Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **1**, January **2017**

A Lossless Fingerprinting-Watermarking Hybrid Scheme for Digital Right Management of Fundus Images

Jingyu Du, Beiji Zou, Xiyao Liu*, Fangfang Li and Huanxi Zhao

School of Information Science and Engineering, Central South university, Changsha, China
Center for Ophthalmic Imaging Research, Central South university, Changsha, China
Center for Information and Automation of China Nonferrous Metals
Industry Association, Changsha, China
jingyudu@csu.edu.cn; bjzou@csu.edu.cn;
*Corresponding Author: lxyzoewx@csu.edu.cn

Received March, 2016; revised June, 2016

Abstract. *Fundus images are critical data to record visual health and play an important role in the diagnosis of ocular diseases. Therefore, protecting the copyrights of those valuable data becomes an important issue in telemedicine applications where fundus images are exchanged across different hospitals and medical institutes. In this paper, a novel lossless fingerprinting-watermarking hybrid scheme is proposed for the digital right management (DRM) of fundus images. In our hybrid scheme, the features with strong distinguishability and robustness are extracted from fundus images as fingerprints for content-based retrieval. And then the relationships between the fingerprints and the watermark are established following the zero watermarking manner for the copyright identification. Our experiment results demonstrate that the proposed scheme can identify copyright ownership of different fundus images precisely and reliably without ownership dispute or image distortion.*
Keywords: Fundus image, Digital right management, Fingerprinting-watermarking hybrid scheme, Telemedicine.

1. **Introduction.** Fundus images, which contains large amounts of retinal features including optic disc, fovea, blood vessels etc., are critical and valuable for the diagnosis and research ocular diseases such as glaucoma, diabetic retinopathy and age-related macular degeneration [1, 2, 3, 4, 5]. With the development of telemedicine systems, the exchange of medical images, including fundus images, has become the current trend for improving clinical interpretation, diagnosis and research [6]. However, those exchanging processes may cause copyright disputes of fundus images, which will bring serious losses to their owners. Therefore, the digital rights management (DRM) of fundus images has become an important issue in those telemedicine services.

Digital watermarking is an effective technique for the security protection of digital content [7, 8, 9, 10]. There are three main categories of watermarking schemes for the security protection of medical images, which are the region of interest (ROI) lossless watermarking [11, 12], reversible watermarking [13, 14, 15] and zero watermarking [16, 17, 18, 19, 20].

ROI lossless watermarking schemes embed watermark into the transform domain of the region of non-interest (RONI) to avoid distortions of ROI [11, 12]. However, these

methods are not suitable for the DRM of fundus images due to two reasons. On one hand, the automatic segmentation methods of ROIs in fundus images are fragile to image attacks whereas the manual or interactive segmentation methods are inefficient. On the other hand, the distortions of RONI still have slight impacts on the medical diagnosis, which need to be further improved.

Recently, several robust reversible watermarking schemes [13, 14, 15] have been proposed and applied to protect medical images. Reversible watermarking schemes can ensure that the medical images are recovered losslessly and their diagnosis value are unchanged after the watermark extraction. Simultaneously, they can overcome the disadvantages caused by the ROI segmentation in the ROI lossless watermarking schemes. Therefore, the reversible watermarking schemes are more suitable for protecting medical images than the ROI lossless ones. However, there are still several disadvantages when they are utilized for the DRM of fundus images. For one thing, the copyright have to be identified before medical diagnosis because the image for diagnosis can be recovered only when the watermark has been extracted, which is inconvenient. For another, the reversible watermarking schemes can only offer one-off copyright identification because there is no copyright information any more in the entirely recovered image, which limits the applicability of reversible watermarking schemes.

Those above-mentioned disadvantages of reversible watermarking schemes can be overcome in the zero watermarking schemes [16, 17, 18, 19, 20]. In these schemes, the mapping relationships between copyright information and features of medical images are generated for DRM. Since the copyright information is not directly embedded into the medical images, the distortions can be completely avoided in the medical images. Additionally, the robustness from the image features can be inherited for the reliable DRM. However, the existing zero watermarking schemes are still not suitable for DRM of fundus images mainly due to the following two reasons. Firstly, the fundus images of different patients are similar to each other in some extent and thus the distinguishability of the features must be ensured for the precise copyright identification. Unfortunately, most of zero watermarking schemes [16, 17, 18, 19] only focus on the robustness of the extracted features but rarely consider or analyze their distinguishability. Secondly, all those schemes are under the premise that the relevant mapping relationship of a particular image has been already known before the copyright identification, otherwise the copyright identification would fail. Because the number of fundus images is usually quite large in a medical database for medical diagnosis and research, it is difficult for zero watermarking schemes to search for the right mapping relationship relevant to a particular fundus image without a efficient retrieval method.

