Scalable Image Self-Embedding Based on Dual-Rate SPIHT-LDPC Reference Generation Scheme

Navid DANESHMANDPOUR, Habibollah DANYALI, Mohammad Sadegh HELFROUSH

Dept. of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran

{n.daneshmand, danyali, ms_helfroush}@sutech.ac.ir

Submitted February 16, 2018 / Accepted November 12, 2018

Abstract. *Image Self-Embedding is a method of embedding two sets of data into the original image, authentication data for tamper detection and reference data for image recovery. In this paper, a scalable self-embedding method is proposed based on dual-rate source-channel coding for reference data generation. The proposed method uses Set Partitioning in Hierarchical Tree (SPIHT) algorithm for source coding and Low-Density Parity Check (LDPC) for channel coding. Accordingly, the proposed recovery system provides higher reconstruction quality at low tampering rates, while it can handle higher tampering rates with less reconstruction quality. Therefore, the proposed method has the ability of both preserving the image quality and recovering higher tampering rates. Simulation results show noticeable improvements compared with the related self-embedding methods in the literature.*

Keywords

Tamper detection, image recovery, self-embedding, source-channel coding, SPIHT, LDPC

1. Introduction

Nowadays, by developing the internet and social networks, image authentication is a very crucial issue as a result of information explosion [1–4]. Moreover, modern image manipulation software, like Photoshop, operating in powerful computers facilitate the image forgery [5–9].

Passive authentication is a fundamental method for detecting counterfeit images without having any information about the original image. Thus, pixels statistics and learning based algorithms are served for detecting tampered regions [1], [2], [10]. On the other hand, in active authentication schemes, prior information of the original image are used for tamper detection [11], [12]. A digital signature is a simple method for investigating the integrity of the image [13]. In this method, hash function generates a unique code for the image. For forgery detection, another signature is produced based on the test image. The image is labeled authentic if the received code matches the generated one. Digital watermarking is widely used for image authentication [14–17]. The methods based on fragile watermarking detect every little modification of the image [16–18], while semi-fragile watermarking authorizes some image modifications like compression [8], [20]. In [21], an authentication method is proposed based on both statistical correlation and digital watermarking. For generating authentication data in the fragile watermarking scheme, the digital signature techniques are very helpful [9], [10]. In this scheme, the image is partitioned into non-overlapping blocks and the digital signature is generated for each block using a hash function, embedding into the same block. For tamper detection, the extracted data is compared with the generated one and in the case of mismatches, the block is labeled as tampered [22].

Self-embedding is a tamper detection and image recovery algorithm based on digital watermarking. Two types of data are embedded into the original image, authentication data for tamper detection and reference data for image recovery [23]. Fridrich et al. introduced a self-embedding method based on fragile watermarking, not only for tamper detection but also for image recovery [24]. A three-level authentication system based on fragile image watermarking was proposed by Lin et al. [25]. In this method, parity check bits were generated as authentication data and the average of the block utilized as reference data. The proposed dual-watermarking scheme by Lee and Lin [14] compensates the drawback of the previous scheme in [25]. In this method, two reference data are generated for every block in order to provide higher tamper resilience. Since high reference payload was the main disadvantage of the proposed method in [14], Zhang et al. proposed a flexible self-embedding scheme based on compressive sensing for reducing data redundancy [26]. In this scheme, the reference data is generated for several blocks in DCT domain. By using image compression, the reference data is generated more efficient and the image can be recovered with higher reconstruction quality. Yang and Shen proposed a tamper recovery method based on vector quantization (VQ) [27]. In this method, the indices of the blocks were embedded into the main image using fragile watermarking. Korus et al. [23] proposed a fragile watermarking scheme for tamper recovery based on quantization and channel coding. In this scheme, the image is partitioned into non-overlapping blocks and each block is transformed

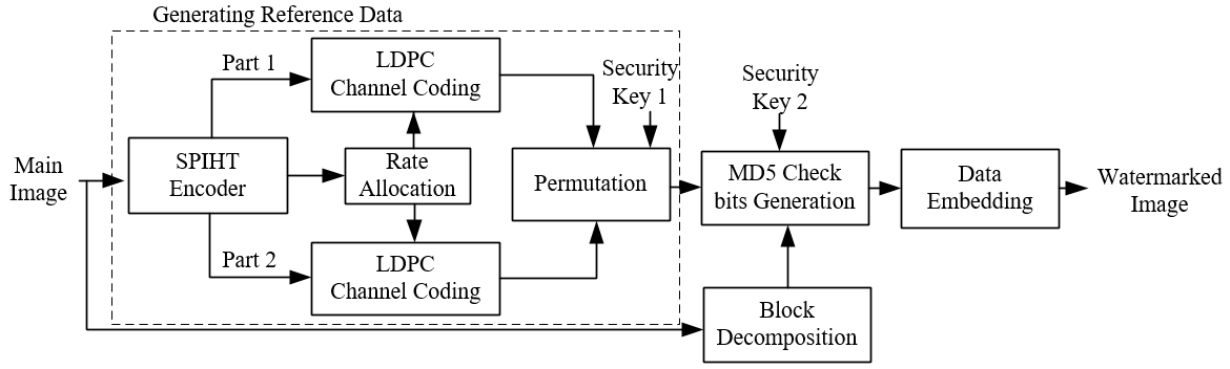


Fig. 1. The block diagram of embedding process of the proposed method.

