PAPER Special Section on Information and Communication System Security—Against Cyberattacks—

ROI-Based Reversible Data Hiding Scheme for Medical Images with Tamper Detection

Yuling LIU[†a)], **Xinxin QU**[†], **Guojiang XIN**[††], ***Nonmembers***, ***and*** **Peng LIU**[†], ***Member***

SUMMARY A novel ROI-based reversible data hiding scheme is proposed for medical images, which is able to hide electronic patient record (EPR) and protect the region of interest (ROI) with tamper localization and recovery. The proposed scheme combines prediction error expansion with the sorting technique for embedding EPR into ROI, and the recovery information is embedded into the region of non-interest (RONI) using histogram shifting (HS) method which hardly leads to the overflow and underflow problems. The experimental results show that the proposed scheme not only can embed a large amount of information with low distortion, but also can localize and recover the tampered area inside ROI.

key words: *reversible data hiding, medical images, ROI-based, prediction error expansion, sorting*

1. Introduction

Medical images and EPR play an increasingly significant role in diagnosis. However, medical images are easily copied illegally and tampered maliciously. Reversible data hiding has the excellent property that the carrier image can be lossless recovered after the embedded information is extracted [1]. Therefore, huge attentions are paid to reversible data hiding for data hiding, integrity authentication and tamper detection of medical images.

Many reversible data hiding techniques have been proposed for medical images. Zain et al. proposed a LSB based reversible data hiding scheme, and the SHA-256 hash message of ROI was embedded into the LSB of RONI for authenticating ultrasonic images [2]. The scheme is simple, and image distortion is small. Zhou et al. presented two lossless schemes to embed digital signature into medical images [3]. The first scheme was based on compressing the LSBs of randomly selected images pixels; the second scheme was based on a regular/singular (RS) approach that was introduced in the work of Goljan et al. [4]. Wu et al. proposed two schemes which combined Modulo 256 with DCT, and used for tamper detection and recovery for medical images [5]. Huang et al. improved HS technique developed by Ni et al. [6], the scheme keeps good image quality after data hiding, but embedding capacity is small [7]. In the schemes proposed in Ref. [8]–[11], Tian's difference expansion (DE) technique [12] was improved to further increase the embedding capacity. Tan et al. proposed a dual-watermarking algorithm for hiding EPR and tamper detection [13]. A random signal was used to control the embedded location, and combined with the RSA encryption algorithm to further improve the security of system. The embedding capacity of the scheme is large, but it can only locate the tampered area but not recover the tampered area. AI-Qershi and Khoo proposed two ROI-based schemes. In Ref [14], a combination of DE technique and the modified DE technique was adopted. In Ref [15], the DE algorithm and the three-level DWT algorithm were combined. EPR and the authentication information of ROI were embedded into ROI, the detection and recovery information are embedded into RONI. The drawback of Ref [15] is the lack of reversible capacity of RONI area.

To sum up, the reversible data hiding technique for medical images should consider the following points: (1) The division of ROI and RONI; (2) The integrity authentication of ROI; (3) Localization and recovery of the tampered area inside ROI; (4) High embedding capacity; (5) The security of the system.

By considering the above problems, a ROI-based reversible data hiding scheme for medical images is proposed in this paper. The original image can be lossless recovered after the embedded information is extracted.

2. Proposed Reversible Data Hiding Scheme

The proposed scheme combines the modified DE technique with the HS technique.

2.1 Prediction Error Expansion

The current pixel can be predicted according to its neighboring pixels, and then the prediction error can be computed. Because of high relevance of image pixel values, the value of the prediction error is close to zero. Prediction using a rhombus pattern is the most accurate prediction method [16], which four neighboring pixels (i.e., $v_{i,j-1}$, $v_{i+1,j}$, $v_{i,j+1}$, and $v_{i-1,j}$) are used to predict the current pixel (i.e., $u_{i,j}$) (see Fig. 1).

All pixels of the image are divided into two sets: the Cross set and the Dot set. In the first round, the Cross set is used to embed data, the Dot set remains unchanged and is used to calculate prediction values, and vice versa in the second round. Without loss of generality, a pixel value of the

Manuscript received May 9, 2014.
Manuscript revised September 12, 2014.
Manuscript publicized December 4, 2014.