The schemes for content-based retrieval of images (CBIR) [21, 22, 23, 24] have the potential to overcome the disadvantages of zero-watermarking since these schemes have strong distinguishability and efficient content-based retrieval methods. In these schemes, the content-based features with strong distinguishability and robustness are extracted as the fingerprints to index and retrieve images. However, the CBIR schemes do not utilize any copyright information, which may cause undesired copyright disputes when they are directly utilized for the DRM of fundus images.

Fortunately, it can be found that the advantages of the zero watermarking and fingerprinting schemes are complementary. To combine the advantages of them, a fingerprinting-watermarking hybrid scheme for DRM of videos has been proposed [25]. In this scheme, a suspicious video is firstly retrieved following the fingerprinting manner and then its copyright information is identified following the zero watermarking manner. However, the copyright identification is based on the features of watermark images rather than directly using the watermark images itself, which weakens the distinguishability. Therefore, it

needs to be further improved for the DRM of fundus images. In addition, the fingerprints designed for videos cannot be directly applied for the DRM of fundus images, and suitable fingerprints for fundus image should be designed.

In this paper, a lossless hybrid scheme for the DRM of fundus images is proposed. The key points of our proposed scheme are as follows.

1) To the best of our knowledge, it is the first work for the DRM of fundus images.

2) The hybrid framework in [25] is improved for the DRM of fundus images. The copyright identification in our proposed scheme is directly based on the watermark images instead of their features to enhance the distinguishability.

3) The weights of frequency components of 2D-DCT domain are set different to generate suitable fingerprints for the effective trade-off between distinguishability and robustness.

4) The size of the fingerprints is set much larger than that in [25] to further enhance the precision of the content-based retrieval.

2. **Background.** In this section, the concepts of two dimensional discrete cosine transform (2D-DCT) and visual secret sharing (VSS) scheme are briefly described.

2.1. **Two dimensional discrete cosine transform.** The 2D-DCT is often used in signal and image processing, because it has an important property, that is, most of the signal information tends to be concentrated in a few low-frequency components of the 2D-DCT. The transform formula of 2D-DCT is as follows:

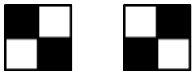
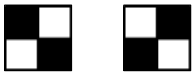
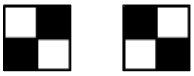
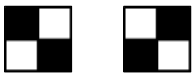
$$F(u,v) = \begin{cases} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y), & u=0, v=0 \\ \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2y+1)v\pi}{2N}, & u=0, v=1,2,...,N-1 \\ \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2x+1)u\pi}{2N}, & u=1,2,...,N-1, v=0 \\ \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}, & u=1,2,...,N-1, v=1,2,...,N-1 \end{cases} \tag{1}$$

where $f(x,y)$ is the function of time domain, the variables x and y represent the row and the column respectively. $F(u,v)$ is cosine transform coefficient of the frequency domain, the variables u and v represent the row and the column respectively.

2.2. **Visual secret sharing scheme.** The concept of (m,n) VSS scheme (where $m \leq n$) is proposed by M. Naor and A. Shamir [26]. This scheme splits a binary image into n different shares. The image can be recovered from k shares when $k \geq m$, and any $k-1$ shares give absolutely no information about the image. The (2, 2) VSS scheme is used to generate the master share and ownership share in this paper. A binary image with size $M \times N$ is divided into two shares with size $2M \times 2N$. Each pixel of the binary image is transformed into two 2×2 blocks, and each block belongs to the corresponding share image. The two blocks transformed from a white pixel are the same while those from a black pixel are complementary. The concept of (2, 2) VSS scheme is show in table 1.

3. **Proposed scheme.** The proposed scheme consists of two phases: the copyright registration phase and the retrieval and copyright identification phase. The copyright registration phase is shown in Fig.1, in which a fingerprint database and an ownership database are established according to the fundus images and their relative watermarks. Once a suspicious fundus image is found, a content-based retrieval operation will be performed in the retrieval and copyright identification phase. If the retrieval succeeds, the suspicious

TABLE 1. Concept of (2,2) VSS scheme

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

fundus image is likely to be an illegal copy. In this case, the copyright identification is executed. The retrieval and copyright identification phase is shown in Fig.2.

