Received: 23 November 2018 | Revised: 14 November 2019 | Accepted: 24 March 2020

DOI: 10.4218/etrij.2018-0631

ORIGINAL ARTICLE

ETRI Journal WILEY

Region-based scalable self-recovery for salient-object images

Navid Daneshmandpour | **Habibollah Danyali** | **Mohammad Sadegh Helfroush**

Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran

Correspondence
Habibollah Danyali, Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran.
Email: danyali@sutech.ac.ir

Self-recovery is a tamper-detection and image recovery methods based on data hiding. It generates two types of data and embeds them into the original image: authentication data for tamper detection and reference data for image recovery. In this paper, a region-based scalable self-recovery (RSS) method is proposed for salient-object images. As the images consist of two main regions, the region of interest (ROI) and the region of non-interest (RONI), the proposed method is aimed at achieving higher reconstruction quality for the ROI. Moreover, tamper tolerability is improved by using scalable recovery. In the RSS method, separate reference data are generated for the ROI and RONI. Initially, two compressed bitstreams at different rates are generated using the embedded zero-block coding source encoder. Subsequently, each bitstream is divided into several parts, which are protected through various redundancy rates, using the Reed-Solomon channel encoder. The proposed method is tested on 10 000 salient-object images from the MSRA database. The results show that the RSS method, compared to related methods, improves reconstruction quality and tamper tolerability by approximately 30% and 15%, respectively.

KEYWORDS
image authentication, region-based, salient object, scalable self-recovery, tamper detection

1 | INTRODUCTION

With the development of technology, image authentication has found new applications in areas such as education, health care, and social networks. Moreover, low-cost and straightforward image-processing software facilitates image forgery. Therefore, image authentication is a critical issue for preserving content against forgery [1,2]. Conventional image authentication methods, such as digital signatures, can only prove the integrity of an image, whereas the exact tamper location cannot be determined [3]. Digital watermarking is an alternative approach not only for tamper detection but also for image recovery. In tamper detection and recovery, also termed self-recovery, authentication and reference data are generated and embedded into the original image. On the receiver side, the tampered area is detected and localized by the authentication data, and the image is recovered using the authentic parts of the extracted reference data [4–6].

Most self-recovery methods are classified into two categories: flexible [7–9] and adaptive [10–14]. In the former, the same reference data are generated for all tampering rates without considering image content. In [8], reference data are generated by sampling pixel data of several image blocks using a compressive sensing algorithm. By contrast, in adaptive schemes, one or more types of reference data are generated by considering different recovery profiles. For example, image blocks are classified, and different reference data are generated for each class [12–14]. In [14], an image block is categorized into three profiles based on the texture characteristics of pixels. Low-rate reference data are generated for smooth blocks, whereas higher rate data are generated for complex blocks. For

This is an Open Access article distributed under the term of Korea Open Government License (KOGL) Type 4: Source Indication + Commercial Use Prohibition + Change Prohibition (http://www.kogl.or.kr/info/licenseTypeEn.do).
1225-6463/$ © 2020 ETRI

this purpose, the discrete-cosine-transform (DCT) coefficients of each block are quantized according to the defined profiles. The generated reference data and the corresponding quality descriptors are error-protected against tampering.

Region-based self-recovery is an adaptive method because it uses different reconstruction profiles for the region of interest (ROI) and the region of non-interest (RONI). Generally, some regions or objects in an image are more important. In region-based self-recovery methods, higher quality recovery is performed for the ROI. Some methods are only focused on ROI recovery and use the RONI for data embedding [15–18]. Tsai and others [16] proposed a region-based method that only provides ROI recovery. In this method, fractal encoding is performed on the ROI, and the generated code is embedded into the main image using least-significant-bit (LSB) substitution. In [17], the image is segmented into two regions: ROI and region of embedding (ROE). The ROI is compressed to produce 66 bits of reference data, which are embedded into six ROE blocks in the DCT domain. The method does not provide RONI-content recovery; however, other methods allow tampered-image recovery for both the ROI and RONI [19].

For robust recovery, channel-coding algorithms are used for reference-data generation, which is also applicable to adaptive self-recovery methods [20–23]. Korus and others [20] partitioned the original image into blocks of 8 pixels × 8 pixels for DCT. For reference-data generation, the coefficients are quantized and protected. Furthermore, a hash-based method is used for producing authentication data. Although the watermarked image can resist tampering rates of up to 50%, higher rates are not tolerable. Sarreshtedari and others [22] improved the source-channel coding technique by using two well-performing algorithms: set partitioning in hierarchical trees (SPIHT) for source coding and Reed-Solomon (RS) for channel coding. The generated reference and authentication data are embedded into two LSBs of the image. The main drawback of the source-channel coding self-recovery scheme [20,22] is the maximal tampering limit (MTL) problem: either the recovered image has high reconstruction quality (for low tampering rates), or the image is not recoverable. The MTL value is determined according to the amount of generated redundancy data with respect to the reference data. In [24,25], we proposed a solution for the MTL problem (termed scalable self-recovery). In the present study, this method is improved for region-based recovery.

In this paper, a region-based scalable self-recovery (RSS) method is proposed. It is aimed at 1) providing higher ROI-reconstruction quality, and 2) solving the MTL problem using scalable self-recovery. The proposed approach separates the image into two regions (ROI and RONI) according to a user-defined ROI mask. Subsequently, by using the embedded zero-block coding (EZBC) algorithm, these regions are compressed at different data rates. The higher data rate is assigned to the ROI so that higher reconstruction quality may be achieved. To extend the tampering limit, the compressed bitstreams corresponding to the ROI and RONI are partitioned into three unequal parts. For scalable self-recovery, each part is protected based on its importance by using the RS algorithm. Thus, higher tampering rates can be handled by allocating a higher redundancy rate to the most important part. Moreover, the highest reconstruction quality is achieved for low tampering rates. The main advantages of the proposed method are as follows:

- Region-based recovery in the source-channel scheme: In source-channel coding approaches [20,22], the reference data are generated using compression and error-protection algorithms. In this study, separate reference data are generated for the ROI and RONI using the source-channel scheme.
- Multi-scale performance for both ROI and RONI reference data: The proposed method provides three levels of reconstruction quality and MTL.
- Region-based image compression: The proposed method takes advantage of EZBC, a block-based, random access, source-coding algorithm. Random access allows encoding only a region of the image and ignoring the rest.
- Object-based recovery: There are several algorithms for detecting salient objects in an image. By using these methods, the ROI can be segmented automatically. In this study, the proposed scheme is designed based on the MSRA database containing 10 000 salient-object images.

The remainder of the paper is organized as follows. In Section 2, the proposed RSS embedding process is described. Tamper detection and recovery are described in Section 3. In Section 4, the related parameters are designed, and in Section 5, the experimental results are discussed. Finally, Section 6 concludes the paper.

