

Loughborough University Institutional Repository

Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images

This item was submitted to Loughborough University's Institutional Repository by the/an author.

Citation: LIU, X. ... et al, 2018. Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images. IN: Zhang, J. and Chen, P-H. (eds). Proc. SPIE 10579, Medical Imaging 2018: Imaging Informatics for Healthcare, Research, and Applications, 105791I (6 March 2018); doi: 10.1117/12.2292852.

Additional Information:

- Copyright (2018) Society of Photo-Optical Instrumentation Engineers (SPIE). One print or electronic copy may be made for personal use only. Systematic reproduction and distribution, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper are prohibited.

Metadata Record: <https://dspace.lboro.ac.uk/2134/32538>

Version: Published

Publisher: © Society of Photo-Optical Instrumentation Engineers (SPIE)

Rights: This work is made available according to the conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) licence. Full details of this licence are available at: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

Please cite the published version.

PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images

Xiyao Liu, Jieting Lou, Yifan Wang, Jingyu Du, Beiji Zou, et al.

Xiyao Liu, Jieting Lou, Yifan Wang, Jingyu Du, Beiji Zou, Yan Chen, "Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images," Proc. SPIE 10579, Medical Imaging 2018: Imaging Informatics for Healthcare, Research, and Applications, 105791I (6 March 2018); doi: 10.1117/12.2292852

SPIE.

Event: SPIE Medical Imaging, 2018, Houston, Texas, United States

Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images

Xiyao Liu^a, Jieting Lou^a, Yifan Wang^a, Jingyu Du^a, Beiji Zou^a, and Yan Chen^{*b}

^aSchool of Information Science and Engineering, Central South University, Changsha, China;

^bApplied Vision Research Centre, Loughborough University, Loughborough, UK

ABSTRACT

Authentication and copyright identification are two critical security issues for medical images. Although zero-watermarking schemes can provide durable, reliable and distortion-free protection for medical images, the existing zero-watermarking schemes for medical images still face two problems. On one hand, they rarely considered the distinguishability for medical images, which is critical because different medical images are sometimes similar to each other. On the other hand, their robustness against geometric attacks, such as cropping, rotation and flipping, is insufficient. In this study, a novel discriminative and robust zero-watermarking (DRZW) is proposed to address these two problems. In DRZW, content-based features of medical images are first extracted based on completed local binary pattern (CLBP) operator to ensure the distinguishability and robustness, especially against geometric attacks. Then, master shares and ownership shares are generated from the content-based features and watermark according to (2,2) visual cryptography. Finally, the ownership shares are stored for authentication and copyright identification. For queried medical images, their content-based features are extracted and master shares are generated. Their watermarks for authentication and copyright identification are recovered by stacking the generated master shares and stored ownership shares. 200 different medical images of 5 types are collected as the testing data and our experimental results demonstrate that DRZW ensures both the accuracy and reliability of authentication and copyright identification. When fixing the false positive rate to 1.00%, the average value of false negative rates by using DRZW is only 1.75% under 20 common attacks with different parameters.

Keywords: Medical image, authentication, copyright identification, zero-watermarking, completed local binary pattern

1. INTRODUCTION

The sharing and exchanging of medical images between different hospital and health institutes have become a trend in medicine teaching, telemedicine and other cooperative working applications. However, the risks of patient misidentification, image forgery, and copyright infringement are increasing concomitantly because that the medical images can be easily tempered, forged, copied and disseminated by lawless users during their exchanging and sharing procedures. Therefore, the authentication and copyright identification have become two crucial security issues for medical images.

The watermarking technique is an effective method for authentication and copyright identification. The existing watermarking schemes for medical images can be classified into three main categories: the regions of interest (ROI) lossless watermarking¹⁻⁵, reversible watermarking⁶⁻⁸ and zero-watermarking⁹⁻¹¹. All of them use the information for authentication or copyright identification as watermark.