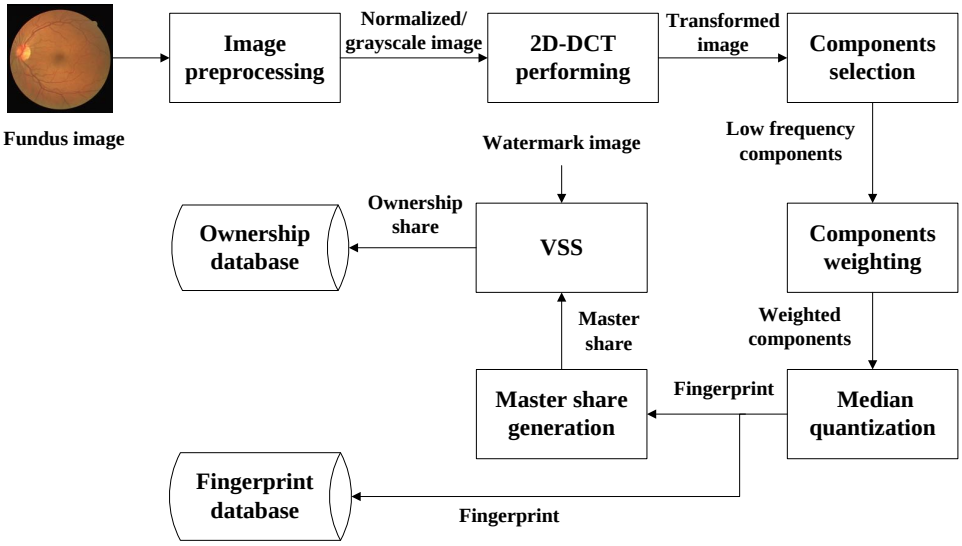


FIGURE 1. Copyright registration phase

3.1. **The copyright registration phase.** In order to avoid the copyright dispute, copyright registration is required. The registration procedure is as follows:

Step1. Normalize the size of the fundus image to 512×512. Then convert the image into grayscale image.

Step2. Perform the 2D-DCT on the normalized grayscale image to obtain the transform-domain image U.

Step3. Since the low-frequency components of transform domain image determine the outline of original image. Select the low frequency components of transformed image U as a matrix X. The selection method as Eq. 2.

$$X(i,j) = U(i+1, j+1) \tag{2}$$

where $1 \leq i, j \leq 32$, $X(i,j)$ is the element of X.

Step4. partition the matrix X as Eq. 3.

$$\begin{aligned} &A(i,j) = X(i,j), 1 \leq i, j \leq 16 \\ &B(i,j-16) = X(i,j), 1 \leq i \leq 16, 17 \leq j \leq 32 \\ &C(i-16,j) = X(i,j), 17 \leq i \leq 32, 1 \leq i \leq 16 \\ &D(i-16,j-16) = X(i,j), 17 \leq i, j \leq 32 \end{aligned} \tag{3}$$