[†]The authors are with College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China.
[††]The author is with College of Management and Information Engineering, Hunan University of Chinese Medicine, Changsha 410082, China.
a) E-mail: yuling_liu@126.com

DOI: 10.1587/transinf.2014ICP0001

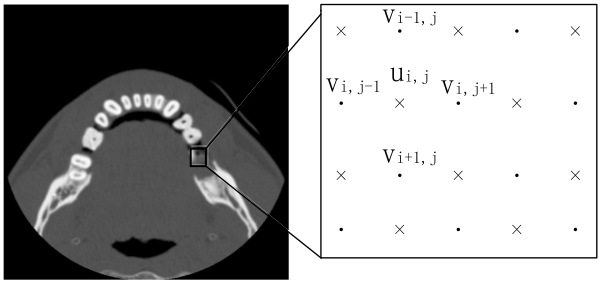

Fig. 1 Prediction using a rhombus pattern.

Cross set ($u_{i,j}$, see Fig. 1) is used to explain the embedding process as follows.

The predicted value $u'_{i,j}$ is calculated by:

$$u'_{i,j} = \left\lfloor \frac{v_{i,j-1} + v_{i+1,j} + v_{i.j+1} + v_{i-1,j}}{4} \right\rfloor \tag{1}$$

Then the prediction error $d_{i,j}$ is calculated by:

$$d_{i,j} = u_{i,j} - u'_{i,j} \tag{2}$$

The prediction error $d_{i,j}$ is expanded to embed information, as shown below:

$$D_{i,j} = \begin{cases} 2 \times d_{i,j} + b, & d_{i,j} \in [T_n, T_p] \\ d_{i,j} + T_p + 1, & d_{i,j} > T_p \\ d_{i,j} + T_n, & d_{i,j} < T_n \end{cases} \tag{3}$$

where $D_{i,j}$ is called the modified prediction error, and bϵ [0, 1] is one bit of embedded information. T_n is a negative threshold value and T_p is a positive threshold value. The prediction error in the range of $\left[T_n, T_p\right]$ is used to embed information. The image distortion and the embedding capacity will decrease when T_n and T_p are changed to close to zero. Therefore, the choices of T_n and T_p are decided by the actual needs.

When one bit of embedded information has been embedded into the current pixel $u_{i,j}$, and $u_{i,j}$ is changed as:

$$U_{i,j} = u'_{i,j} + D_{i,j} \tag{4}$$

At the receiving end, the modified prediction error is calculated by:

$$D_{i,j} = U_{i,j} - u'_{i,j} \tag{5}$$

The original prediction error is calculated as follows:

$$d_{i,j} = \begin{cases} \left\lfloor D_{i,j}/2 \right\rfloor, & D_{i,j} \in \left[2T_n, 2T_p + 1\right] \\ D_{i,j} - T_p - 1, & D_{i,j} > 2T_p + 1 \\ D_{i,j} - T_n, & D_{i,j} < 2T_n \end{cases} \tag{6}$$

At the same time, the embedded information can be recovered without error as shown below:

$$b = D_{i,j} \bmod 2, D_{i,j} \in \left[2T_n, 2T_p + 1\right] \tag{7}$$

Finally, the original pixel value is calculated by:

$$u_{i,j} = u'_{i,j} + d_{i,j} \tag{8}$$

After data hiding, the overflow/underflow problem may occur. Taking one 16-bit DICOM image as an example, to prevent the overflow/underflow problem, $U_{i,j}$ must be restricted in the range of [0, 65535],

$$0 \le u_{i,j} + D_{i,j} \le 65535$$

A location map is used to solve this problem. If there is no overflow/underflow problem occurred after data hiding, a value 1 is assigned in the location map, otherwise a value 0 is assigned.