2 | EMBEDDING PROCESS

Figure 1 shows the block diagram of the embedding process in the proposed RSS scheme. It consists of three steps: authentication-data generation, reference-data generation, and data embedding. To generate authentication data, the image is partitioned into nonoverlapping blocks. Subsequently, the significant bits of the pixels in each block, the block number, and a security key are used to generate hash data through the MD5 function (see Subsection 2.1). To generate reference data, as explained in Subsection 2.2, the image is segmented into the ROI and RONI based on a predefined ROI mask. Both segmented regions are compressed using the EZBC source-coding algorithm. To achieve higher reconstruction quality for the ROI, the corresponding compressed bitstream has higher rate, and a lower rate is assigned to the RONI for payload management.

For scalable self-recovery, both compressed bitstreams are partitioned into three unequal parts, and each part is

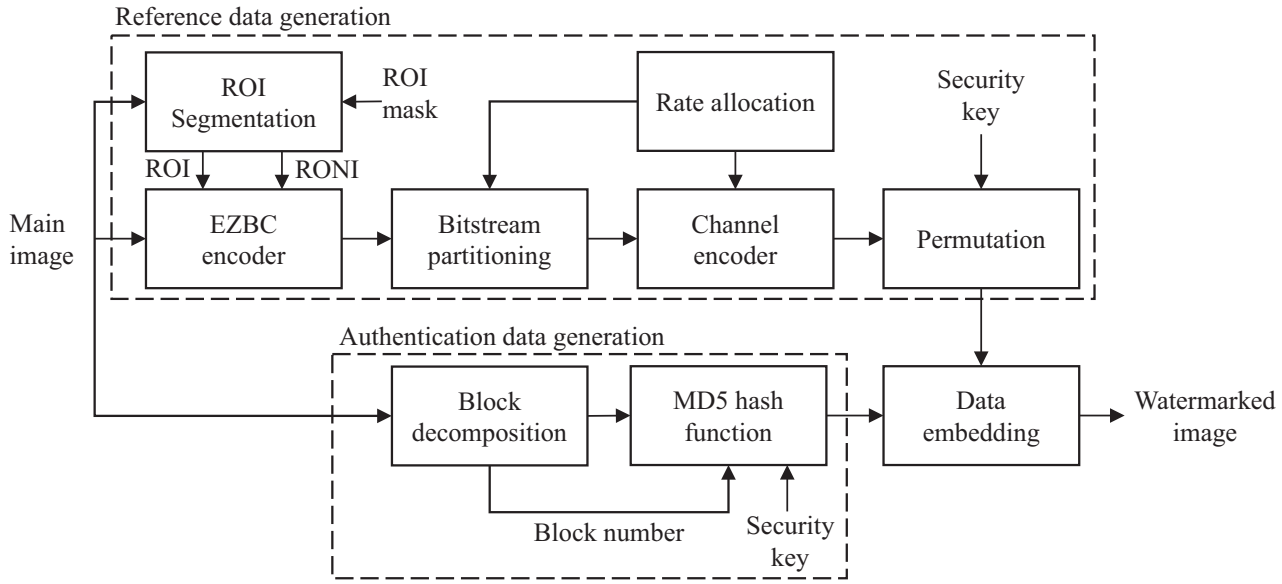

FIGURE 1 Block diagram of embedding process in the proposed RSS method.

separately protected by the RS channel-coding algorithms. Finally, the generated ROI and RONI reference data are permuted before data embedding to ensure security. For data embedding, as explained in Subsection 2.3, the generated authentication and reference data (for both the ROI and RONI) are placed at two or three LSBs of the image pixels.

2.1 | Authentication-data generation

In this section, we describe the authentication-data generation for each block. The purpose of authentication-data generation is tamper detection. Specifically, a highly accurate and secure hash-based method is proposed to detect all tamper types. In this method, as seen in Figure 1, the image is separated into blocks of 8 pixels × 8 pixels, and a security key and the block number are concatenated to the most significant bits (MSB) of the pixels in each block; thereby, input data are provided to the MD5 function, as follows:

$$\text{Hash Data} = \text{MD5}\,(\text{MSBs} \,\|\text{Block Number}\|\, \text{Security Key})\,. \tag{1}$$

In this equation, ‖ denotes the concatenation operator. The block number and the security key are used to prevent vector quantization and collage attacks, respectively [8,14,20,22]. Therefore, any type of image forgery, including block replacement, is detectable by this method. In (1), the block number is in its 16-bit binary representation. Moreover, the security key is a 20-bit pseudo-random binary sequence that is known on the receiver side. The MD5 hash function generates 128-bit data, which are excessively large. The generated hash data are truncated to 32 bits to generate the authentication data. By generating 32 bits for every 64 pixels, the authentication-data rate is 0.5 bits per pixel (bpp).

2.2 | Reference-data generation

As seen in Figure 1, the procedure of reference data generation consists of five steps: ROI segmentation, EZBC source coding, bitstream partitioning, channel encoding, and rate allocation. This procedure starts with segmenting the image so that ROI and RONI reference images are obtained according to the user-defined ROI mask. The EZBC algorithm is used to compress these reference images. As the proposed RSS method is aimed at achieving higher reconstruction quality for the ROI, a higher rate is assigned to the ROI compressed bitstream. The rate allocation unit defines partitioning rates for separating the compressed bitstream into three parts. According to the assigned redundancy rates, every part of each compressed bitstream is protected to provide scalable recovery. The details of these steps are discussed below.

- **ROI Segmentation:** To generate two types of reference data for each region, the image is first segmented into ROI and RONI reference images. For this purpose, a predefined ROI mask is applied to the main image. Figure 2 shows the procedure of manually segmenting the ROI. The ROI mask is a binary ground truth that determines the ROI and RONI. In several applications, such as medical images, the ROI mask need only be defined once for all images of the same type. In this study, the proposed method is designed for images with salient objects. In each of these images, there is an object that is segmented as the ROI. For example, in Figure 2, Lena is a salient object, which is labeled as the ROI, and the background is the RONI. We use a learning-based algorithm to extract salient objects from the background [26]. ROI segmentation is manually performed by setting all the RONI pixels to zero.

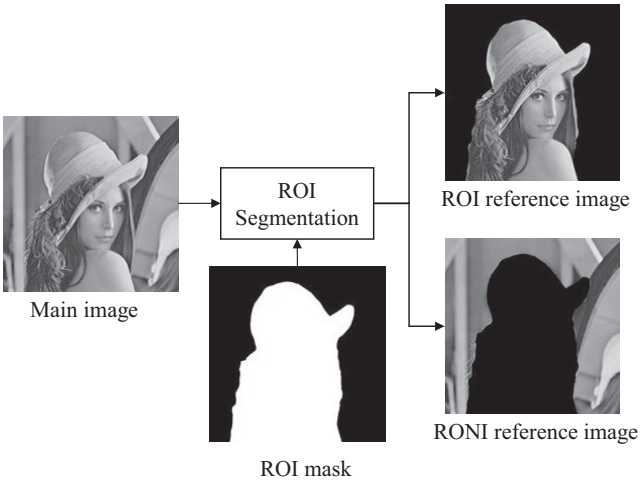

FIGURE 2 ROI segmentation using the ROI mask.