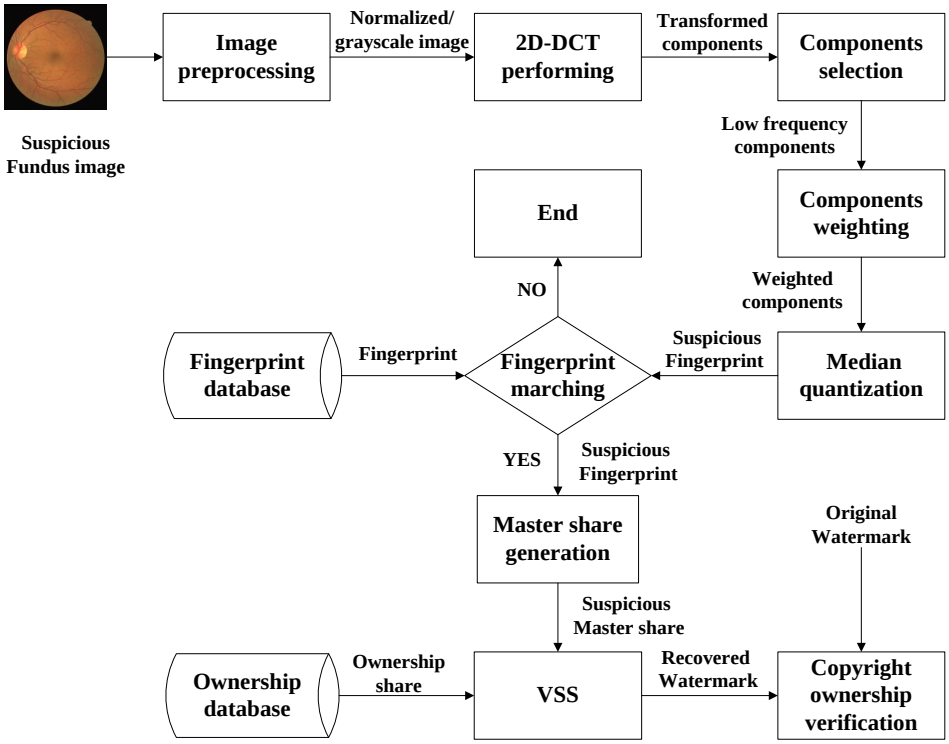


FIGURE 2. Retrieval and copyright identification phase

Step5. To generate suitable fingerprint with an effective tradeoff between robustness and distinguishability, different weights are set to different areas of the matrix X. The weights of the elements in A where the low frequency part of X are set to a higher value ($w_A = 2$), whereas those of the elements in D which is the high frequency part of X are set to zero ($w_D = 0$) to strengthen the robustness of fingerprint. The weights of the elements in B and C which belong to the middle frequency of X are retained ($w_B = w_C = 1$) because they contain more details of the image.

Step 6. Generate a new matrix X' following the way of weights distribution in Step 5.

$$X'(i,j) = \begin{cases} A(i,j), & 1 \le i,j \le 16 \\ B(i,j-16), & 1 \le i \le 16, 17 \le j \le 32 \\ C(i-16,j), & 17 \le i \le 32, 1 \le j \le 16 \\ A(i-16,j-16), & 17 \le i,j \le 32 \end{cases} \tag{4}$$

Step7. Convert the matrix X' into a vector I. Generate the fingerprint *fin* based on the median quantization as Eq. 5.

$$fin(t) = \begin{cases} 1, & I(t) \ge \varepsilon \\ 0, & I(t) < \varepsilon; \end{cases} \tag{5}$$

where $1 \le t \le 1024$, ε is the median of vector I, that is weighted median of the matrix X'.

Step8. Store the fingerprint *fin* into the fingerprint database to provide the basis for retrieval.

Step9. Rearrange the binary fingerprint *fin* into a 32×32 matrix G.

Step10. Transform each element $G(i,j)$ in matrix G into a 2×2 matrix $M_{i,j}$, The transformation rule is shown in Eq.6.

$$M_{i,j} = \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & G(i,j) = 1 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & G(i,j) = 0; \end{cases} \tag{6}$$

In this manner, a 64×64 matrix M, that is the master share, is generated from the matrix G.

Step11. Generate the ownership share O, following the (2,2) VSS mapping rule:

$$O_{i,j} = \begin{cases} M_{i,j}, & W(i,j) = 1 \\ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - M_{i,j}, & W(i,j) = 0 \end{cases} \tag{7}$$

where $W(i,j)$ is the pixel of the watermark image and $1 \leq i,j \leq 32$.

Step12. Store the ownership share O into the ownership database to provide the basis for copyright identification.

3.2. **The retrieval and copyright identification phase.** For the suspicious fundus images, the retrieval and copyright identification phase is executed. The procedures of this phase are given below:

Step1. Extract the fingerprint *fin'* of the suspicious fundus image following the methods in the copyright registration phase.

Step2. Find the fingerprint *fin* which is most similar to the suspicious fingerprint *fin'* from the fingerprint database according to their hamming distance.

Step3. Compare the hamming distance between *fin* and *fin'* with the predefined threshold T. If the distance smaller than T, the suspicious fundus image is considered to be a illegal copy and Step 4 is performed to verify its ownership. Otherwise, the suspicious fundus image is seen as legitimate and the whole procedure is finished.

Step4. Obtain the relevant ownership share O from the ownership database based on the fingerprint *fin*.

Step5. Rearrange the suspicious fingerprint *fin'* into a 32×32 matrix G'.