2.2 Sorting Techniques

Before data hiding, prediction errors are sorted in ascending order by local variance which keeps unchanged after data hiding. Local variance reflects the detail information of the image, which means that, the smaller the local variance is, the smaller the prediction error is. Local variance for each pixel value can be calculated as follows:

$$u_{i,j} = \frac{1}{4} \sum_{k=1}^{4} (\Delta v_k - \Delta \bar{v}_k)^2 \tag{9}$$

where $\Delta v_1 = |v_{i,j-1} - v_{i-1,j}|$, $\Delta v_2 = |v_{i-1,j} - v_{i,j+1}|$, $\Delta v_3 = |v_{i,j+1} - v_{i+1,j}|$, $\Delta v_4 = |v_{i+1,j} - v_{i,j-1}|$ and $\Delta \bar{v}_k = (\Delta v_1 + \Delta v_2 + \Delta v_3 + \Delta v_4)/4$.

With the sorting technique, the pixel with the smallest local variance will be selected firstly for embedding information. In this way the image distortion can be effectively reduced especially while little information is embedded.

2.3 Embedding and Extracting Procedure

In this section, the details of embedding and extracting processes are described.

A. Image Partition and Watermark Generation

Before data hiding, the medical image should be divided into three parts: ROI, RONI and border area.

1. ROI is selected by a polygon. Border area is the bottom line of the image (see Fig. 2). The number of vertices and the vertices of the polygon should be recorded for describing ROI, denoted by Droi. The first 8 bits of Droi are used to represent the number of vertices. Let Lc denote the total length of Droi.
2. Calculate the hash message of ROI area using MD5 algorithm, denoted by H.
3. Pixel values inside ROI are compressed by Huffman coding, denoted by ROIcomp. It will be used for recovery in case of tampered ROI.
4. ROI area is divided into blocks of 16×16 pixels each. The average of every block is computed, and compressed by Huffman coding, denoted by AVEcomp,

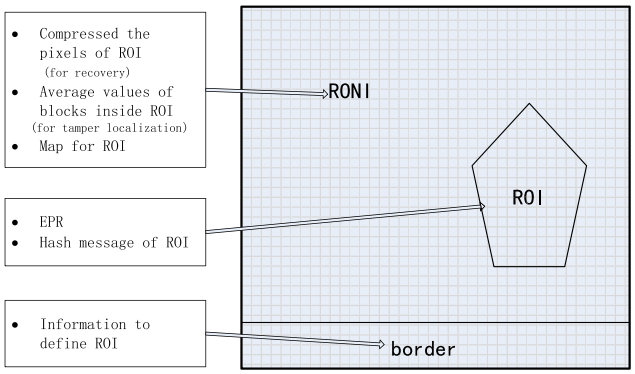

Fig. 2 Three areas used for data hiding.

which will be used for tamper detection.

B. Reversible Embedding

1. Extract the LSBs of the pixel values inside border area with the length L_c. These values are concatenated to form B_{LSB}. Then Droi are embedded by replacing the LSB of these pixel values.
2. The first watermark w_1 is formed by concatenating EPR, H and B_{LSB}, and embedded into ROI. Let Len_1 denote the total length of w_1. Before data hiding, pixels in ROI are firstly categorized into two sets: the Cross set and the Dot set. Taking the Cross set as an example, prediction values and local variances are calculated, then prediction values are sorted in ascending order of local variances. Finally, w_1 is embedded into the sorted prediction values sequentially until all Len_1 bits are embedded. A location map is formed, denoted by LM.
3. The second watermark w_2 is formed by combining ROIcomp, AVEcomp and LM, which will be embedded into RONI. The first 20 bits of w_2 were reserved to represent the length of ROIcomp and AVEcomp, and the length of ROIcomp and AVEcomp are represented by 10 bits respectively. Let Len_2 denote the total length of w_2. RONI is a smoother area where the pixels tend to zero. HS algorithm developed by Ni is employed. First, the peak point and the zero point are searched. The peak point corresponds to the pixel value of the maximum number of pixels in RONI, and the zero point corresponds to the pixel value of the minimum number of pixels in RONI. First, generate the histogram of RONI and find the peak point with the value a and the zero point with the value b. If the number of the pixel which pixel value is b is not zero, record the coordinate (i, j) of those pixels, and then this record will send to the receiving end with the value of a and b as the key. But this situation happens rarely. Then scan the image again to embed w_2. If the pixel value is equal to a, check the to-be-embedded bit. When the to-be-embedded bit is "1", the pixel value is changed to $a + 1$; When the to-be-embedded bit is "0", the pixel value remains a. If the pixel value is in the range of $[a, b)$, it is changed by adding 1.