to DCT domain. The DC coefficients are quantized using scalar quantization and AC coefficients are quantized by using VQ. For the first time, Lee et al. introduced a tamper recovery scheme based on channel coding algorithms [28]. Since the generated reference data is hidden in the image, tampers might affect the embedded data. Channel coding is an effective method to ensure better error resiliency for the reference data. Sarreshtedari et al. [29] proposed a source-channel coding self-embedding scheme based on SPIHT and Reed-Solomon (RS) algorithms. In this method, the image is compressed at 1 bit per pixel (bpp) data rate and 0.5 bpp redundancy is added to the compressed data for error protection. The generated reference data is permuted and embedded into the original image. Qin et al. proposed an overlapping-block embedding strategy which provides block-based tamper detection and content recovery [30]. In this method, check bits are generated according to the complexity of each block. For tamper recovery, the average value of the overlapping blocks is used for generating reference data.

In this paper, a scalable self-embedding method is proposed based on a dual-rate source-channel coding. The main contribution of this scheme is generating reference data consisting of two data parts. The first part is well protected to be prepared for high tampering rates and the second part is suitable for low tampering rates for providing higher reconstruction quality. The reference data is produced using SPIHT for image compression and LDPC algorithms for error protection. The compressed SPIHT bitstream is partitioned into two parts. The first part provides fundamental quality for content recovery, and therefore protected with higher redundancy rate. However, the second part consists in enhancement information and can be protected by less redundancy rate. For tamper detection at the receiver side, the image is partitioned into non-overlapping blocks and the authentication data is extracted to detect the modifications of the block. For image recovery, the extracted reference data is partitioned into two parts according to the embedding procedure. After inverse permutation, each part is error-corrected individually. The bitstream is decompressed to generate an image representation which is used for image recovery by replacing tampered regions.

By allocating dual-rate source-channel coding, the quality-robustness performance of the proposed scheme is formed in two scales. For low tampering rates, higher reconstruction quality is expected, called scale 1. At the second scale, less reconstruction quality is provided, instead, higher tampering rates are achievable. The contributions of the proposed method are listed as follows:

- Better quality-robustness performance to handle both increasing the recovered quality and the tolerable tampering rate.
- Scalable self-recovery provides two levels (scales) of image recovery: higher reconstruction quality at low tampering rates and lower reconstruction quality at high tampering rate.
- Configurable rate-allocation based on recovery requirement.

The rest of this paper is organized as follows. The proposed method is discussed in Sec. 2. In Sec. 3, tamper detection and recovery procedure are described and Section 4 is dedicated to the experimental results. Finally, in Sec. 5, the proposed scheme is concluded.

2. The Proposed Method

Figure 1 represents block diagram of the embedding process of the proposed method. The original image is first compressed using SPIHT, an image compression algorithm based on multi-level wavelet decomposition which generates scalable bitstreams [31]. According to the scalable property of SPIHT, the compressed bitstream is formed with multiple bitplanes providing several quality scales, from the basic quality to the enhancement levels. In this paper, the SPIHT bitstream is not arithmetically codded and just a proportion of the beginning of the bitstream is used for generating reference data. The selected data part is partitioned into two parts according to the assigned source coding rates (R_1^s and R_2^s). The proposed scalable self-embedding method takes advantage of the scalable property of the SPIHT's compressed bitstream. Two unequal redundancy rates are allocated using LDPC channel coding.

The functionality of rate-allocation unit is to assign source and redundancy rates according to the data embedding payload. In permutation stage, the protected data parts are mixed and scrambled using a security key. Besides providing security, data permutation spreads the generated watermark all over the image. Therefore, the effect of tampering uniformly distributed between part one and two. As a matter of fact, the permutation prevents massive erasing.