ROI lossless watermarking schemes embed watermark into regions of non-interest (RONI) of medical images without modifying ROI to decrease the impact on medical diagnosis. Gunjal *et al.*¹ proposed a robust watermarking scheme, in which the watermark is embedded into the Discrete Wavelet Transform (DWT) domain of the RONI. Parah *et al.*² proposed another robust watermarking scheme, in which the watermark is embedded into Discrete Cosine Transform (DCT) domain of RONI. To enhance the watermarking security, Memon *et al.*³ proposed a dual watermarking scheme based on image morphology and LSB technique. To improve the watermark robustness, Pandey *et al.*⁴ combined the DWT and Singular Value Decomposition (SVD) and embedded the watermark into the DWT-SVD domain of RONI. Priyanka *et al.*⁵ embedded watermark into the RONI of medical image based on Integer Wavelet transform (IWT) and

SVD transform. These ROI lossless watermarking schemes are sufficient robust. However, it is easy for attackers to remove the embedded watermark by substituting the RONI because its division is executed in spatial domain. In addition, the slight distortions in RONIs caused by watermark embedding still have potential impact on medical diagnosis, which needs further improvements.

In recent years, robust reversible watermarking schemes⁶⁻⁸ have been proposed to protect medical images. An *et al.*⁶ proposed a content-adaptive reversible watermarking scheme based on histogram rotation technique. An *et al.*⁷ embedded a watermark in the wavelet domain based on shifting and clustering of statistical histograms. Lei *et al.*⁸ embedded the signature information and textual data into DWT-SVD domain of medical images based on recursive dither modulation (RDM). These reversible watermarking schemes can recover medical images losslessly after watermark extraction and their embedded watermark is hardly to be removed, which is superior to ROI lossless watermarking schemes. However, there are still two disadvantages of these schemes. First, medical diagnosis must be performed after watermark extraction because the image needs to be recovered for medical diagnosis, which causes inconveniences. Second, there is no watermark in the recovered medical image and thus these schemes cannot protect medical images anymore once the medical images are recovered, which limits their applicability.

The disadvantages of the ROI lossless watermarking and reversible watermarking schemes can be overcome in zero-watermarking schemes. Different from ROI lossless and reversible watermarking schemes, zero-watermarking schemes establish the relationships between watermark and content-based features of medical images without direct watermark embedding. By using content-based features of medical images, zero-watermarking schemes can provide authentication and copyright identification durably, reliably and losslessly during the whole healthcare procedure. Dong *et al.*⁹ proposed a DCT-based zero-watermarking scheme, in which a DCT-based feature is extracted and then a binary vector for authentication and copyright identification is generated based on the extracted feature and watermark information. Vellaisamy *et al.*¹⁰⁻¹¹ proposed two zero-watermarking schemes by utilizing of the first 3 and 6 sign bits of Hu's invariant moments¹² in the Contourlet Transform (CT)-SVD domain of medical images, respectively. Although zero-watermarking are more suitable to protect medical images than the former two categories of watermarking schemes and have good robustness against various common signal attacks, there are still two problems to be addressed. First, the existing zero-watermarking schemes for medical images mainly emphasize the robustness of extracted features *but rarely consider or analyze their distinguishability*. However, different medical images in the same type, such as fundus images, may be similar to each other. Therefore, the possibility of wrongly authenticating two similar medical images from different patients as from a same patient or wrongly identifying a similar medical image as a copy by using these zero-watermarking schemes cannot be ignored. Second, the robustness of existing zero-watermarking schemes for medical images is *insufficient against some geometric attacks*, such as cropping, rotation and flipping, which needs further improvements.