Step6. Generate the suspicious master share M' following the same rule in the copyright registration phase.

Step7. Obtain the copyright information matrix W' by stacking the suspicious master share M' with the relevant ownership O based on the (2,2) VSS scheme.

Step8. Divide the copyright information matrix W' into 1024 non-overlapping 2×2 blocks $W'_{i,j}$, where $1 \leq i,j \leq 32$.

Step9. Obtain the suspicious watermark image by the following process:

$$\widetilde{W}(i,j) = \begin{cases} 0, & \sum\limits_{x}\sum\limits_{y} W'_{i,j}(x,y) < 2 \\ 1, & \sum\limits_{x}\sum\limits_{y} W'_{i,j}(x,y) \geq 2 \end{cases} \tag{8}$$

where $\widetilde{W}(i,j)$ is the pixel of the suspicious watermark, $1 \leq i,j \leq 32$ and $1 \leq x,y \leq 2$.

Step10. Calculate the normalized correlation (NC) to measure the similarity between the extracted watermark and the original watermark to identify the ownership of the

fundus images. NC is defined as

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\overline{W(i,j)\bigoplus\widetilde{W}(i,j)}}{m \times n} \tag{9}$$

where W and $\widetilde{W}$ represent the original watermark and the recovered watermark respectively, $\bigoplus$ denotes the exclusive-or (XOR) operation, $n \times m$ is the size of watermark and $n, m = 32$.

4. **Experimental results.**

4.1. **Experimental settings.** In this section, several experiments are carried out to assess the performance of the proposed scheme. 150 fundus images which are selected from public databases DRIVE (Digital Retinal Images for Vessel Extraction) [27] and our own database are used for experimentation. A binary logo of size 32×32 is used as the watermark image. The robustness and distinguishability of the proposed scheme is estimated by performing various image processing attacks. All these attack simulations are implemented on Matlab platform. The attacks are described as follows:

Gaussian Blurring: The Gaussian blur with 9×9 window and 15×15 window are applied.

Contrast adjustment: The contrast is adjusted by increasing and decreasing 30% and 50% respectively.

Brightness adjustment: The brightness is increased and decreased by 30% and 50% respectively.

Filtering: Average filter and median filter with 9×9 window and 15×15 window are applied.

Gaussian noise: Gaussian noise is added and its parameters are set to 10% and 30% respectively.

Salt and pepper noise: Salt and pepper noise is also added and the noise density is set to 0.03 and 0.05 respectively.

Resizing: The fundus images are resized. The scale factors of resizing are set to 0.5 and 0.2.

Rotation: The fundus images are rotated by 1° and 2°.

JPEG compression: JPEG compression is implemented with quality factor 70% and 50%.

The results of the experiment consist of three aspects: the retrieval performance, the copyright identification performance and qualitative analysis. The details of experiments are described below.

4.2. **The evaluation of Retrieval.** Firstly, a pre-defined threshold T should be determined. Once the smallest hamming distance between the fingerprint of suspicious fundus image and that of fundus image in our database is smaller than T, the suspicious fundus image is confirmed to be a copy. T can be determined by either the false positive rate P_{fp} or the false negative rate P_{fn}. P_{fp} presents a probability of identifying the different images into the same image and can illustrate the distinguishability of the fingerprint, whereas P_{fn} presents a probability of identifying the same image into different images and can manifest the robustness of the fingerprint. P_{fp} and P_{fn} is defined in Eq.10 and Eq.11 respectively:

$$P_{fp} = \frac{N_{fp}}{N_{td}} \tag{10}$$

$$P_{fn} = \frac{N_{fn}}{N_{ts}} \tag{11}$$

where N_{fp} is the number of fingerprint pairs whose hamming distance is smaller than T but they are from two different images. N_{td} is the true number of different fundus images pairs and its value is 11175 which is the number of the generated different image pairs from the 150 fundus images in this paper. N_{fn} is the number of fundus image pairs whose hamming distance is larger than T but they are from the same fundus images. N_{ts} is the true number of same fundus image pair and its value is 150.