Figure 2 presents the three areas used for embedding information. Through the above three steps, all the information has been embedded into a medical image, then the image can be stored for clinical treatment, research and teaching.

C. Extracting and Recovering

1. From the same location as the embedding process, Droi can be extracted. Then ROI area and RONI area are determined.
2. Scan RONI of the marked image, if the pixel value is equal to a, a bit "1" is extracted; if the pixel value is equal to $a + 1$, a bit "0" is extracted, then this pixel value is recovered to a; if the pixel value is in the range of $(a, b]$, it is recovered by subtracting 1. In this way, w_2 is extracted. ROIcomp, AVEcomp and LM can be obtained by decomposing w_2. If the key contains not only the value of a and b, but also the coordinate (i, j), recover the pixel value of those location to b.
3. Pixel values in ROI are categorized into two sets: the Cross set and the Dot set. In contrast to embedding process, the embedded information is firstly extracted from the Dot set. With LM, w_1 is extracted. EPR, H and B_{LSB} can be obtained by decomposing w_1.
4. With B_{LSB}, the modified LSBs inside border area are restored.
5. Calculate the hash message of the recovered ROI, denoted by H′. If H is equal to H′, the image is authentic; if not, ROI has been tampered, and go to the next step for tamper localization and recovery.

The recovered ROI is divided into blocks of 16×16 pixels each, and then the average of every block is computed, denoted by AVE'. AVEcomp and ROIcomp are decompressed to achieve AVE and ROI. Comparing AVE' and AVE, and the blocks with different average are recorded, and then those blocks are recovered with ROI.

3. Experimental Results

Three medical images of different modalities (CT, MRI and MG), which were downloaded from http://imaging.cancer.gov/, were provided to verify the performance of the algorithm. In experiments, each vertex coordinates are represented by 20 bits. The values of T_n and T_p are set as -4 and 4, respectively.

3.1 Capacity Versus Distortion Performance

Figure 3 and Table 1 show the results of embedding the information into the medical image. The size of CT, MRI and MG are 512×512 (16 bits), 640×640 (16 bits) and 4096×3328 (16 bits), respectively. The left column of Fig. 3 shows the partition of the original image, the middle column shows

