor (0.5m). (2013). *Satellite Imaging Corporation, Airbus Defence and Space*. Accessed: Jun. 1, 2020. [Online]. Available: https://www.satimagingcorp.com/satellite-sensors/pleiades-1/

[34] J. G. Proakis, M. Salehi, *Digital communications*. New York, NY, USA: McGraw-Hil, 2008, pp. 471–475.

[35] T. K. Moon, *Error Correction Coding*. Hoboken, NJ, USA: Wiley, 2004.

[36] *Reedsolo 1.5.4. 2020*. Accessed: Mar. 31, 2020. [Online]. Available: https://pypi.org/project/reedsolo/

GUNAWAN WIBISONO (Member, IEEE) received the B.Eng. degree in electrical engineering from the University of Indonesia, Depok, Indonesia, in 1990, and the M.Eng. and Ph.D. degrees from Keio University, Japan, in 1995 and 1998, respectively. He is the former Head of the Department of Electrical Engineering, University of Indonesia. His research interests include coding and wireless communications, electronics and optical communications, and telecommunication regulation.

ALI SYAHPUTRA NASUTION was born in Deli Serdang, Indonesia, in 1983. He received the S.T. degree in telecommunication engineering from the Sekolah Tinggi Teknologi Telkom, Bandung, Indonesia, in 2005, and the M.T. degree in electrical engineering from the University of Indonesia, Depok, Indonesia, in 2020. Since 2008, he has been an Engineer with the Remote Sensing Technology and Data Center, National Institute of Aeronautics and Space. His research interests include remote sensing ground station development, error control coding, signal and image processing, and data hiding application.

TEGUH FIRMANSYAH (Member, IEEE) was born in Subang, Indonesia. He received the B.Eng. (S.T.) degree in electrical engineering and the M.Eng. (M.T.) degree in telecommunication engineering from the Department of Electrical Engineering, Universitas Indonesia, in 2010 and 2012, respectively. He is currently pursuing the Ph.D. degree (double degree program) in electrical engineering with Universitas Indonesia and Shizuoka University. In 2012, he joined the Department of Electrical Engineering, Universitas Sultan Ageng Tirtayasa, as a Researcher and a Lecturer. He has authored or coauthored over 40 articles published in refereed journals and conferences. He holds two patents for wideband antenna and multiband antenna. His research interests include microstrip antenna and microwave circuit for various applications. He is a member of the IEEE Antenna and Propagation Society and the IEEE Microwave Theory and Technique Society. He has been a Reviewer of *Electronics Letters*, the *International Journal of Microwave and Wireless Technologies* (Cambridge), *Wireless Personal Communications* (Springer), the *International Journal of Electronics and Communications* (Elsevier), *Microwave and Optical Technology Letters* (Wiley), the *International Journal of RF and Microwave Computer-Aided Engineering* (Wiley), and IEEE Access.

ANTON SATRIA PRABUWONO (Senior Member, IEEE) started his academic career at the Institute of Electronics, National Chiao Tung University, Taiwan, in 2006, and the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, in 2007. He joined the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia in 2009. He joined the Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia, in 2013, where he is currently a Professor. He was an Erasmus Mundus Visiting Professor with the Department of Mechanical Engineering and Mechatronics, Karlsruhe University of Applied Sciences, Germany. His research interests include computer vision, intelligent systems, and industrial computing. He is a Senior Member of ACM.