- **EZBC source coding:** Modern wavelet-based compression algorithms use two common structures: one is zero tree, which is used in Embedded Zero-tree Wavelet [27] and SPIHT [28], and the other is zero block, which is used in EZBC [29] and the JPEG2000 standard. EZBC is an iterative algorithm based on the quadtree structure and uses significant testing. In this algorithm, if all coefficients of a block are insignificant, the entire block will be regarded as a zero block that will be encoded with only one bit (zero). By contrast, if the block is significant, it is separated into four subblocks to form a quadtree. Significant testing is applied to the subblocks through zigzag scanning, and this procedure is continued until the quadtree cannot be further split and all the coefficients are encoded. For region-based compression, the ROI and RONI reference images are encoded separately. Therefore, two compressed bitstreams are generated. The ROI bitstream is used to recover the ROI and has higher data rate to achieve higher reconstruction quality.
- **Bitstream partitioning and rate allocation:** Figure 3 shows the rate allocation process of the proposed RSS method. Two rate types are assigned to every partition of each bitstream: partition rate (R^{p}) for bitstream partitioning, and redundancy rate (R^{r}) for error protection. The first part receives the highest redundancy rate (leading to the highest protection), whereas the third part receives the lowest. To manage data payload, the first part receives the lowest partition rate, whereas the highest rate is assigned to the third part with the least redundancy rate.

The rate allocation procedure is individually applied to the ROI and RONI reference data. The user defines the total partition rate and the total redundancy rate. For this purpose, we assume that a typical $R_{\mathrm{T}}^{\mathrm{p}}$ (bpp) compressed bitstream is partitioned into three parts according to the partition rates (R_i^{p}, $i = 1, 2, 3$) as follows:

$$R_{\mathrm{T}}^{\mathrm{p}} = \sum_{i=1}^{3} R_i^{\mathrm{p}}. \tag{2}$$

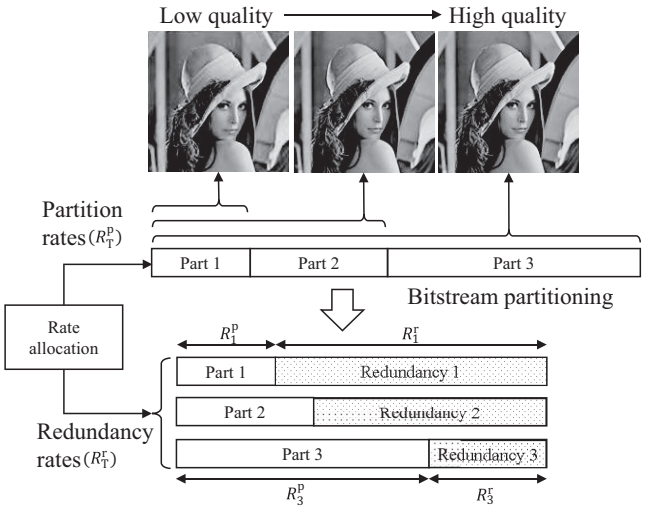

FIGURE 3 Bitstream partitioning and rate allocation.

In this equation, R_i^{p} is the rate of part i. The partition rates define the share of each part in bitstream partitioning. The compressed bitstream is partitioned into three parts with R_1^{p}, R_2^{p}, and R_3^{p} bpp. To obtain an invariant procedure, the partition rates are chosen as follows:

$$\begin{aligned} R_1^{\mathrm{p}} &= 0.2 \times R_{\mathrm{T}}^{\mathrm{p}}, \\ R_2^{\mathrm{p}} &= 0.3 \times R_{\mathrm{T}}^{\mathrm{p}}, \\ R_3^{\mathrm{p}} &= 0.5 \times R_{\mathrm{T}}^{\mathrm{p}}. \end{aligned} \tag{3}$$

The constants in (3) are determined empirically. Depending on the application, these numbers can be changed provided that they satisfy (2). Every part is protected using a channel-coding algorithm based on the assigned redundancy rate (R_i^{r}, $i = 1, 2, 3$). To manage data payload, the sum of all redundancy rates must be equal to the user-defined total redundancy rate:

$$R_{\mathrm{T}}^{\mathrm{r}} = \sum_{i=1}^{3} R_i^{\mathrm{r}}. \tag{4}$$

As in (3), the following rules are considered for allocating redundancy rates:

$$\begin{aligned} R_1^{\mathrm{r}} &= 0.45 \times R_{\mathrm{T}}^{r}, \\ R_2^{\mathrm{r}} &= 0.30 \times R_{\mathrm{T}}^{r}, \\ R_3^{\mathrm{r}} &= 0.25 \times R_{\mathrm{T}}^{r}. \end{aligned} \tag{5}$$

It should be noticed that the fixed coefficients in (5) are selected empirically and can be adjusted provided that (4) is satisfied. The partition and redundancy rates of part i are defined as

$$R_i^{\mathrm{p}} = \frac{k_i}{w \times l}, R_i^{\mathrm{r}} = \frac{n_i - k_i}{w \times l}; i = 1,\ 2,\ 3. \tag{6}$$

In this equation, k_i is the number of bits in the partition i, n_i is the number of bits of the error-protected part, and $w \times l$ is the image dimension. R_i^{p} and R_i^{r} are the partition and redundancy rates in bpp, respectively. It should be noted that the allocated rates should satisfy (7).

$$\sum_{i=1}^{3} R_i^{\mathrm{p}} + R_i^{\mathrm{r}} = R_{\mathrm{T}}^{\mathrm{p}} + R_{\mathrm{T}}^{\mathrm{p}} = C_{\mathrm{w}}. \tag{7}$$

In this equation, C_{w} is the dedicated capacity of the watermarking system for reference data (in bpp). Each partition provides a quality scale, which is limited for tampering rates below the MTL. The theoretical calculation of the MTL for each scale is as follows:

$$\lambda_i = \frac{n_i - k_i}{n_i} = \frac{R_i^{\mathrm{r}}}{R_i^{\mathrm{p}} + R_i^{\mathrm{r}}}. \tag{8}$$

In this equation, λ_i is the MTL of the scale i, for all $i = 1$, 2, 3. To modify λ_i, the corresponding partition and redundancy rates should be changed by considering (2) and (4).

- **RS channel coding:** Recently, image tampering has been modeled as an erasure channel [14,20,22]. Accordingly, the embedded watermark in an image is modeled as a passing message through the communication channel. Tampering is modeled as erasure because the extracted reference data from the tampered blocks are not authentic. One of the best-performing algorithms based in this model is the RS algorithm over large Galva fields and encoding blocks [22].