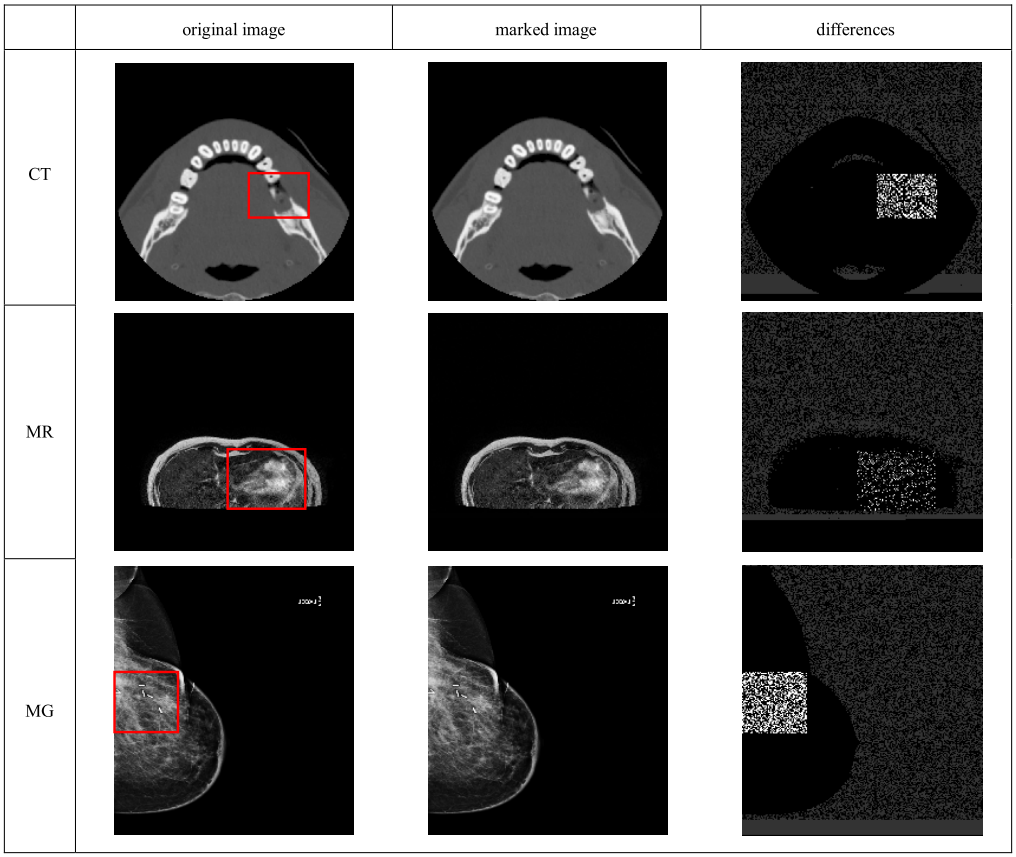

Fig. 3 Embedding and extracting results for 3 images of different modalities.

Table 1 Embedding results for 3 images of different modalities.

Modality (Image)	Image Size	Size of w_1 (bits)	Size of w_2 (bits)	Size of ROI (%)	Embedding Capacity (bpp)	PSNR (dB)	SSIM
CT	512×512	5260	123448	4.69	0.4444	97.0287	0.9999
MR	640×640	7060	270782	8.01	0.6783	98.5473	0.9999
MG	4096×3328	35260	9523014	6.08	0.7012	92.5755	1.0000

Note: embedding capacity calculated as: (size of w_1 + size of w_2)/image size.

the results after data hiding, and the right column shows the difference between the original image and the marked one. As shown in Table 1, the marked images show good performance in term of PSNR and the embedding capacity. The embedding capacity of ROI depends on the size of the ROI, and the value of T_n and T_p. The embedding capacity of ROI can be increased either by increasing the size of ROI or by changing the value of T_n and T_p. When T_n and T_p are changed to close to zero, the embedding capacity of ROI will decrease, but the image quality will increase. Therefore, the choices of T_n and T_p and the size of ROI are decided by the actual needs.

3.2 Tamper Detection and Recovery Capability

If the marked image had not been tampered, it can be recovered pixel by pixel after data extracting, otherwise the tampered area inside ROI can be localized and recovered. To verify the performance of tamper localization and recovery, some pixels inside ROI of the marked image were replaced. During extracting process, EPR cannot be extracted sometimes because of the changes on pixel level, but the tampered area can be successfully localized and recovered, as shown in Fig. 4. The image (a) is the marked image, and some pixels inside ROI were modified to form the tampered image (b), and the modification is on the pixel level. The hash message for the recovered image is computed as "90F796FFE95B06552D7B6740F557C759", and the extracted hash message from the image (a) is "F63F0AF0AA6C9DF3ACC74979B2BC8344", thus it is sure that the image (a) has been tampered. The image (c) shows the differences between the original image and the recovered image. The tampered area can be localized with the extracted AVE (the smaller red-block in the image (d)), and this area are recovered with the corresponding compressed version of the same area.