To address these two problems of zero-watermarking, a novel discriminative and robust zero-watermarking (DRZW) is proposed in this study. In DRZW, content-based features of medical images are first extracted based on completed local binary pattern (CLBP) operator¹³ which is one of the best handcraft operators for texture classification, to ensure the *remarkable distinguishability and robustness, especially against geometric attacks*. Then, master shares and ownership shares are generated from the content-based features and watermark according to (2,2) visual cryptography¹⁴. Finally, the ownership shares are stored for authentication and copyright identification. For queried medical images, their content-based features are extracted and master shares are generated. Their watermarks for authentication and copyright identification are recovered by stacking the generated master shares and stored ownership shares.

200 different medical images of 5 types are collected as the testing data and our experimental results demonstrate that DRZW ensures both the accuracy and reliability of the identification of authenticity and copyright. When fixing the false positive rate to 1.00%, the average value of false negative rates by using DRZW is only 1.75% under 20 common attacks with different parameters, which outperforms the existing zero-watermarking schemes for medical images.

The rest of this paper is organized as follows. The proposed scheme is described in Section 2. The experimental results are provided and analyzed in Section 3. Finally, the paper is concluded in Section 4.

2. THE PROPOSED SCHEME

The proposed DRZW includes two phases, which are the watermark-sharing phase and watermark-recovery phase, as shown in Fig. 1. In the watermark-sharing phase, the copyright information of the medical images will be registered by establishing an ownership database according to the medical images and their relevant watermarks. In watermark-

recovery phase, the watermark is recovered. The authentication and copyright identification are accomplished by comparing the recovered watermark with the original watermark. The detailed procedures of the two phases are below.

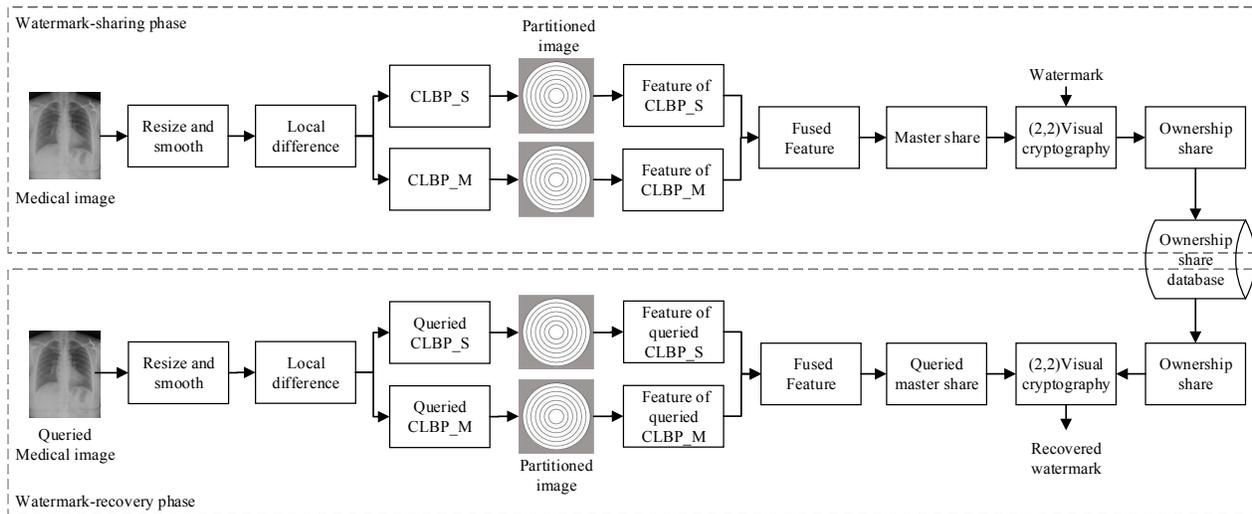


Fig. 1. The procedure of DRZW.

2.1 Watermark-sharing phase

Step 1. The input image is resized from $w \times h$ to 370×370 . Here, w and h are the width and height the original medical image, respectively. In this manner, the robustness against resizing attacks is enhanced.

Step 2. The resized image is smoothed by Gaussian low pass filter to enhance the robustness against noise addition attacks.