According to the allocated partition and redundancy rate for part i (i = 1, 2, 3), each bitstream part for both the ROI and RONI reference data is protected against tampering. The RS error-protection algorithm receives k_i bits of input data and produces n_i bits of output data by generating $n_i - k_i$ bits of redundancy data, as in (6). In this study, RS (n_i, k_i) is used with 16-bit symbols, and puncturing is used to encode any arbitrary redundancy rate.

- **Permutation:** In this step, the generated ROI and RONI reference data are scrambled randomly. This permutation has two benefits: 1) It increases the security of the ROI and RONI reference data by preventing their being changed. 2) It distributes these reference data uniformly among all image blocks. Therefore, if the ROI is completely tampered, some parts of the ROI reference data remain in authentic blocks, and they participate in ROI recovery.

2.3 | Data embedding

In this paper, two RSS(2-LSB) and RSS(3-LSB) scenarios are proposed based on embedding into two and three LSBs of the image, respectively. The significant bits are not used for watermarking and are kept unchanged. As mentioned previously, two types of data are generated: authentication and reference data. The former is generated for each block and are embedded into the same block. The latter are generated for the entire image but are shared between all blocks.

3 | TAMPER DETECTION AND IMAGE RECOVERY

Figure 4 shows the block diagram of tamper detection and image recovery in the proposed RSS method. For tamper detection, the test image is separated into blocks of 8 pixels × 8 pixels, and authentication data are generated for every block, as described Section 2.1. That is, the MSBs of pixels in the block, the block number, and the security key are concatenated to generate hash code using the MD5 function. The hash code is truncated to 32 bits to generate authentication

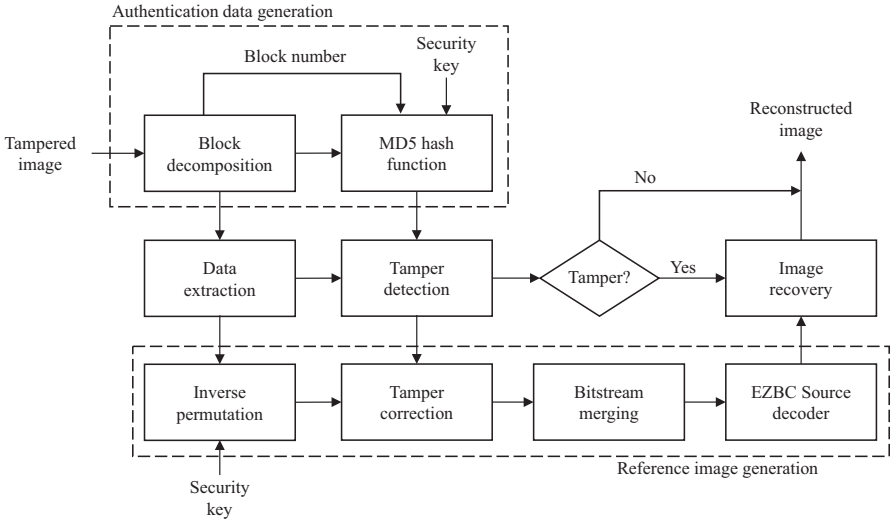

FIGURE 4 Block diagram of tamper detection and image recovery in the proposed RSS method.

TABLE 1 Designed parameters of the proposed RSS approach

Scenario	Authentication Data (bpp)	Total reference data (bpp)	Reference types	Reference data (bpp)	Partition rate:R_T^p (bpp)	Redundancy rate:R_T^r (bpp)	Partition rates (bpp)			Redundancy rates (bpp)		
							R_1^p	R_2^p	R_3^p	R_1^r	R_2^r	R_3^r
RSS (2-LSB)	0.5	1.5	ROI (80%)	1.2	0.8	0.4	0.16	0.24	0.4	0.18	0.12	0.1
			RONI (20%)	0.3	0.2	0.1	0.04	0.06	0.1	0.045	0.03	0.025
RSS (3-LSB)	0.5	2.5	ROI (80%)	2	1	1	0.2	0.3	0.5	0.45	0.3	0.25
			RONI (20%)	0.5	0.25	0.25	0.05	0.075	0.125	0.113	0.075	0.062

data. In a tampered block, the generated and the extracted authentication data are different, but they are the same if the block is authentic. Thus, the tampered block is detected by comparing the generated and the extracted authentication data. The tamper detection method used in this study is sufficiently accurate to detect all types of image forgery. Even by changing a pixel bit in the block, the entire block becomes unauthorized.

The extracted reference data from authentic blocks (not tampered) are used for image recovery. For this purpose, in the inverse permutation step, the data are first rearranged to the correct orders. We note that by using a permutation, even if the ROI is completely tampered, its embedded reference data are not entirely erased, and the ROI is recoverable. Subsequently, the erased symbols of the reference data are error-corrected using the RS channel decoder. Both the ROI and RONI reference data consist of three parts that provide three scales of self-recovery. Based on the amount of redundancy, each part provides different levels of tamper tolerability. The first part of the reference data (both ROI and RONI) tolerates the most, and the last part the least. The error-corrected parts of the ROI and RONI reference data are merged to generate compressed bitstreams, which are decompressed by the EZBC source decoder to generate the ROI and RONI reference images. We note that the ROI mask is available on the receiver side. Finally, the tampered regions of the image are replaced by the corresponding regions of the reference images. The ROI reference image is used to reconstruct the ROI, whereas the RONI reference image is used to recover the RONI.

4 | PARAMETER DESIGN

Table 1 presents the designed parameters of the proposed RSS method. Two scenarios are considered, namely RSS(2-LSB) and RSS(3-LSB), based on embedding into the two and three LSBs of the image, respectively. In both scenarios, 0.5 bpp authentication data are generated for tamper detection. Therefore, 1.5 and 2.5 bpp reference data are generated for RSS(2-LSB) and RSS(3-LSB), respectively. In the RSS(2-LSB) scenario, 1 bpp is assigned to the total partition rate $\left(R_T^p\right)$, which is shared between the ROI and RONI reference data.

To achieve higher reconstruction quality for the ROI, 80% of the total partition rate and total redundancy rate $\left(R_T^r\right)$ are allocated to the ROI, and 20% to the RONI. Moreover, a total redundancy rate of 0.5 bpp is assigned under the RSS(2-LSB) scenario: 0.4 bpp to the ROI, and 0.1 bpp to the RONI.