For generating check bits, the image is partitioned into 8 × 8 non-overlapping blocks. Six most significant bits (MSB) of the pixel intensity, security key2 and the share of generated watermark for the block are used for check bit generation. An MD5 hash function is used for producing a digital signature. 32 bits of the generated digital signature is truncated as in [23], [29]. Generating 32 bits for 64 pixels (8 × 8 block size) means creating 0.5 bpp check bits data rate. The watermark consists of 1.5 bpp reference data and 0.5 bpp check bits are embedded into two Least Significant Bits (LSBs) of the main image. Before data embedding, 2 LSBs of the image are set to zero, according to (1).

$$p(i,j) = 4 \times \lfloor p(i,j)/4 \rfloor . \tag{1}$$

In this equation, $p(i,j)$ is the pixel intensity in coordination (i,j). Note that the LSBs do not corporate in check bit generation. Therefore, data embedding does not affect the integrity of the image.

In the next two sections, more details about producing reference data are presented. In Sec. 2.1 the concept of dual-rate allocation is proposed. Also, the proposed channel coding algorithm is mentioned in Sec. 2.2.

2.1 Rate Allocation

In the proposed dual-rate allocation technique, the compressed bitstream is separated into two parts, part one with rate R_1^{s} and part two with rate R_2^{s}, where $R_1^{\mathrm{s}} + R_2^{\mathrm{s}} = 0.5$ bpp. Two unequal redundancy rates are allocated using LDPC channel coding, R_1^{r} for the first part and R_2^{r} for the second part (Fig. 2). Since the first part provides fundamental quality scale, assigning higher redundancy rate for this part enables the recovery system for high tampering rates. In order to manage data payload for watermarking, the allocated rates should satisfy (2).

$$\left(R_1^{\mathrm{s}} + R_1^{\mathrm{r}}\right) + \left(R_2^{\mathrm{s}} + R_2^{\mathrm{r}}\right) = 1.5 \text{ bpp} . \tag{2}$$

In this paper, source and redundancy rates are assigned as $R_1^{\mathrm{s}} = 0.25$ bpp, $R_1^{\mathrm{r}} = 0.75$ bpp for the first part and $R_2^{\mathrm{s}} = 0.25$ bpp, $R_2^{\mathrm{r}} = 0.25$ bpp for the second part. Therefore, the allocated rates satisfy equation (2), (0.25 + 0.75) + (0.25 + 0.25) = 1.5 bpp.

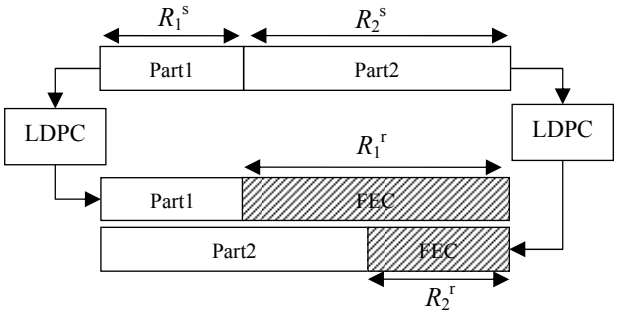


Fig. 2. Rate allocation procedure for the proposed reference generation.

2.2 Channel Coding: LDPC

The self-embedding scheme has modeled as an erasure in communication channel [23], [29] as a result of erasing embedded watermark in a tampered block. Therefore, the proposed method takes advantage of the finite-length near ideal low-density parity-check (LDPC) codes [32], designed for the binary erasure channel (BEC).

An LDPC block code (n,k) encodes k-bits message data $\mathbf{U} = [u_1, u_2, \ldots, u_k]$ to n-bits codeword data with $m = n - k$ bits redundancy, as in (3).

$$\mathbf{V} = \mathbf{U} \times \mathbf{G} . \tag{3}$$

In (3), $\mathbf{G}$ is a generator matrix which can be found by performing Gauss-Jordan elimination on parity check matrix, $\mathbf{H}$. LDPC code is called low density because of using sparse parity check matrix which causes dense generator matrix. By using a dense generator matrix, the encoding process would be very complex. In [33], the idea of semi-random parity check matrix is proposed for reducing the complexity of the encoding process. According to this method, the parity check matrix consists of two parts. A deterministic part which is mainly a diagonal matrix concatenated with a random matrix (4).

$$\mathbf{H}_{m \times n} = \left[\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & \\ 1 & 1 & \cdots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \mathbf{A}_{m \times k} \\ 0 & 0 & 1 & 1 & \end{array}\right] . \tag{4}$$

The fast encoding method generates codeword $\mathbf{V} = [p_1, p_2, \ldots, p_m, u_1, u_2, \ldots, u_k]$, according to (5). In this paper, a three-step algorithm is used for designing parity check matrix according to [34].

$$\begin{cases} p_1 = \sum_{j=1}^{k} u_j h_{1,m+j} \\ p_i = p_{i-1} \sum_{j=1}^{k} u_j h_{i,m+j}, i > 1 \end{cases} \tag{5}$$

