A Copyright- and Privacy-Protected Diabetic Retinopathy Diagnosis Network

Wannida Sae-Tang[1], Non-member

ABSTRACT

This paper proposes a copyright- and privacy-protected diabetic retinopathy (DR) diagnosis network. In the network, DR lesions are automatically detected from a fundus image by firstly estimating non-uniform illumination of the image, and then the lesions are detected from the balanced image by using level-set evolution without re-initialization. The lesions are subsequently marked by using contours. The lesion-marked fundus image is subsequently shared for intra or inter hospital network diagnosis with copyright and privacy protection. Watermarking technique is used for image copyright protection, and visual encryption is used for privacy protection. Sign scrambling of two dimensional (2D) discrete cosine transform (DCT) and one dimensional (1D) DCT is proposed for lesion-marked fundus image encryption. The proposed encryption methods are compared with other transform-based encryption methods, i.e., discrete Fourier transform (DFT) amplitude-only images (AOIs), DCT AOIs, and JPEG 2000-based discrete wavelet transform (DWT) sign scrambling which were proposed for image trading system. Since the encryption is done after DR diagnosis, contours used for DR marking must also be visually encrypted. The proposed encryption methods are effective for strong-edge images that are suitable for lesion-marked fundus images, while random sign-based JPEG 2000, DFT AOIs, and DCT AOIs encrypt the images imperfectly. Moreover, the proposed methods are better in terms of image quality. In addition, watermarking performance and compression performance are confirmed by experiments.

Keywords: Diabetic Retinopathy, Fundus Image, Copyright Protection, Privacy Protection, Network Diagnosis

1. INTRODUCTION

DR is a major cause of vision loss. Early detection of DR helps reduce the risk of blindness [1]. However, it is not an easy task to detect the DR precisely. The earliest sign of DR is broken blood vessels. Exudates, a sign of DR, is lipids leaked form broken blood vessels. The characteristics of exudates are bright and yellowish with arbitrary shapes and sizes. For hard exudates, the boundaries are well-defined. On contrary, for soft exudates or cotton wool spots, boundaries are not clear. In some cases, intra or inter hospital network diagnosis is required for diabetic retinopathy diagnosis. In those networks, diagnosis results are needed to be confirmed, or cooperated diagnosis is required. Security of retinal image storage and transmission is then a task of this paper. Reversible watermarking for fundus images was proposed for image copyright protection in [2]. In [3], watermark is encrypted before embedding to medical images for reliable and robust transmission. Anyway, image visual encryption was not considered for fundus images and lesion-marked fundus images.

In copyright-and privacy-protected image trading system [4], the AOI which is the inversely transformed spectra of an image was used as image visual encryption. In the system, an image is transformed using DFT. Then, amplitude components are extracted. Finally, inverse transform is applied to amplitude components to obtain the AOI. This method is quite complex, since intensity range (IR) reduction of the AOI was required [4, 5]. In [6], JPEG 2000-based DWT sign scrambling was proposed in order to encrypt-then-compress the image. However, JPEG 2000 is still not widely used, and the visual encryption performance of the method is not good enough for strong edge-images especially for lesion-marked fundus images.

This paper proposes a copyright- and privacy-protected DR diagnosis network. In the network, DR lesions are automatically detected from a fundus image. Then, the lesion-marked image is shared for intra or inter hospital network diagnosis with copyright and privacy protection. Watermarking technique is used for image copyright protection, and sign scrambling of 2D DCT and 1D DCT is proposed for lesion-marked fundus image encryption for privacy protection. The proposed encryption methods are compared with other transform-based encryption methods, i.e., DFT AOIs, DCT AOIs, and JPEG 2000-based DWT sign scrambling. Visual encryption performance, encrypted image quality, security, complexity, watermarked image quality, watermark extracting performance, and image compression performance are considered in this paper.

Manuscript received on December 8, 2015 ; revised on June 1, 2016.
Final manuscript received on June 14, 2016.
[1] The author is with The Sirindthorn International Thai-German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand. E-mail: wannida.s.sse@tggs-bangkok.org

The rest of this paper is organized as follows. Section 2 introduces DR, fundus images, and requirements for copyright- and privacy-protected DR diagnosis network. Section 3 describes the proposed network and the proposed encryption methods. Experimental results and discussions are given in Section 4. Finally, Section 5 concludes this paper.

2. PRELIMINARIES

This section gives basic knowledge of DR and fundus images. In addition, requirements for copyright- and privacy-protected DR diagnosis network is described.

2.1 Diabetic Retinopathy and Fundus Images

The number of diabetic patients has grown rapidly in the last few years and is expected to raise in the future, since people have the longevity up. The longer a person has diabetes, the more likely they will develop DR. If left untreated, DR may cause human vision loss [7]. Therefore, the early detection of DR is very important. Signs of the early stage of DR are capillary aneurysms, micro-aneurysms, exudates, hemorrhages, and cotton wool spots. In the next stage, abnormal blood vessels are found.