In the RSS(3-LSB) scenario, a total partition rate of 1.25 bpp is assigned as follows: 1 bpp to the ROI and 0.25 bpp to the RONI reference data (80% of 2 bpp is assigned to the ROI, and the other 20% is used for the RONI). Additionally, a

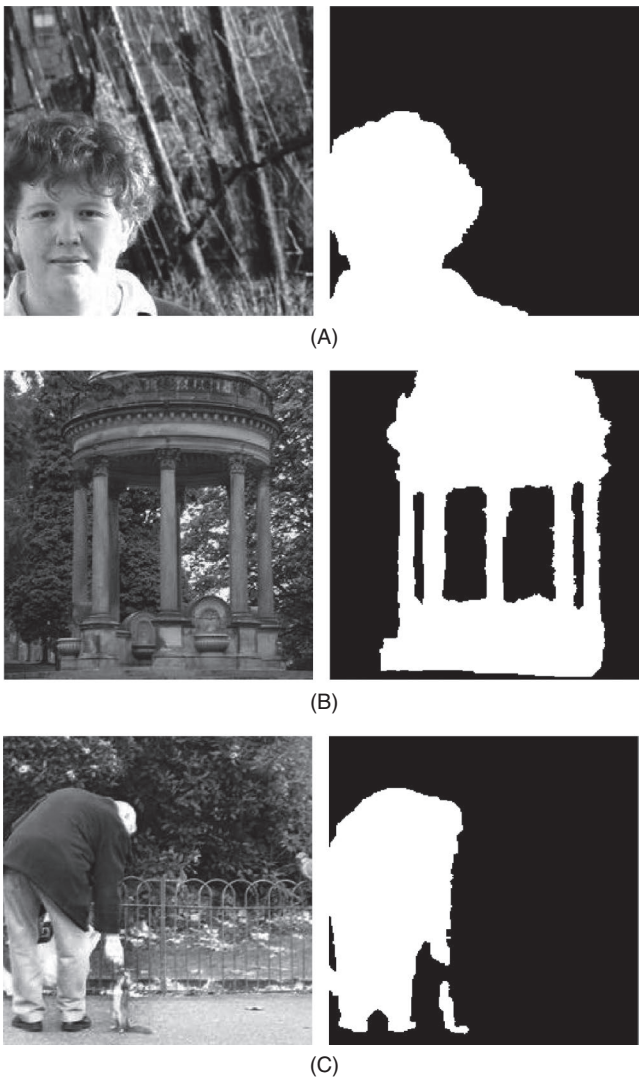

FIGURE 5 Sample images from the MSRA dataset: (A) Image No. 5000, (B) Image No. 1026, and (C) Image No. 4988.

FIGURE 6 Two examples of image tampering and recovery: (A) and (C) tampering 45.28 and 37.54 percent of the protected images in Figure 5 using RSS(2-LSB) and RSS(3-LSB), respectively; (B) and (D) the recovered images of (A) and (C) with reconstruction Peak Signal to Noise Ratio of 25.07 and 27.9 dB, respectively.

TABLE 2 Simulation results of the proposed RSS method for 10 000 test images from MSRA dataset

	Reconstruction quality (PSNR)		
Scenarios	**Scale 1**	**Scale 2**	**Scale 3**
RSS(2-LSB)			
Average of ROI	42.38	34.36	27.97
Variance of ROI	47.9	24.29	15.09
Average of RONI	24.10	22.17	20.14
Variance of RONI	12.31	9.83	7.91
RSS(3-LSB)			
Average of ROI	44.26	34.93	28.07
Variance of ROI	53.93	24.35	15.32
Average of RONI	23.70	21.81	19.72
Variance of RONI	12.77	9.97	7.95

total redundancy rate of 1.25 bpp is assigned to the ROI and RONI: 1 and 0.25 bpp, respectively. Based on (2) and (4), the allocated R_T^p and R_T^r for the ROI and RONI are used for assigning partition and redundancy rates ($R_i^p, R_i^r; i = 1, 2, 3$). According to (6), for the RSS(2-LSB) scenario, the sum of all partition and redundancy rates is equal to 1.5 bpp for both the ROI and RONI. The amount of generated data is completely matched with the capacity of the watermarking system for reference data (C_w). For the RSS(3-LSB) scenario, C_w is 2.5 bpp, which is compatible with the allocated partition and redundancy rates for both the ROI and RONI. According to (7), for the RSS(2-LSB) scenario, the theoretical MTLs are expected to be $\lambda_1 = 0.53$, $\lambda_2 = 0.33$, $\lambda_3 = 0.2$. For RSS(3-LSB), the theoretical MTLs are $\lambda_1 = 0.69$, $\lambda_2 = 0.5$, $\lambda_3 = 0.33$.

For example, in the RSS(2-LSB) embedding scenario shown in Table 1, an image of 256 pixels × 256 pixels provides a 131 072-bit payload for data embedding. The watermarking capacity is divided into two types of data: 0.5 bpp (32 768 bits) for authentication data and 1.5 bpp (98 304 bits) for reference data. The ROI reference data are assigned 1.2 bpp (78 643 bits) of the reference data, and the remaining 0.3 bpp (19 661 bits) is assigned to the RONI data. For the ROI reference data, the bit budget of parts one to three is 10 486, 15 729, and 26 214 bits, respectively. Moreover, the redundancy data are 11 796, 7864, and 6554 bits for parts one to three, respectively. For the RONI reference data, the bit