In our experiment, T is determined by setting P_{fp} to 1.5% and P_{fn} are calculated to evaluate the retrieval performances of the fingerprints under different attacks. The experiment results are show in Table 2. As can be seen from the table 2, all the P_{fn}

Table 2. Retrieval performance evaluation

Attacks	Parameter	P_{fn} under different attacks($P_{fp} = 1.5\%$)	Parameter	P_{fn} under different attacks($P_{fp} = 1.5\%$)
Caussian blurring	9×9	0%	15×15	0%
Contrast adjustment	−30%	0%	+30%	0.67%
	−50%	0%	+50%	14.67%
Brightness adjustment	−30%	0%	+30%	0%
	−50%	1.33%	+50%	0%
Average filtering	9×9	0%	15×15	0%
Median filtering	9×9	0%	15×15	0%
Gaussian noise	10%	0%	30%	15.33%
Salt and pepper noise	0.03	0%	0.05	0%
Rotation	1°	0%	2°	12.00%
Cropping(3%)	Left	0%	Right	0%
	Up	2.67%	Down	0.67%
Cropping(5%)	Left	0%	Right	0%
	Up	8.67%	Down	1.33%
Resizing	0.5	0%	0.2	0.67%
JPEG compression	70%	0%	50%	0%

of the proposed scheme are below 15.33% under different attacks and many of them are merely 0%, which demonstrates the retrieval phase in our proposed scheme performs well and the fingerprint is robust and distinguishable. The reason is that the low-frequency components of the 2D-DCT are well considered and the different weights are assigned to the different components. Therefore, the ownership share relevant to the fingerprint can be obtained precisely in the copyright identification phase according to the retrieval result even under various image processing attacks.

4.3. **The evaluation of copyright identification.** In this experiment, 150 fundus images suffered various attacks and the mean NC values between the recovered watermark and the original watermark are calculated in Table 3. The experimental results show that almost all the mean NC values are close to 1 and the minimum one is still as large as 0.8947, which indicates that the copyright identification is sufficiently robust against various image processing attacks.

To further demonstrate our effectiveness of the proposed scheme, we compare the performance of the proposed scheme with the scheme in [20]. The comparison results under common image processing attacks show in table 4. From the table, it can be seen that all the results of our scheme are not worse than those in [20], particularly the NC values

Table 3. Robustness performance evaluation

Attacks	Parameter	Mean NC	Parameter	Mean NC
Caussian blurring	9×9	0.9948	15×15	0.9949
Contrast adjustment	-30%	0.9827	$+30\%$	0.9336
	-50%	0.9717	$+50\%$	0.8947
Brightness adjustment	-30%	0.9583	$+30\%$	0.9671
	-50%	0.9409	$+50\%$	0.9420
Average filtering	9×9	0.9895	15×15	0.9811
Median filtering	9×9	0.9865	15×15	0.9761
Gaussian noise	10%	0.9571	30%	0.8992
Salt and pepper noise	0.03	0.9531	0.05	0.9427
Rotation	1°	0.9449	2°	0.9010
Cropping(3%)	Left	0.9776	Right	0.9767
	Up	0.9538	Down	0.9618
Cropping(5%)	Left	0.9503	Right	0.9554
	Up	0.9430	Down	0.9482
Resizing	0.5	0.9954	0.2	0.9225
JPEG compression	70%	0.9874	50%	0.9772

under blurring, filtering, resizing and JPEG compression attacks are much higher than those in [20], which indicates that our proposed scheme outperforms their work in term of robustness.

Table 4. Comparison of NC

Attacks	Parameter	V. Seenivasagm scheme [20]	Proposed scheme
Caussian blurring	9×9	0.8974	0.9948
Contrast adjustment	$+50\%$	0.8935	0.8947
Average filtering	9×9	0.8949	0.9895
Median filtering	9×9	0.8946	0.9865
Gaussian noise	30%	0.8955	0.8992
Resizing	0.5	0.7526	0.9954
JPEG Compression	50%	0.8879	0.9772

4.4. **Qualitative comparisons.** In this experiment, the proposed scheme are compared with the ROI-lossless watermarking [11, 12], the reversible watermarking [13, 14], the zero-watermarking [18, 19, 20] and the fingerprinting schemes [22, 23] in terms of six aspects, which are the effects on images, the durability of identification, the precision of identification, the reliability of identification, the efficiency of retrieval scheme and the utilization of copyright information. The appropriateness for the DRM of fundus image is demonstrated in the first aspect. The performances for the DRM of fundus image is reflected from the second aspect to the fifth aspect. The capability to avoid the possible copyright dispute is manifested in the last aspect. The results are listed in Table 5.