Step 3. The local differences of luminance component of input image are calculated at different scales. In our study, the local differences between the center pixels with their 8 circularly and evenly spaced neighbors with radius 1, 16 neighbors with radius 2, and 24 neighbors with radius 3 are calculated to generate three local difference images.

Step 4. Three CLBP-Sign (CLBP_S) and three CLBP-Magnitude (CLBP_M) images are generated from the three local differences images following the same procedure in Guo's scheme¹³. These CLBP_S and CLBP_M images are utilized to extract features for protecting the medical images due to their strong distinguishability for texture classification and robustness against flipping, rotation, contrast adjustment and brightness adjustment.

Step 5. Each CLBP-based image is partitioned into a central circle and $N-1$ concentric rings. The radius of the central circle and the widths of concentric rings are set to r , as shown in Fig. 2. For each pixel (i, j) in the CLBP-based image, its distance $Dist(i, j)$ to the center point of this image (i_o, j_o) is calculated as shown in (1).

$$Dist(i, j) = \sqrt{(i - i_o)^2 + (j - j_o)^2} \quad (1)$$

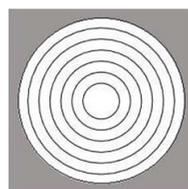


Fig. 2. Example of a partitioned CLBP-based image.

In our study, N is equal to 24, r is equal to 7.5. A pixel (i, j) is divided into the k -th partition based on its $Dist(i, j)$, as shown in (2).

$$k = \lfloor Dist(i, j) / r \rfloor \quad (2)$$

In this manner, the robustness against flipping and rotation is enhanced because the pixels still belong to their original associated partitions when the images are flipped or rotated. In addition, we only use the pixels when their $Dist(i, j)$ are smaller than 180. The pixels outside the largest ring, which are shown as dark regions in Fig. 2, are not utilized in our scheme due to two reasons. First, these regions are the most common places for cropping attacks, the robustness of image features can be enhanced by discarding them. Second, the main visual components of image are usually concentrated in its central region. Therefore, the image features generated by discarding these dark regions do not lose much distinguishability.

Step 6. Calculate the mean μ , variance δ , skewness s , and kurtosis w of each partition as shown in (3)-(6).

$$\mu_k = \frac{1}{N_k} \sum_{i=1}^{N_k} I_k(i) \quad (3)$$

$$\delta_k = \frac{1}{N_k - 1} \sum_{i=1}^{N_k} (I_k(i) - \mu_k)^2 \quad (4)$$

$$s_k = \frac{\frac{1}{N_k} \sum_{i=1}^{N_k} (I_k(i) - \mu_k)^3}{\left(\sqrt{\frac{1}{N_k} \sum_{i=1}^{N_k} (I_k(i) - \mu_k)^2} \right)^3} \quad (5)$$

$$w_k = \frac{\frac{1}{N_k} \sum_{i=1}^{N_k} (I_k(i) - \mu_k)^4}{\left(\frac{1}{N_k} \sum_{i=1}^{N_k} (I_k(i) - \mu_k)^2 \right)^2} \quad (6)$$

where I_k is the k -th partition of CLBP-based images, N_k is the total number of pixels in I_k , and $I_k(i)$ is the i -th pixel of I_k .

Step 7. For each CLBP-based image, these four statistics are binarized based on their own median values. Concatenate the binary bits generated from all the three CLBP_S and three CLBP_M as the final extracted feature vector f . In our study, the dimension of the feature vector is $3 \times 2 \times 24 \times 4 = 576$ bits.

Step 8. Rearrange the vector f into a binary matrix F of size 24×24 . Generate master share M and ownership share O from the matrix F and a binary watermark of size 24×24 , which contains information for authentication and copyright identification, according to (2,2) visual cryptography. The (2, 2) visual cryptography is a typical visual cryptography scheme proposed by M. Naor *et al.*¹⁴, in which each pixel of a binary image is substituted by a pair of shares consisting of four sub-pixels. A white pixel is split into two identical shares, whereas a black pixel is split into two complementary shares, as shown in Table 1.