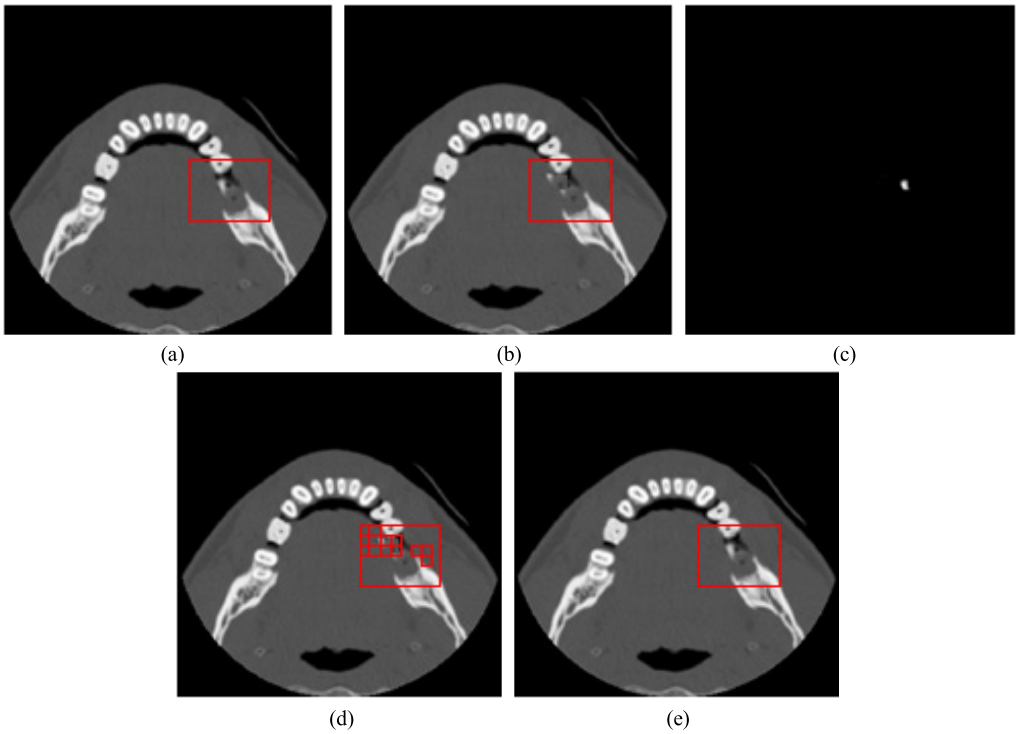

Fig. 4 Tamper localization and recovery: (a) marked image, (b) tampered image, (c) the differences between the original image and the recovered image, (d) localizing tampered area and (e) recovering tampered area.

3.3 Comparison with Other Algorithms

Compared with the previous similar schemes developed by AI-Qershi and Khoo [14], [15], the proposed scheme has better performance in terms of PSNR and SSIM (see Table 2). 100 medical images were used with the same size of EPR and the same ROI, and the proposed scheme is better in term of PSNR and SSIM. The available capacity of the whole image is also larger than the compared schemes. Because the RONI of most medical images are black backgrounds which pixel values are close to zero, the histogram of RONI has a high peak point. As we all know that the more dramatically changing in amplitude a given histogram is, the larger the embedding capacity is. Therefore, the proposed scheme has a large embedding capacity. At the same time, the sorting of prediction errors can effectively reduced image distortion inside ROI.

The medical image is an important reference for medical diagnosis and the medical image itself is more important than the to-be-embedded information. Therefore, the tamper detection capability is necessary. As shown in Fig. 4, the proposed scheme can locate and recover the tampered area inside ROI. If the tampered area is inside RONI, it can be confirmed by comparing the recovered pixel values of ROI and the extracted ROIcomp. Although the tampered area inside RONI will not affect the use of the medical image, it can warn the managers of the hospital management system that the system is under attack. A comparison between our scheme and the previous schemes for the tamper detection capability is illustrated in Table 3.

Table 2 Comparisons between the proposed scheme and the reviewed schemes.

Method	Available Capacity (b/pixel)	PSNR (dB)	SSIM
AI-Qershi et al.'s [14]	0.4880	70.2326	0.99985
AI-Qershi et al.'s [15]	0.4735	85.0866	0.99991
Proposed	0.4899	92.4579	0.99993

Note: the values in the table are the average values of 100 medical images.

Table 3 Comparisons between the proposed scheme and other schemes for the tamper detection capability.

Method	Tamper Detection Capability		Reversible
	ROI	RONI	
Zain.'s [2]	×	×	√
Wu.'s [5]	√	√	×
Chiang.'s [9]	√	√	Only ROI
Guo.'s [10]	×	×	√
AI-Qershi et al.'s [14]	√	√	√
AI-Qershi et al.'s [15]	√	×	Only ROI
Proposed	√	√	√

4. Conclusion

This paper proposes a reversible data hiding scheme for medical images. In the scheme, the different texture characteristic between ROI and RONI is taken into account. Inside ROI, the sorting of prediction errors can effectively reduce

the distortion especially for less embedded information, but it might be useless when the data is fully embedded in the space. Inside RONI, where pixel values are close to zero, HS method is used with a large embedding capacity without the overflow and underflow problems. The medical image is authenticated by the hash message of ROI, and the tampered area inside ROI can be localized and recovered. However, the proposed scheme is image-dependent because that HS technique is image-dependent.