As shown in Table 5, our proposed scheme outperforms these schemes. Compared with the ROI-lossless watermarking schemes, the whole procedure of our proposed scheme is

TABLE 5. Qualitative comparisons

Schemes	Effects on images	Durability of identification	Precision of identification	Reliability of identification	Retrieval method	Copyright information
S. A. Parah[11]	ROI-lossless	Durable	Good	Good	None	Utilized
N. Solanki[12]	ROI-lossless	Durable	Good	Good	None	Utilized
L. An[13]	Lossless	One-off	Good	Moderate	None	Utilized
B. Lei[15]	Lossless	One-off	Good	Good	None	Utilized
J. Waleed[18]	Lossless	Durable	Not applied	Good	None	Utilized
V. Seenivasagam[19]	Lossless	Durable	Not applied	Good	None	Utilized
V. Seenivasagam[20]	Lossless	Durable	Good	Good	None	Utilized
L. Liu[22]	Lossless	Durable	Good	Good	Effective	Not utilized
F. Zou[23]	Lossless	Durable	Good	Good	Effective	Not utilized
Proposed	Lossless	Durable	Good	Good	Effective	Utilized

lossless, which satisfies the requirements of accurate diagnosis. Compared with the reversible watermarking schemes, identification of our scheme can be executed multiple times during the medical care applications, which protects the copyright of fundus images durably. Compared with the zero-watermarking schemes, both the distinguishability and the robustness of content-based features are ensured and an effective content-based retrieval is applied in our proposed scheme, which ensures that a particular fundus image with its relevant ownership share can be retrieved precisely and the copyright ownership can also be identified reliably. Compared with the fingerprinting schemes, the copyright ownership information is utilized in our proposed scheme, which ensures that the copyright ownership can be identified explicitly to avoid the possible copyright dispute.

5. **Conclusion.** In this paper, a lossless hybrid scheme for the DRM of fundus images is proposed. Our analytic and experimental results have demonstrated that our proposed scheme has some advantages over other existing schemes. Firstly, the whole procedure of our proposed scheme is lossless, which can satisfy the requirement of accurate diagnosis. Secondly, the copyright protection of fundus images is durable, which can avoid one-off copyright identification. Thirdly, the different fundus images can be distinguished precisely though they are quite similar to each other. Finally, the copyright ownership can be identified reliably without dispute.

Acknowledgment. This work is supported by the National Nature Science Foundations of China (61573380).

REFERENCES

[1] J. Cheng, J. Liu, Y. Xu, F. Yin, D. W. K. Wong, N. M. Tan, D. Tao, C. Y. Cheng, T. Aung and T. Y. Wong, Superpixel classification based optic disc and optic cup segmentation for glaucoma screening, *IEEE Trans. on Medical Imaging*, vol. 32, no. 6, pp. 1019-1032, 2013.

[2] C. Zhu, B. Zou, R. Zhao, J. Cui, X. Duan, Z. Chen and Y. Liang, Retinal vessel segmentation in colour fundus images using Extreme Learning Machine, *Computerized Medical Imaging and Graphics*, 2016.

[3] C. Zhu, B. Zou, Y. Xiang, J. Cui and H. Wu, An Ensemble Retinal Vessel Segmentation Based on Supervised Learning in Fundus Images, *Chinese Journal of Electronics*, vol. 25, no. 3, pp. 503-511, 2016.

[4] O. Faust, R. Acharya, E. Ng, K. H. Ng, and J. S. Suri, Algorithms for the automated detection of diabetic retinopathy using digital fundus images : a review, *Journal of medical systems*, vol. 36, no. 1, pp. 145-157, 2012.

[5] S. D. Schwartz, C. D. Regillo, B. L. Lam, D. Eliott, P. J. Rosenfeld, N. Z. Gregori, J. P. Hubschman, J. L. Davis, G. Heilwell and M. Spirn, Human embryonic stem cell-derived retinal pigment epithelium in patients with age-related macular degeneration and Stargardt's macular dystrophy: follow-up of two open-label phase 1/2 studies, *The Lancet*, vol. 385, no. 9967, pp. 509-516, 2015.

[6] H. Nyeem, W. Boles and C. Boyd, A review of medical image watermarking requirements for teleradiology, *Journal of digital imaging*, vol. 26, no. 2, pp. 326-343, 2013.

[7] S. Weng, J. S. Pan, Integer transform based reversible watermarking incorporating block selection, *Journal of Visual Communication and Image Representation*, vol. 35, pp. 25-35, 2016.