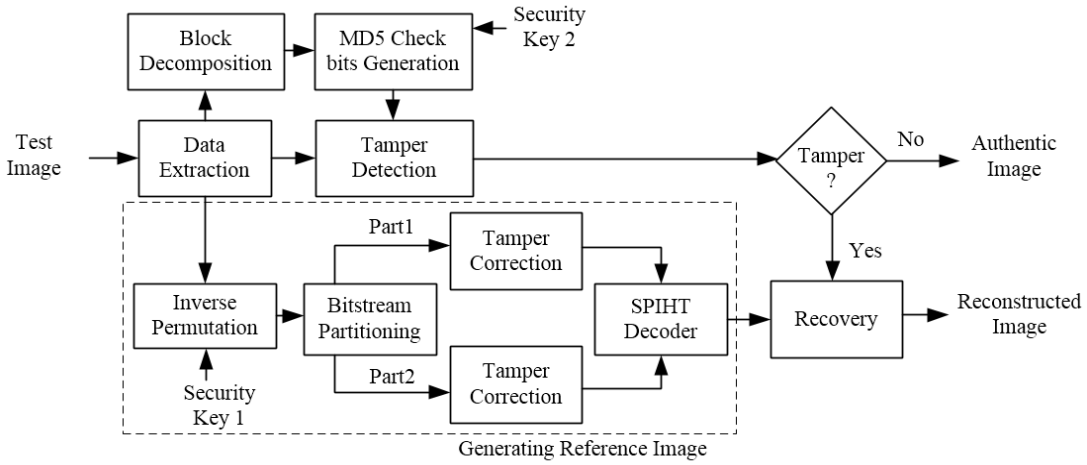


Fig. 3. Block diagram of tamper detection and recovery process of the proposed method.

3. Tamper Detection and Recovery

Figure 3 represents the block diagram of tamper detection and recovery. In this procedure, first, the watermark is extracted which consists of check bits and reference data. For tamper detection, the extracted check bits of a block are compared with the generated one for the block. The method of producing check bits is the same as the embedding process. Since the proposed method uses fragile watermarking for strict authentication, even little changes in the image content are considered as tampers. Thus, lossy image compression is not acceptable as a result of changing the embedded data in the LSB layers, while lossless image compression is acceptable.

For content restoration, a tampered block is replaced with the same block from the reference image. The procedure of generating reference image is initiated with inverse permutation on the extracted reference data [35]. Then, the data is partitioned into two parts, according to the assigned rates in Sec. 2.1. Both parts are channel decoded using message passing iterative algorithm. Then part 1 and part 2 are merged together for SPIHT decoding in order to generate the reference image. In the recovery stage, the tampered regions of the image are replaced with the same regions of the reference image. The generated reference image provides two quality scales for tamper recovery. For low tampering rates, the image is recovered by scale 1 with higher restoration quality. However, higher tampering rates are tolerable with lower reconstruction quality, called scale 2.

4. Experimental Results

For performance evaluation, four 8-bit grayscale 512 × 512 standard images including Lena, Airplane, Lake, and Crowd, are used as original images (Fig. 4). The proposed method uses two LSBs of the image for data embedding, 0.5 bpp for check bits and 1.5 bpp for reference data. The mentioned images are tamper-protected using the proposed self-embedding scheme. Figure 5 shows the corresponding watermarked images and their PSNR values are 44.15, 44.12, 44.16 and 44.18 dB, respectively.

The distortion caused by data embedding above 36 dB cannot be considered noticeable by human vision system [29]. The contents of the watermarked images in Fig. 5 are modified with different versions and tampering rates, shown in Fig. 6. The tampering rate is defined as the ratio of the number of tampered pixels to the whole image pixels. The tampering rates for the images in Fig. 6 are 27, 23.73, 5.15 and 32.03 percent, respectively. In Fig. 7, the result of tamper detection and localization is represented. In this figure, tamper masks of the tampered images in Fig. 6 are displayed, white pixels represent tampered region and black pixels are authentic. The tamper masks show that the authentication algorithm based on MD5 function can accurately detect modifications. The localization accuracy is 8 × 8 pixels as a result of the block size. Although tamper detection is block-based, the proposed content recovery method is pixel-wise. Figure 8 shows the recovered images which were modified in Fig. 6. The quality of recovery for Lena, Airplane, Lake and Crowd image are 35.51, 37.16, 41.28 and 33.18 dB, respectively.