Table 1. The concept of (2, 2) visual cryptography.

Pixel value	1 (white pixel)	0 (black pixel)
Master share		
Ownership share		
Stack result		

The (2, 2) visual cryptography is a low-cost injective function which can offer reversibility of watermark to maintain the distinguishability and robustness of the extracted feature f . In our study, the sizes of matrices M and O are set to 48×48 .

Divide M and O into 24×24 non-overlapping 2×2 blocks denoted as $m(i, j)$ and $o(i, j)$. The detailed generation processes of the master share and the ownership share are shown in (7)-(8).

$$m(i, j) = \begin{cases} \begin{bmatrix} 1, 0 \\ 0, 1 \end{bmatrix}, & \text{if } F(i, j) = 1; \\ \begin{bmatrix} 0, 1 \\ 1, 0 \end{bmatrix}, & \text{otherwise} \end{cases} \quad (7)$$

$$o(i, j) = \begin{cases} \begin{bmatrix} 1, 0 \\ 0, 1 \end{bmatrix}, & \text{if } m(i, j) = \begin{bmatrix} 1, 0 \\ 0, 1 \end{bmatrix}, W(i, j) = 1; \\ \begin{bmatrix} 0, 1 \\ 1, 0 \end{bmatrix}, & \text{if } m(i, j) = \begin{bmatrix} 1, 0 \\ 0, 1 \end{bmatrix}, W(i, j) = 0; \\ \begin{bmatrix} 0, 1 \\ 1, 0 \end{bmatrix}, & \text{if } m(i, j) = \begin{bmatrix} 0, 1 \\ 1, 0 \end{bmatrix}, W(i, j) = 1; \\ \begin{bmatrix} 1, 0 \\ 0, 1 \end{bmatrix}, & \text{if } m(i, j) = \begin{bmatrix} 0, 1 \\ 1, 0 \end{bmatrix}, W(i, j) = 0 \end{cases} \quad (8)$$

where $1 \leq i \leq 24$ and $1 \leq j \leq 24$, $W(i, j)$ is the pixels of watermark information.

Step 9. Store the generated O and into the certificate authority (CA) databases for watermark-recovery.

2.2 Watermark-recovery phase

Step 1. Content-based feature f' of the queried medical image is extracted following the Steps 1-7 of watermark-sharing phase. Then, the queried master share M' is generated following the Step 8 of watermark-sharing phase.

Step 2. Stack the queried master shares M' with the ownership shares stored in CA databases to construct intermediate matrices S as shown in Table 1.

Step 3. Recover the watermark information W' from S as shown in (9).

$$W'(i, j) = \begin{cases} 1, & \text{if } \sum s_{i,j}(x, y) \geq 2; \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

where $s_{i,j}(x, y)$ are non-overlapping 2×2 blocks of S , $1 \leq i \leq 24$, $1 \leq j \leq 24$, $1 \leq x \leq 2$, and $1 \leq y \leq 2$.

Step 4. The recovered watermark is compared with the original watermark W by calculating their bit error rate (BER) to identify the authenticity and copyright of the queried medical image, as shown in (10).

$$BER = \frac{\sum W(i, j) \oplus W'(i, j)}{m_w \times m_w} \quad (10)$$

where $W'(i, j)$ and $W(i, j)$ represent the pixels of the recovered and original watermarks, respectively, \oplus denotes the exclusive-or (XOR) operation, and $m_w \times m_w$ is the size of the watermark. In our study, m_w is set to 24.