[8] S. Weng, J. S. Pan, Adaptive reversible data hiding based on a local smoothness estimator, *Multimedia Tools and Applications*, vol. 74, no. 23, pp. 10657-10678, 2015.

[9] A. Benhocine, L. Laouamer, L. Nana and A. C. Pascu, New images watermarking scheme based on singular value decomposition, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 9-18, 2013.

[10] J. Lua, W. Meng, D. Junping, Q. Huanga, L. Lia and C. C. Changc, Multiple Watermark Scheme based on DWT-DCT Quantization for Medical Images, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 3, pp. 458-472, 2015.

[11] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan and G. M. Bhat, Information hiding in medical images: a robust medical image watermarking system for E-healthcare, *Multimedia Tools and Applications*, pp. 1-35, 2015.

[12] N. Solanki, S. Kumar Malik and S. Chhikara, RONI Medical Image Watermarking using DWT and RSA, *International Journal of Computer Applications*, vol. 96, no. 9, pp. 30-35, 2014.

[13] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng and F. Ji, Content-adaptive reliable robust lossless data embedding, *Neurocomputing*, vol. 79, pp. 1-11, 2012.

[14] L. An, X. Gao, X. Li, D. Tao, C. Deng and J.Li, Robust reversible watermarking via clustering and enhanced pixel-wise masking, *IEEE Trans. on Image Processing*, vol. 21, no. 8, pp. 3598-3611, 2012.

[15] B. Lei, E. L. Tan, S. Chen, D. Ni, T. Wang and H. Lei, Reversible watermarking scheme for medical image based on differential evolution, *Expert Systems with Applications*, vol. 41, no. 7, pp. 3178-3188, 2014.

[16] C. Dong, J. Li and Y. W. Chen, DWT-DCT Based Robust Multiple Watermarks for Medical Image in *Symposium on Photonics and Optoelectronics (SOPO 2012), IEEE*, pp. 1-4, 2012.

[17] B. Han, J. Li and M. A. Huang, A Novel Medical Image Watermarking in Three-dimensional Fourier Compressed Domain, *International Journal Bioautomation*, vol. 19, no. 3, 2015.

[18] J. Waleed, H. D. Jun, S. Saadoon, S. Hameed and H. Hatem, An Immune Secret QR-Code Sharing based on a Twofold Zero-Watermarking Scheme, *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 4, pp. 399-412, 2015.

[19] V. Seenivasagam and R. A. Velumani, A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud, *Computational and mathematical methods in medicine*, 2013.

[20] V. Seenivasagam and R. A. Velumani, Inversion attack resilient zero-watermarking scheme for medical image authentication, *IET Image Processing*, vol. 8, no. 12, pp. 718-727, 2014.

[21] F. X. Yu, Y. Q. Lei, Y. G. Wang and Z. M. Lu, Robust image hashing based on statistical invariance of dct coefficients, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 4, pp. 286-291, 2010.

[22] L. Liu, Y. Lu and C. Y. Suen, Variable-Length Signature for Near-Duplicate Image Matching, *IEEE Trans. on Image Processing*, vol. 24, no. 4, pp. 1282-1296, 2015.

[23] F. Zou, Y. Chen, J. Song, K. Zhou, Y. Yang and N. Sebe, Compact image fingerprint via multiple kernel hashing, *IEEE Trans. on Multimedia*, vol.17, no. 7, pp. 1006-1018, 2015.

[24] F. Nian, T. Li, X. Wu, Q. Gao and F. Li, Efficient near-duplicate image detection with a local-based binary representation, *Multimedia Tools and Applications*, pp. 1-18, 2015.

[25] X. Liu, Y. Zhu, Z. Sun, M. Diao and L.Zhang, A novel robust video fingerprinting-watermarking hybrid scheme based on visual secret sharing, *Multimedia Tools and Applications*, vol. 74, no. 21, pp. 9157-9174, 2015.

[26] M. Naor and A. Shamir, Visual cryptography, in *Advances in CryptologyEUROCRYPT'94. Springer Berlin Heidelberg*, pp. 1-12, 1995.

[27] M. S. Haleem, L. Han, H. J. van and B. Li, Automatic extraction of retinal features from colour retinal images for glaucoma diagnosis: A review, in *Computerized medical imaging and graphics*, vol. 37, no. 7, pp. 581-596, 2013.