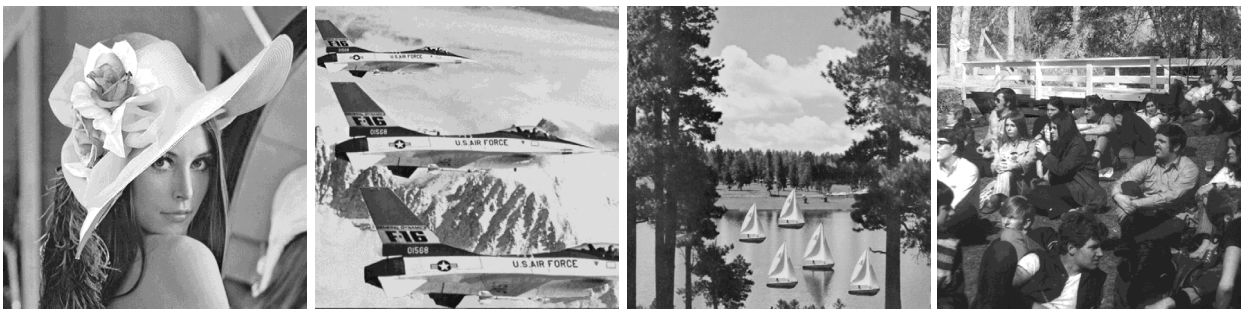
In Fig. 9, the recovery performance of the proposed method is compared with two related methods [29], [30]. Both methods use two LSBs for data embedding in a pixel-wise image recovery. In this figure, the quality of the recovered image is plotted for various tampering rates. In this figure, the tampering rates are created using cropping method for the purpose of evaluating the proposed method by the worst tampers. In this case, all the pixels' values in the tampered area are set to zero and thus, the reference and authentication data are destroyed. The tampered area is a square in the center of the image according to the desired tampering rate, as in [29], [30]. Note that the image center mainly contains the most important information of the image.

According to the proposed scalable recovery method, the quality-robustness performance is formed in two steps (Fig. 9 (a-d)). For low tampering rates less than 30 percent,

the entire reference data are completely reconstructed, leading to the highest quality level (scale 1). For more tampers above 30, the second part of the reference data with less redundancy rate cannot be decoded. Therefore, the quality of the recovered image is reduced to a lower quality level (scale 2). Instead, the image can tolerate higher tampering rates, more than 45 percent. Although the proposed method in [29] provides higher reconstruction

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

Fig. 4. Four watermarked test images: (a) PSNR = 44.15 dB, (b) PSNR = 44.12 dB, (c) PSNR = 44.16 dB, (d) PSNR = 44.18 dB.



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

Fig. 5. Four tampered images with different tampering rates: (a) 27%, (b) 23.73%, (c) 5.15%, (d) 32.03%.

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

Fig. 6. Tamper detection results in Fig. 6(a-d), (a) Lena, (b) Airplane, (c) Lake, (d) Crowd.

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

Fig. 7. Image recovery results, the quality of recovered image (a) PSNR = 35.51 dB, (b) PSNR = 37.16 dB, (c) PSNR = 41.28 dB, (d) PSNR = 33.18 dB.