3. EXPERIMENT

3.1 Experiment setting up

Our experiments are conducted on a database consisting of 200 different medical images. These medical images include 40 Computed Tomography (CT) images, 40 magnetic resonance images (MRI), 40 Ultrasound images, 40 X-ray images, which are collected from Internet, and 40 fundus images from the open database DRIVE¹⁵. 20 common attacks with different parameters, as shown in Table 2, are performed on the database and a total of 4000 attacked medical images are generated as queried images for our experiments.

Table 2. Types of attacks with different parameters.

Attack Type	Parameters
Gaussian blurring (GB)	window=3×3; variance=0.5, 1
Gamma transform (GT)	$\gamma=0.8, 1.2$
Brightness adjustment (BA)	-20%, +20%
Contrast adjustment (CA)	-20%, +20%
Gaussian noise addition (GN)	Mean=0; variance=0.0003, 0.0005
JPEG compression (JC)	Compression quality 90%, 70%
Resizing (RS)	0.8, 1.2
Crop (CR) from image edges	10%, 15%
Rotation (RT)	45°, 90°
Flip (FL)	Horizontal, Vertical

3.2 Evaluation of the performance for authentication and copyright identification

To evaluate the watermarking distinguishability for authentication and copyright identification, we first calculate the inter-BERs (BERs between the watermark recovered by stacking the ownership share with master share of a same medical image and watermark recovered by stacking the ownership share with master shares of different medical images) by using DRZW and compare them with the those by using Seenivasagam's scheme¹¹, which is one of the latest zero-watermarking scheme for medical images. The distinguishability is considered to be stronger if the inter-BERs are larger. The average and minimum values of inter-BERs in by using DRZW are 0.4636 and 0.1111, respectively. These values are much larger than those by using Seenivasagam's scheme, which are 0.2007 and 0, respectively. These results demonstrated that the distinguishability of Seenivasagam's scheme for medical images is insufficient whereas the distinguishability of our proposed DRZW for medical images is much stronger. Therefore, DRZW outperforms Seenivasagam's scheme in terms of accuracy. The reason for this result is that the feature extracted in DRZW is based on the CLBP_S and CLBP_M images, which have strong distinguishability for texture classification.

After that, to evaluate the watermarking robustness for authentication and copyright identification, we calculate the mean intra-BERs (the BERs between the watermarks recovered from original and attacked medical images) by using DRZW and Seenivasagam's scheme. The robustness is considered to be stronger if the mean intra-BERs are smaller. The comparison result is listed in Table 3.

As shown in Table 3, although average value of mean intra-BERs by using DRZW is almost the same with that by using Seenivasagam's scheme, which are 0.0723 and 0.0815 respectively, the mean intra-BERs by using DRZW are smaller than those by using Seenivasagam's scheme under geometric attacks such as cropping, rotation and flipping attacks. The result demonstrates that the robustness of DRZW against geometric attacks is stronger than that of Seenivasagam's scheme. The reason for this result is the utilizing of the CLBP_S and CLBP_M images, which have strong robustness against geometric attacks, and the concentric-ring-based partition method, which further enhances the robustness against geometric attacks.

Finally, to evaluate the performances of these two schemes in terms of both accuracy and reliability, their false negative rates P_{fn} s are compared under the fixed false positive rates P_{fp} s. P_{fp} and P_{fn} are defined by (11)-(12).

Table 3. Evaluation of watermarking robustness for authentication and copyright identification.

Attacks	Mean intra-BER	
	Seenivasagam's scheme ¹¹	DRZW
GB 0.5	0.0043	0.0446
GB 1	0.0105	0.0798
GT 0.8	0.0179	0.0575
GT 1.2	0.0773	0.0565
BA -20%	0.0147	0.0643
BA +20%	0.0182	0.0594
CA -20%	0.1285	0.0665
CA +20%	0.1955	0.1108
GN 0.0003	0.1245	0.1343
GN 0.0005	0.1245	0.1530
JC 90%	0.0186	0.0966
JC 70%	0.1153	0.1116
RS 0.8	0.0088	0.0437
RS 1.2	0.0058	0.0319
CR 10%	0.1094	0.0544
CR 15%	0.1631	0.0935
RT 45°	0.1744	0.0887
RT 90°	0.1558	0.0641
FL Horizontal	0.0736	0.0061
FL Vertical	0.0899	0.0290
Average	0.0815	0.0723