Acknowledgments

This work was partially supported by National Natural Science Foundation of China (No. 61103215, 61173141, 61173142, 61173136, 61232016, 61202439, 61202496, 61373132, 61373133), National Basic Research Program 973 (No. 2011CB311808), Hunan Provincial Natural Science Key Foundation of China (No. 13JJ2031), Youth Growth Plan of Hunan University.

References

[1] N.O. Abokhdair and A.B.A. Manaf, "A review of reversible watermarking properties, applications and techniques for medical images," 6th International Conference on Information Technology, pp.1–6, 2013.
[2] J.M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," arXiv preprint arXiv:1101.1603, 2011.
[3] Z. Zhou, H.K. Huang, and B.J. Liu, "Digital signature embedding (DES) for medical image integrity in a data grid off-site backup archive," Proc. SPIE 5748, pp.306–317, 2005.
[4] M. Goljan, J.J. Fridrich, and R. Du, "Distortion-free data embedding for images," Information Hiding, Springer Berlin Heidelberg, pp.27–41, 2001.
[5] J.H.K. Wu, R.F. Chang, C.J. Chen, C.L. Wang, T.H. Kuo, W.K. Moon, and D.R. Chen, "Tamper detection and recovery for medical images using near-lossless information hiding technique," J. Digital Imaging, vol.21, no.1, pp.59–76, 2008,
[6] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.16, no.3, pp.354–362, 2006.
[7] L.C. Huang, L.Y. Tseng, and M.S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," J. Systems and Software, vol.86, no.3, pp.716–727, 2013.
[8] D.C. Lou, M.C. Hu, and J.L. Liu, "Multiple layer data hiding scheme for medical images," Computer Standards & Interfaces, vol.31, no.2, pp.329–335, 2009.
[9] K.H. Chiang, K.C. Chang-Chien, R.F. Chang, and H.Y. Yen, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding," J. Digital Imaging, vol.21, no.1, pp.77–90, 2008.
[10] X. Guo and T. Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," J. Digital Imaging, vol.22, no.1, pp.53–64, 2009.
[11] O.M. Al-Qershi and B.E. Khoo, "High capacity data hiding schemes for medical images based on difference expansion," J. Systems and Software, vol.84, no.1, pp.105–112, 2011.
[12] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol.13, no.8, pp.890–896, 2003.
[13] C.K. Tan, J.C. Ng, X. Xu, C.L. Poh, Y.L. Guan, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," J. Digital Imaging, vol.24, no.3, pp.528–540, 2011.
[14] O.M. Al-Qershi and B.E. Khoo, "Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images," Proc. International Conference on Medical Systems Engineering (ICMSE), pp.829–834, 2009.
[15] O.M. Al-Qershi and B.E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images," J. Digital Imaging, vol.24, no.1, pp.114–125, 2011.
[16] V. Sachnev, H.J. Kim, J. Nam, S. Suresh, and Y.Q. Shi, "Reversible Watermarking Algorithm Using Sorting and Prediction," IEEE Trans. Circuits Syst. Video Technol., vol.19, no.7, pp.989–999, 2009.

Yuling Liu is an assistant professor at Hunan University. She received her BS and PhD degree in computer science from Hunan University, in 2003 and 2008, respectively. She is the author of more than 20 journal papers. Her research interests include information hiding, information security, digital watermarking and natural language processing.

Xinxin Qu received her BS Degree in network engineering from Tianjin Polytechnic University in 2012. She is currently pursuing the MS degree in Information Science and Engineering from Hunan University. Her research interests include digital watermarking, data hiding and information security.

Guojiang Xin is an assistant professor at Hunan University of Chinese Medicine. He received his PhD degree in computer science from Central South University in 2013. His main research interest is image processing.

Peng Liu was born in 1984. He received his BSc degree in applied mathematics from Xiangtan University in 2006. Now, he is a PhD candidate in software science at Hunan University. He is a student member of the IEICE. His main research interest is test generation.