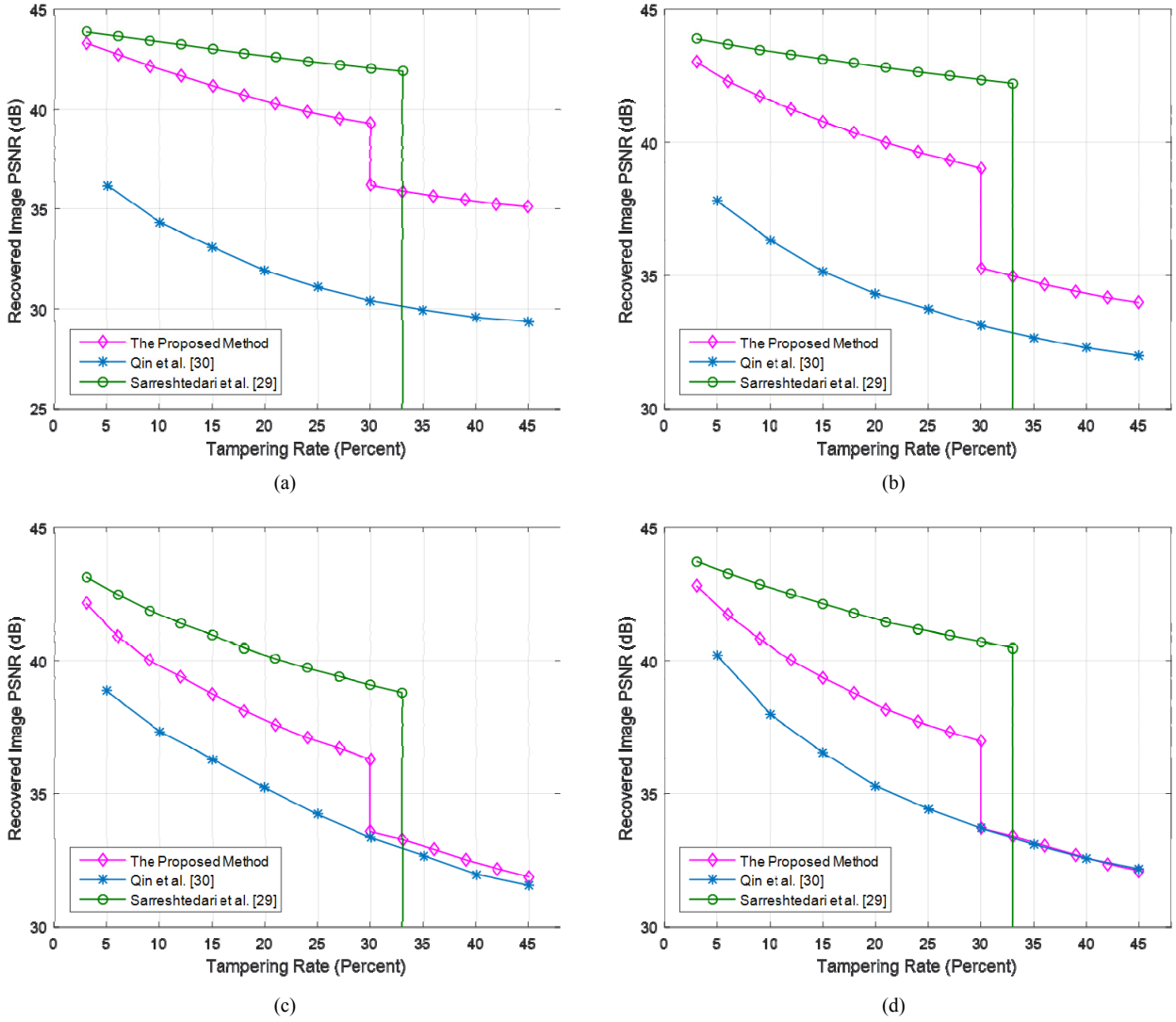


Fig. 8. The performance of the proposed method in comparison with two related works for the test images of Fig. 4: (a) Lena, (b) Airplane, (c) Lake, (d) Crowd.

quality, it is applicable for low tampering rates less than 33 percent. However, the proposed method can achieve higher tampering rates (more than 45 percent). The simulation results in Fig. 9 show that the proposed method provides higher reconstruction quality for the test images for most tampering rates in comparison with [30]. The proposed method has better performance for low texture images like Airplane (Fig. 9(b)) as a result of using SPIHT algorithm which has more efficiency for low texture images. In Fig. 9(d), the performance of the proposed method for Crowd image is the same as [30] at high tampering rates.

For a general result, the proposed method is evaluated by 1000 images and the average PSNR for the first scale is 39.7 dB and for the second scale 35.86 dB. Moreover, the standard deviations are 6.3 and 6.29 for the scale one and two, respectively.

5. Conclusion

In this paper, a scalable self-embedding method based on source-channel coding scheme was proposed. The proposed method generated the reference data by compressing the original image with 0.5 bpp. Then, the bitstream was partitioned into two parts. The first part was provided a rough approximation of the main image and the second part provided an enhancement. Therefore, the first part was received with higher redundancy rate to be prepared for high tampering rates. The second part was received with less redundancy rate which is applicable at low rate tamper correction. The proposed method used near-optimal LDPC algorithm for channel coding. The contributions of the proposed method in this paper are listed as follows: (1) Better quality-robustness performance related to reported methods. The proposed method can handle both increasing

the recovered quality and the tolerable tampering rate. (2) Scalable self-recovery not only provides higher reconstruction quality at low tampering rates, but also it increases the tolerable tampering rate. The first scale of the proposed method can recover 30 percent tampering rates with high restoration quality. The second scale can achieve higher tampering rates (more than 45 percent), however, with less quality level. (3) Configurable rate-allocation based on recovery requirement. In most self-embedding methods, the system configuration is fixed which makes them impractical. In the proposed method, quality levels can be designed by adjusting source coding rates. Also, redundancy rates are flexible based on the desired tolerable tampering rates.