$$P_{fp} = \frac{N_{fp}}{N_{dis}} \quad (11)$$

$$P_{fn} = \frac{N_{fn}}{N_s} \quad (12)$$

where N_{fp} is the number of different medical image pairs when inter-BER of their recovered watermarks is smaller than a threshold T , N_{dis} is the true number of different medical image pairs, N_{fn} is the number when intra-BERs between the watermarks recovered from original and attacked medical images is larger than the threshold T , and N_s is the true number of pairs of original and attacked medical images.

The performance is considered to be better if the P_{fn} s are smaller under the fixed P_{fp} s. In Seenivasagam's scheme, the redefined threshold T is set to 0.0129 by fixing the P_{fp} to 6.33%. The P_{fp} is not fixed to a lower value because all the inter-BERs of these 6.33% images are equal to 0. In our proposed DRZW, T is set to 0.3194 and 0.2205 by fixing the P_{fp} s to 6.33% and 1.00%, respectively. The evaluation result is listed in Table 4.

Table 4. Evaluation of both accuracy and reliability for authentication and copyright identification.

Attacks	P_{fn}		
	Seenivasagam's scheme ¹¹ ($P_{fp}=6.33\%$)	DRZW ($P_{fp}=6.33\%$)	DRZW ($P_{fp}=1.00\%$)
GB 0.5	27.50%	0.00%	0.00%
GB 1	54.00%	0.00%	0.00%
GT 0.8	45.00%	0.00%	0.00%
GT 1.2	89.00%	0.00%	0.00%
BA -20%	35.50%	0.00%	0.00%
BA +20%	44.00%	1.00%	4.00%
CA -20%	75.50%	0.00%	0.00%
CA +20%	95.50%	0.50%	7.50%
GN 0.0003	75.00%	1.00%	6.00%
GN 0.0005	75.00%	2.00%	10.50%
JC 90%	65.50%	0.00%	0.00%
JC 70%	81.50%	0.00%	0.50%
RS 0.8	45.50%	0.00%	0.00%
RS 1.2	35.50%	0.00%	0.00%
CR 10%	100.00%	0.00%	0.00%
CR 15%	100.00%	0.00%	1.50%
RT 45°	99.50%	0.00%	2.50%
RT 90°	95.00%	0.00%	3.00%
FL Horizontal	77.50%	0.00%	0.00%
FL Vertical	77.50%	0.00%	0.00%
Average	69.68%	0.23%	1.75%

As shown in Table 4, all the P_{fn} s of DRZW are *much lower* than those of Seenivasagam's scheme with their average values as 0.23% and 69.68% when the P_{fp} s are 6.33%. In addition, all the P_{fn} s of DRZW are still smaller than 10.50% when the P_{fp} is 1.00%, with the average value as 1.75%. Especially, the P_{fn} s of Seenivasagam's scheme under cropping and rotation attacks are larger than 95.00% when the P_{fp} is 6.33% whereas the P_{fn} s of DRZW are equal to 0.00% when the P_{fp} is 6.33% and still smaller than 3.00% even when the P_{fp} is 1.00%. The result demonstrates that the accuracy and reliability of DRZW is much stronger than those of Seenivasagam's scheme, especially against cropping and rotation attacks. The reasons for this result are as follows: 1) The feature extracted in DRZW is based on the CLBP_S and CLBP_M images, which ensures both the strong distinguishability for medical images and the strong robustness against flipping, rotation, flipping, contrast adjustment and brightness adjustment. 2) All the input images are resized and smoothed in DRZW, which enhances the robustness against resizing and noise addition. 3) The concentric-ring-based partition method is utilized in DRZW, which further enhances the robustness against cropping, rotation and flipping.