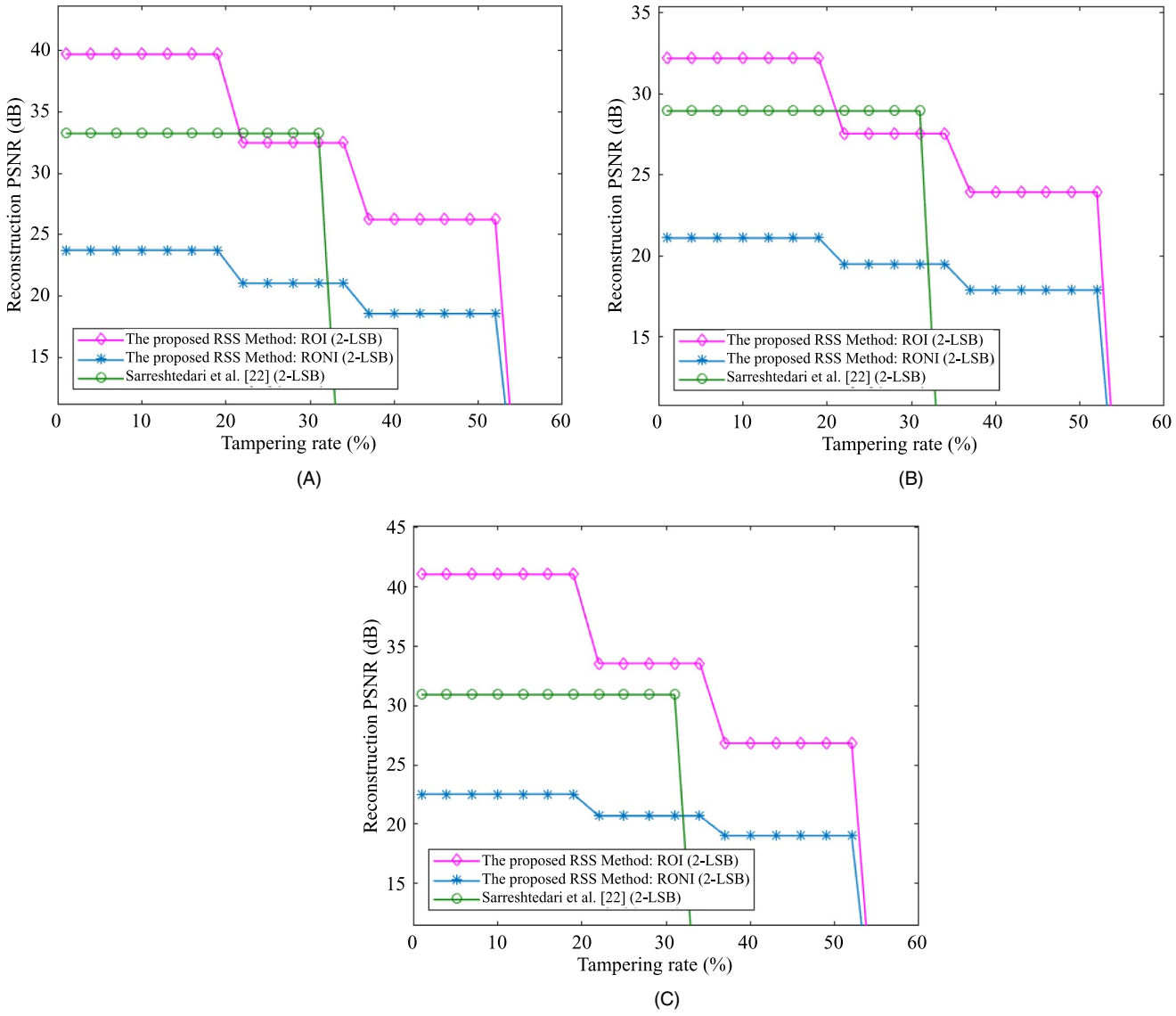

FIGURE 7 Proposed RSS(2-LSB) compared with related methods for several images in the dataset: (A) Image No. 5000, (B) Image No. 1026, and (C) Image No. 4988 [Colour figure can be viewed at wileyonlinelibrary.com]

budget of parts one to three is 2621, 3932, and 6554 bits, respectively. Finally, the redundancy data are 2949, 1967, and 1638 bits for parts one to three, respectively.

5 | EXPERIMENTAL RESULTS

For performance evaluation, we used 10 000 test images from the MSRA database provided by Liu and others [26]. The ROIs of the images are labeled as separate files that can be used as ROI masks. Figure 5 shows sample images of the database. The test images for the proposed RSS method are 8-bit grayscale, with 256 pixels × 256 pixels. For performance evaluation, the reconstruction quality is studied for all tampering rates. According to the proposed region-based scalable method, we expect two performance curves for the ROI and RONI. Moreover, performance should be investigated for both RSS(2-LSB) and RSS(3-LSB) embedding scenarios in comparison with the related methods.

Figure 6 shows two recovery examples by the proposed method used for image forgery detection. In Figure 6A, image No. 5000 of the database is modified. Previously, the original image was protected by the proposed RSS(2-LSB) before tampering. In Figure 6B, the self-recovery algorithm detects a 45.28% tampering rate, and successful recovery is achieved, with a quality of 25.07 dB. Additionally, in Figure 6C, the image No. 1026 is protected using the proposed RSS(3-LSB), and it is modified using a 37.54% tampering rate. The recovered image is shown in Figure 6D, with a quality of 27.9 dB. The ROI masks of Figure 6A and 6C are shown in Figure 5.

The results of the simulation on 10 000 test images from the database are presented in Table 2. The results are