References

[1] WANG, H., WANG, H-X., SUN, X-M., et al. A passive authentication scheme for copy-move forgery based on package clustering algorithm. *Multimedia Tools and Applications*, 2017, vol. 76, no. 10, p. 12627–12644. DOI: 10.1007/s11042-016-3687-5

[2] ULUTAS, G., USTUBIOGLU, A., USTUBIOGLU, B., et al. Medical image tamper detection based on passive image authentication. *Journal of Digital Imaging*, 2017, vol. 30, no. 6, p. 695–709. DOI: 10.1007/s10278-017-9961-x

[3] QIN, C., JI, P., WANG, J., et al. Fragile image watermarking scheme based on VQ index sharing and self-embedding. *Multimedia Tools and Applications*, 2017, vol. 76, no. 2, p. 2267–2287. DOI: 10.1007/s11042-015-3218-9

[4] KHOR, H. L., LIEW, S. C., ZAIN, J. M. Region of interest-based tamper detection and lossless recovery watermarking scheme (ROI-DR) on ultrasound medical images. *Journal of Digital Imaging*, 2017, vol. 30, no. 3, p. 328–349. DOI: 10.1007/s10278-016-9930-9

[5] AGARWAL, S., CHAND, S. Image forgery detection using co-occurrence-based texture operator in frequency domain. In *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications: Proceedings of ICACNI 2016*. 2017, p. 117–122. DOI: 10.1007/978-981-10-3373-5_10

[6] SINGH, A. K., KUMAR, B., SINGH, S. K., et al. Guest editorial: Robust and secure data hiding techniques for telemedicine applications. *Multimedia Tools and Applications*, 2017, vol. 76, no. 5, p. 7563–7573. DOI: 10.1007/s11042-017-4507-2

[7] LIU, X. L., LIN, C. C., YUAN, S. M. Blind dual watermarking for color images' authentication and copyright protection. *IEEE Transactions on Circuits and Systems for Video Technology*, 2016, vol. 28, no. 5, p. 1047–1055. DOI: 10.1109/TCSVT.2016.2633878

[8] FARFOURA, M. E., HORNG, S. J., GUO, J. M., et al. Low complexity semi-fragile watermarking scheme for H.264/AVC authentication. *Multimedia Tools and Applications*, 2016, vol. 75, no. 13, p. 7465–7493. DOI: 10.1007/s11042-015-2672-8

[9] BADSHAH, G., LIEW, S. C., ZAIN, J. M., et al. Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. *Journal of Digital Imaging*, 2016, vol. 29, no. 2, p. 216–225. DOI: 10.1007/s10278-015-9822-4

[10] QAZI, T., HAYAT, K., KHAN, S. U., et al. Survey on blind image forgery detection. *IET Image Processing*, 2013, vol. 7, no. 7, p. 660–670. DOI: 10.1049/iet-ipr.2012.0388

[11] UTKU CELIK, M., SHARMA, G., SABER, E., et al. Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing*, 2002, vol. 11, no. 6, p. 585–595. DOI: 10.1109/TIP.2002.1014990

[12] LIEW, S. C., LIEW, S. W., ZAIN, J. M. Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. *Journal of Digital Imaging*, 2013, vol. 26, no. 2, p. 316–325. DOI: 10.1007/s10278-012-9484-4

[13] TAGLIASACCHI, M., VALENZISE, G., TUBARO, S. Hash-based identification of sparse image tampering. *IEEE Transactions on Image Processing*, 2009, vol. 18, no. 11, p. 2491–2504. DOI: 10.1109/TIP.2009.2028251

[14] LEE, T. Y., LIN, S. D. Dual watermark for image tamper detection and recovery. *Pattern Recognition*, 2008, vol. 41, no. 11, p. 3497–3506. DOI: 10.1016/j.patcog.2008.05.003

[15] KORUS, P., BIALAS, J., DZIECH, A. Towards practical self-embedding for JPEG-compressed digital images. *IEEE Transactions on Multimedia*, 2015, vol. 17, no. 2, p. 157–170. DOI: 10.1109/TMM.2014.2368696

[16] SARRESHTEDARI, S., ABBASFAR, A., AKHAEE, M. A. A joint source-channel coding approach to digital image self-recovery. *Signal, Image and Video Processing*, 2017, vol. 11, no. 7, p. 1371–1378. DOI: 10.1007/s11760-017-1095-6

[17] QIN, C., WANG, H., ZHANG, X., et al. Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode. *Information Sciences*, 2016, vol. 373, p. 233–250. DOI: 10.1016/j.ins.2016.09.001

[18] SINGH, D., SINGH, S. K. DCT based efficient fragile watermarking scheme for image authentication and restoration. *Multimedia Tools and Applications*, 2017, vol. 76, no. 1, p. 953–977. DOI: 10.1007/s11042-015-3010-x

[19] ANSARI, I. A., PANT, M., AHN, C. W. SVD based fragile watermarking scheme for tamper localization and self-recovery. *International Journal of Machine Learning and Cybernetics*, 2016, vol. 7, no. 6, p. 1225–1239. DOI: 10.1007/s13042-015-0455-1

[20] WANG, H., HO, A. T. S., ZHAO, X. A novel fast self-restoration semi-fragile watermarking algorithm for image content authentication resistant to JPEG compression. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, vol. 7128 LNCS, p. 72–85. DOI: 10.1007/978-3-642-32205-1_8