4. CONCLUSIONS

In this study, a discriminative and robust zero-watermarking (DRZW) scheme for medical images is proposed. The experiment results on 200 medical images of 5 different types have demonstrated that DRZW ensures sufficient distinguishability for medical image and robustness against various attacks. Therefore, DRZW can better address the

authentication and copyright identification issues compared with existing zero-watermarking schemes for medical images.

ACKNOWLEDGEMENTS

This research is supported by the National Natural Science Foundations of China (61602527, 61573380), Hunan Provincial Natural Science Foundation of China (2017JJ3416) and China Postdoctoral Science Foundation (2017M612585). The authors would like to thank for the supports from Dr. Leng Dong and Dr. Qiang Tang of Loughborough University, UK.

REFERENCES

- [1] Gunjal, B. L. and Mali, S. N., "ROI based embedded watermarking of medical images for secured communication in telemedicine," *Int. J. Comput. Commun. Eng.* 6(48), 293-298 (2012).
- [2] Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A. and Bhat, G. M., "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimed. Tools Appl.* 76(8), 10599-10633 (2017).
- [3] Memon, N. A., Keerio, Z. A. and Abbasi, F., "Dual Watermarking of CT Scan Medical Images for Content Authentication and Copyright Protection," *Int. Conf. Multi Topic*, 173-183 (2013).
- [4] Pandey, R., Singh, A. K., Kumar, B. and Mohan, A., "Iris based secure NROI multiple eye image watermarking for teleophthalmology," *Multimed. Tools Appl.* 75(22), 14381-14397 (2016).
- [5] Priyanka, S. M., "Region-based hybrid medical image watermarking for secure telemedicine applications," *Multimed. Tools Appl.* 76(3), 3617-3647 (2016).
- [6] An, L., Gao, X., Yuan, Y., Tao, D., Deng, C. and Ji, F., "Content-adaptive reliable robust lossless data embedding," *Neurocomputing* 79, 1-11 (2012).
- [7] An, L., Gao, X., Li, X., Tao, D., Deng, C. and Li, J., "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Trans. Image Process.* 21(8), 3598-3611 (2012).
- [8] Lei, B., Tan, EL., Chen, S., Ni, D., Wang, T., and Lei, H., "Reversible watermarking scheme for medical image based on differential evolution," *Expert Syst. Appl.* 41(7), 3178-3188 (2014).
- [9] Dong, C., Zhang, H., Li, J., and Chen, Y. W., "Robust zero-watermarking for medical image based on DCT," *Int. Conf. Computer Sciences and Convergence Information Technology (ICCIT)*, 900-904 (2012).
- [10] Vellaisamy, S. and Ramesh, V., "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud," *Comput. Math. Method. M.* 2013(4), 1-16(2013).
- [11] Vellaisamy, S. and Ramesh, V., "Inversion attack resilient zero-watermarking scheme for medical image authentication. *IET Image Processing*," *IET Image Process.* 8(12), 718-727 (2014).
- [12] Hu, M. K., "Visual pattern recognition by moment invariants," *IEEE Trans. Inform. Theory* 8(2), 179-187 (1962).
- [13] Guo, Z., Zhang, L. and Zhang D., "A completed modeling of local binary pattern operator for texture classification," *IEEE Trans. Image Process.* 19(6), 1657-1663 (2010).
- [14] Naor, M. and Shamir, A., "Visual cryptography," *Advances in Cryptology-EUROCRYPT94*. Springer Berlin Heidelberg, 1-12 (1994).
- [15] Staal, J., Abramoff, M. D., Niemeijer, M., Viergever, M. A. and Van Ginneken, B., "Ridge-based vessel segmentation in color images of the retina," *IEEE Trans. Med. Imaging* 23(4), 501-509 (2004).