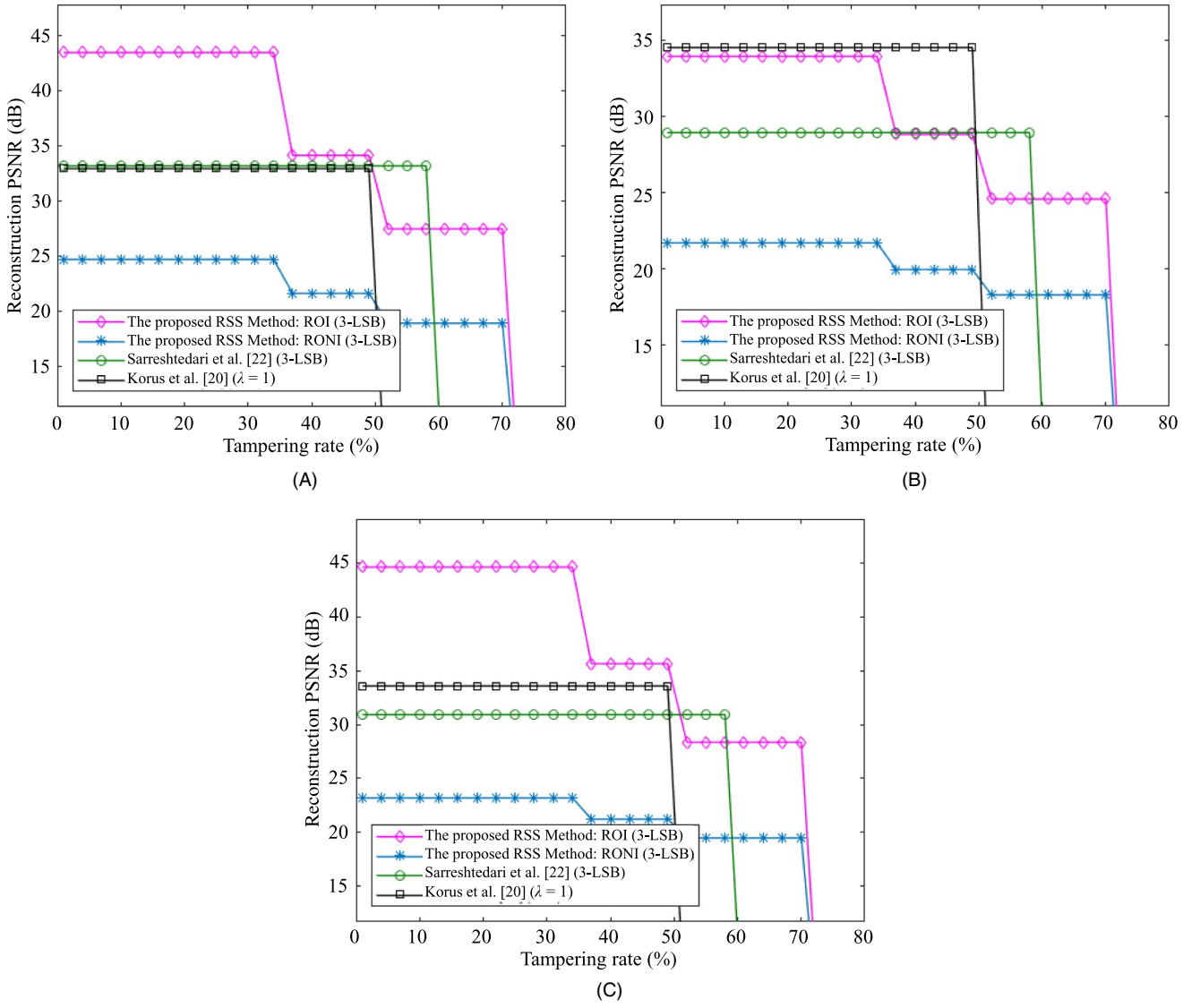

FIGURE 8 Proposed RSS(3-LSB) compared with related methods for several images in the dataset: (A) Image No. 5000, (B) Image No. 1026, and (C) Image No. 4988 [Colour figure can be viewed at wileyonlinelibrary.com]

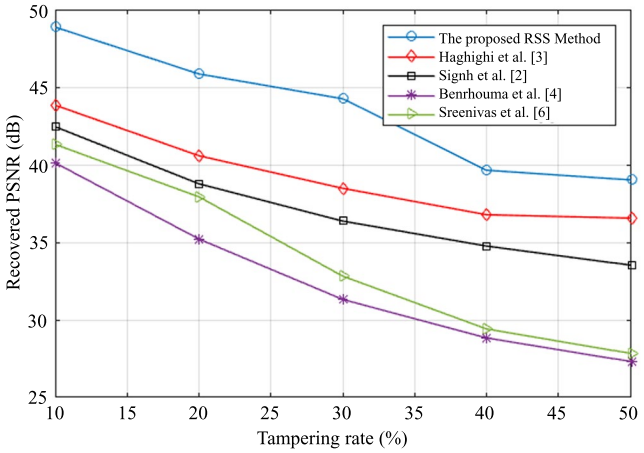

FIGURE 9 Recovered Peak Signal to Noise Ratio by the proposed RSS(2-LSB) compared with that by related methods [Colour figure can be viewed at wileyonlinelibrary.com]

categorized based on the embedding scenarios RSS(2-LSB) and RSS(3-LSB); the average reconstruction quality and variance are shown for three scales (see Section 4). For RSS(2-LSB), scales 1, 2, and 3 correspond to tampering rates from 0% to 20% (λ_1), from 20% to 33% (λ_2), and from 33% to 53% (λ_3), respectively. Moreover, for RSS(3-LSB), scales 1, 2, and 3 correspond to tampering rates from 0% to 33% (λ_1), from 33% to 50% (λ_2), and from 50% to 69% (λ_3). According to Table 2, the highest reconstruction quality is achieved in scale 1 (low tampering rates), and the lowest in scale 3 (high tampering rates). The results clearly indicate that, compared with the RONI, the ROI is recovered by the proposed RSS method with superior quality.

In Figure 7, the performance of the proposed RSS(2-LSB) is compared with the that of the method in [22] for selected test images of Figure 5. Reference [22] presents a similar self-recovery scheme based on conventional source-channel

coding without scalable recovery and ROI. In this method, the image is first compressed using the SPIHT algorithm at a rate of 1 bpp. Then, a redundancy rate of 0.5 bpp is applied by using an RS algorithm. Both the 1.5 bpp reference data and the 0.5 bpp authentication data are embedded into two LSBs of the image. Figure 7 shows higher reconstruction quality for the ROI. Moreover, the proposed method achieved a higher MTL. The MTL value reported in [22] is 33% in the 2-LSB embedding scenario. The proposed RSS(2-LSB) method improved the tampering limit to 53% by using the proposed scalable recovery approach.

In Figure 8, similar results are presented for the proposed RSS(3-LSB) scenario, compared with two related methods in [20,22]. In [22], 1 bpp was used for source coding, and a 1.5 bpp redundancy rate was assigned to the entire compressed bitstream. As mentioned previously, the proposed RSS method uses the scalability of the compressed bitstream. Additionally, the proposed algorithm achieves higher reconstruction quality for the ROI. The method in [20] uses quantized DCT coefficients and a channel-coding algorithm. In [20], two architectures were introduced based on two values of the channel coding parameter: $\lambda = 1$ and $\lambda = 2$. The first design can tolerate a 50% tampering rate, whereas the second can tolerate 33%. Higher restoration quality is achieved in the second design. The first scheme is more comparable with the proposed RSS(3-LSB) in that it handles higher tampering rates. The results imply that the proposed RSS(3-LSB) is preferable.

Figure 9 shows a comparison of the proposed method with several state-of-the-art self-recovery methods. The standard Cameraman image is tampered at various percentages, and the quality of the recovered image is calculated. For the proposed method, the ROI is a square block with 20% of the image placed at the center. The results by the related methods were obtained from [3–6]. It can be seen that the proposed method performs better than the others for all tampering rates.

6 | CONCLUSION

In this paper, a novel RSS method was proposed for image tamper detection and recovery. In the proposed method, two types of data are embedded in the main image: authentication data for tamper detection and reference data for image recovery. Two embedding scenarios were proposed: RSS(2-LSB) and RSS(3-LSB). For both scenarios, 0.5 bpp authentication data were produced by a block-based algorithm using the MD5 hash function. Two types of reference data at different rates are generated for the ROI and RONI. Eighty percent of the embedding capacity is assigned to the ROI reference data so that the ROI may be recovered with superior reconstruction quality. To generate the reference data, the image is manually segmented into the ROI and RONI images using a salient-object ground truth. Subsequently, both the ROI and RONI images are compressed by the region-based EZBC source-coding algorithm. The resulting compressed bitstream is partitioned into three parts. Finally, each part is protected by the RS channel-coding algorithm. For scalable recovery, a higher redundancy rate (higher protection) is considered for the most important part. Therefore, the first part, which is critical for decoding the other part, is highly protected, whereas other parts are less protected. The proposed method has certain advantages compared with previous self-recovery methods: (a) The proposed region-based scenario is employed in the state-of-the-art source-channel coding scheme to achieve higher reconstruction quality for the ROI. (b) A scalable recovery technique is proposed for extending the tampering limit and providing multilevel recovery. (c) The proposed rate allocation algorithm is user-adjustable. (d) The proposed RSS self-recovery method was evaluated using 10 000 salient-object images from the MRSA database. The simulation results demonstrated that scalability combined with the region-based approach yield a highly effective method with improved self-recovery performance in comparison with related methods.