[21] HE, H., CHEN, F., TAI, H., et al. Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme. *IEEE Transactions on Information Forensics and Security*, 2012, vol. 7, no. 1, p. 185–196. DOI: 10.1109/TIFS.2011.2162950

[22] FRIDRICH, J. Security of fragile authentication watermarks with localization. *Proceedings of SPIE- Security and Watermarking of Multimedia Contents*, 2002 vol. 4675, p. 691–700. DOI: 10.1117/12.465330

[23] KORUS, P., DZIECH, A. Efficient method for content reconstruction with self-embedding. *IEEE Transactions on Image Processing*, 2013, vol. 22, no. 3, p. 1134–1147. DOI: 10.1109/TIP.2012.2227769

[24] FRIDRICH, J., GOLJAN, M. Images with self-correcting capabilities. In *Proceedings of 1999 International Conference on Image Processing*. Kobe (Japan), 1999, p. 792–796. DOI: 10.1109/ICIP.1999.817228

[25] LIN, P. L., HSIEH, C. K., HUANG, P. W. A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, 2005, vol. 38, no. 12, p. 2519–2529. DOI: 10.1016/j.patcog.2005.02.007

[26] ZHANG, X., QIAN, Z., REN, Y., et al. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. *IEEE Transactions on Information Forensics and Security*, 2011, vol. 6, no. 4, p. 1223–1232. DOI: 10.1109/TIFS.2011.2159208

[27] YANG, C. W., SHEN, J. J. Recover the tampered image based on VQ indexing. *Signal Processing*, 2010, vol. 90, no. 1, p. 331–343. DOI: 10.1016/j.sigpro.2009.07.007

[28] LEE, J., WON, C. S. Authentication and correction of digital watermarking images. *Electronics Letters*, 1999, vol. 35, no. 11, p. 886–887. DOI: 10.1049/el:19990642

[29] SARRESHTEDARI, S., AKHAEE, M. A. A source-channel coding approach to digital image protection and self-recovery. *IEEE Transactions on Image Processing*, 2015, vol. 24, no. 7, p. 2266–2277. DOI: 10.1109/TIP.2015.2414878

[30] QIN, C., JI, P., ZHANG, X., et al. Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. *Signal Processing*, 2017, vol. 138, p. 280–293. DOI: 10.1016/j.sigpro.2017.03.033

[31] SAID, A., PEARLMAN, W. A. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Transactions on Circuits and Systems for Video Technology*, 1996, vol. 6, no. 3, p. 243–250. DOI: 10.1109/76.499834

[32] MAC KAY, D. J. C., NEAL, R. M. Near Shannon limit performance of low density parity check codes. *Electronics Letters*, 1996, vol. 32, no. 18, p. 1645–1646. DOI: 10.1049/el:19961141

[33] LI PING, LEUNG, W. K., PHAMDO, N. Low density parity check codes with semi-random parity check matrix. *IEE Electronics Letters*, 1999, vol. 35, no. 1, p. 38–39. DOI: 10.1049/el:19990065

[34] TAKI, M., OROOJI, M. A simple algorithm to design irregular LDPC codes for finite length. In *Proceeding of the 10th IEEE Singapore International Conference on Communication Systems*. Singapore, 2006, p. 1–6. DOI: 10.1109/ICCS.2006.301433

[35] JIANG, Y. *A Practical Guide to Error-Control Coding Using Matlab*. Artech House, 2010. ISBN: 9781608070886

About the Authors...

Navid DANESHMANDPOUR received his B.Sc. and M.Sc. degrees in Electrical Engineering from Azad University, Majlesi Branch, Isfahan, Iran, in 2009 and 2011, respectively. He is currently a Ph.D. student in the Dept. of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz, Iran, His research interests include digital watermarking, image retrieval, image and video coding.

Habibollah DANYALI (corresponding author) received his B.Sc. and M.Sc. degrees in Electrical Engineering respectively from Isfahan University of Technology, Isfahan, Iran, in 1991 and Tarbiat Modarres University, Tehran, Iran, in 1993. From 1994 to 2000 he was with the Dept. of Electrical Engineering, University of Kurdistan, Sanandaj, Iran, as a lecturer. In 2004 he received his Ph.D. degree in Computer Engineering from the University of Wollongong, Australia. He is currently working as an associate professor with the Dept. 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 the B.S. and M.S. degrees in Electrical Engineering from Shiraz University, Shiraz, and Sharif University of Technology, Tehran in 1993 and 1995, respectively. He performed his Ph.D. degree in Electrical Engineering from Tarbiat Modares University, Tehran, Iran. He is working as an associate professor in the Dept. of Electrical and Electronics Engineering, Shiraz Univ. of Technology, Shiraz, Iran. His research interests include content-based image retrieval, pattern recognition and medical image processing.