ORCID

Navid Daneshmandpour https://orcid.org/0000-0003-1746-0970

REFERENCES

1. W.-L. L. Tai and Z.-J. J. Liao, *Image self-recovery with watermark self-embedding*, Signal Process. Image Commun. **65** (2018), 11–25.
2. D. Singh and S. K. Singh, *DCT based efficient fragile watermarking scheme for image authentication and restoration*, Multimed. Tools Applicat. **76** (2017), no. 1, 953–977.
3. B. B. Haghighi, A. H. Taherinia, and A. H. Mohajerzadeh, *TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with quality optimized using LWT and GA*, Inf. Sci. **486** (2018), 204–230.
4. O. Benrhouma, H. Hermassi, and S. Belghith, *Security analysis and improvement of an active watermarking system for image tampering detection using a self-recovery scheme*, Multimed. Tools Applicat. **76** (2017), no. 20, 21133–21156.
5. D. Singh and S. K. Singh, *Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability*, J. Vis. Commun. Image Represent. **38** (2016), 775–789.
6. K. Sreenivas and V. Kamakshiprasad, *Improved image tamper localisation using chaotic maps and self-recovery*, J. Vis. Commun. Image Represent. **49** (2017), 164–176.
7. X. Zhang et al., *Reference sharing mechanism for watermark self-embedding*, IEEE Trans. Image Process. **20** (2011), no. 2, 485–495.
8. X. Zhang et al., *Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction*, IEEE Trans. Inf. Forensics Secur. **6** (2011), no. 4, 1223–1232.
9. X. Zhang et al., *Self-embedding watermark with flexible restoration quality*, Multimed. Tools Applicat. **54** (2011), no. 2, 385–395.

10. Z. Qian et al., *Image self-embedding with high-quality restoration capability*, Digit. Signal Process. **21** (2011), no. 2, 278–286.
11. Y. Huo, H. He, and F. Chen, *Alterable-capacity fragile watermarking scheme with restoration capability*, Opt. Commun. **285** (2012), no. 7, 1759–1766.
12. C. Qin, C.-C. Chang, and K.-N. Chen, *Adaptive self-recovery for tampered images based on VQ indexing and inpainting*, Signal Process. **93** (2013), no. 4, 933–946.
13. C. Qin, C.-C. Chang, and P.-Y. Chen, *Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism*, Signal Process. **92** (2012), no. 4, 1137–1150.
14. P. Korus and A. Dziech, *Adaptive self-embedding scheme with controlled reconstruction performance*, IEEE Trans. Inf. Forensics Secur. **9** (2014), no. 2, 169–181.
15. J. M. Zain and A. R. M. Fauzi, *Medical image watermarking with tamper detection and recovery*, in Proc. Int. Conf. IEEE Eng. Med. Biol. Soc. (New York, USA), Aug. 2006, pp. 3270–3273.
16. S. Wang and S. Tsai, *Automatic image authentication and recovery using fractal code embedding and image inpainting*, Pattern Recognit. **41** (2008), no. 2, 701–712.
17. C. Cruz-Ramos et al., *Image authentication scheme based on self-embedding watermarking*, in Proc. Iberoamer. Congr. Pattern Recognit. (Guadalajara, Mexico), Nov. 2009, pp. 1005–1012.
18. K.-S. Kim et al., *Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging*, Comput. Vis. Image Underst. **115** (2011), no. 9, 1308–1323.
19. R. Eswaraiah and E. S. Reddy, *Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI*, Int. J. Telemed. Appl. **2014** (2014), 1–10.
20. P. Korus and A. Dziech, *Efficient method for content reconstruction with self-embedding*, IEEE Trans. Image Process. **22** (2013), no. 3, 1134–1147.
21. P. Korus, J. Bialas, and A. Dziech, *Towards practical self-embedding for JPEG-compressed digital images*, IEEE Trans. Multimed. **17** (2015), no. 2, 157–170.
22. S. Sarreshtedari and M. A. Akhaee, *A source-channel coding approach to digital image protection and self-recovery*, IEEE Trans. Image Process. **24** (2015), no. 7, 2266–2277.
23. S. Sarreshtedari, A. Abbasfar, and M. Ali, *A joint source – channel coding approach to digital image self-recovery*, Signal Image Video Process. **11** (2017), no. 7, 1371–1378.
24. N. Daneshmandpour, H. Danyali, and M. S. Helfroush, *Scalable image self-embedding based on dual-rate SPIHT-LDPC reference generation scheme*, Radioeng. **28** (2019), no. 1, 199–206.
25. N. Daneshmandpour, H. Danyali, and M. S. Helfroush, *Multi-rate reference embedding for highly-scalable self-recovery using fuzzy mamdani*, J. Intell. Fuzzy Syst. **37** (2019), no. 6, 1–11.
26. T. Liu et al., *Learning to detect a salient object*, IEEE Trans. Pattern Anal. Mach. Intell. **33** (2011), no. 2, 353–367.
27. A. Said and W. Pearlman, *A new, fast, and efficient image codec based on set partitioning in hierarchical trees*, IEEE Trans. Circuits Syst. Video Technol. **6** (1996), no. 3, 243–250.
28. J. Shapiro, *Embedded image coding using zerotrees of wavelet coefficients*, IEEE Trans. Signal Process. **41** (1993), no. 12, 3445–3462.
29. S. T. Hsiang, *Embedded image coding using zeroblocks of subband/wavelet coefficients and context modeling*, in Proc. DCC 2001. Data Comp. Conf. IEEE Comput. Soc. (Snowbird, UT, USA), Mar. 2001, pp. 83–92.

AUTHOR BIOGRAPHIES

Navid Daneshmandpour received his BSc and MSc degrees in Electrical Engineering from Azad University, Isfahan, Iran, in 2009 and 2011, respectively. In 2019, he received his PhD in Electrical and Telecommunication Engineering from Shiraz University of Technology, Shiraz, Iran. His research interests include digital watermarking, image retrieval, and image/video coding.

Habibollah Danyali received his BSc and MSc degrees in Electrical Engineering from Isfahan University of Technology, Isfahan, Iran, in 1991, and Tarbiat Modarres University, Tehran, Iran, in 1993, respectively. From 1994 to 2000, he was with the Department of Electrical Engineering, University of Kurdistan, Sanandaj, Iran, as a lecturer. In 2004, he received his PhD in Computer Engineering from University of Wollongong, Australia. He is currently working as an associate professor with the Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran. His research interests include data hiding, medical image processing, scalable image and video coding, and biometrics.

Mohammad Sadegh Helfroush received his BS and MS degrees in Electrical Engineering from Shiraz University of Technology, Shiraz in 1993, and Sharif University of Technology, Tehran in 1995, respectively. He received his PhD in Electrical Engineering from Tarbiat Modares University, Tehran, Iran. He is working as an associate professor in the department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran. His research interests include content-based image retrieval, pattern recognition, and medical image processing.