Figure 1 shows anatomical parts of human eye [8]. Retina which captures scenes and sends the images to the brain is located at the back of the eyeball. Fundus images which are human retinal images are generally used for DR diagnosis. A fundus image normally contains optic disk, fovea, and blood vessels. In diabetic eyes, abnormal things such as abnormal blood vessels, cotton wool spot, and exudates appear. Figure 2 shows an example of diabetic fundus images containing exudates.

There is much research on DR diagnosis from retinal images. In [9], early detection of diabetic eyes using fundus images was proposed. Moreover, fundus images were registered for long-term DR analysis in [10, 11].

Anyway, fundus images normally have non-uniform illumination due to the retina response, image acquisitions, instrumental limitations, and environments. This problem makes the diagnosis of DR difficult. Exudate detection from non-dilated retinal images was proposed in [12]. In addition, non-uniform illumination of retinal images was considered in [13, 14]. It was estimated/corrected before DR diagnosis.

2.2 Requirements for Copyright- and Privacy-Protected Diabetic Retinopathy Diagnosis Network

The following are requirements for copyright- and privacy-protected DR diagnosis network.

(A) DR Diagnosis Performance: DR lesions are detected, and the results are evaluated by sensitivity, specificity, positive predictive value (PPV), accuracy, and misclassified proportion (MP) as described in Section 3.1

(B) Visual encryption performance: It is expected that the image in transmission process is visually encrypted instead of using only secure transmission channels for privacy protection of the diagnosed image. Only the person who has a decryption key, for example, the ophthalmologist can view the image while other staffs cannot. Therefore, the encryption method used in the network should be robust against attacks.

(C) Image quality: The quality of the image which the receiver obtains is expected to be identical with the original diagnosed image. The processes that may degrade the image quality, i.e., watermarking and encryption, should be considered.

(D) Watermarking performance: Watermarking performance is evaluated by watermarked image quality and correct watermark extracting rate. It is expected that both are high, however, there is a trade off between both things.

(E) Compression performance: Compression performance could be evaluated by the compression ratio with the quality of the compressed image.

(F) Complexity: Complexity is desired to be as low as possible. However, it is not the most important requirement, if the task is an offline task.

3. PROPOSED COPYRIGHT- AND PRIVACY-PROTECTED DIABETIC RETINOPATHY DIAGNOSIS NETWORK

Figure 3 shows the proposed network on an assumption of two hospital network diagnosis. In practical, there may be more than two hospitals in the network. In addition, it can also be applied to intra hospital network diagnosis. The result of DR is sent from one user to another/other user (s) for checking (by computer or human) or helping diagnose since there are many types of DR signs. In this paper, exudates detection is performed by the first user. Before sending the diagnosed results to another user, the image is encrypted, watermarked, and compressed, respectively. DR diagnosis is presented in Section 3.1 . The proposed encryption method is described in Section 3.2 Security analysis and complexity analysis are also provided.

3.1 Diabetic Retinopathy Diagnosis

In this paper, exudate detection method proposed in [15] is used. However, the DR diagnosis method is flexible for the proposed network. Figure 4 illustrates the illumination estimation method for color RGB fundus images proposed in [15]. The illumination is estimated from R, G, and B components independently on the assumption that the significant details of retinal structures and lesions may be on any color band of images. Weighted surface fitting is used

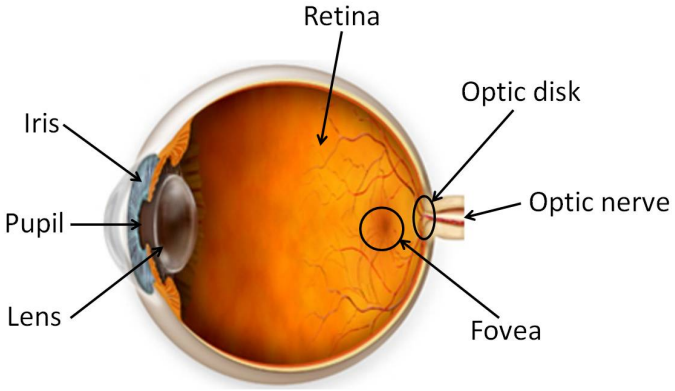


Fig.1: *Anatomical parts of human eye [8].*

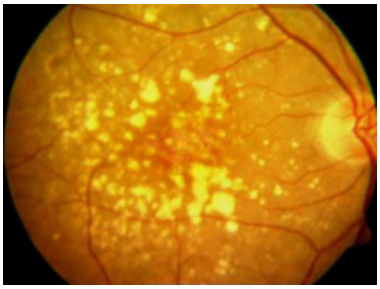


Fig.2: *Diabetic fundus image.*

for illumination estimation. On the assumption that the illumination is smooth, the polynomial surface is applied as described by Eq. 1 and Eq. 2.

$$\vec{E} = S\vec{P}, \tag{1}$$

where $\vec{E}$ is the estimated background vector, S is the surface matrix, and $\vec{P}$ is the parametric surface vector.

$$\begin{bmatrix} E(1,1) \\ \vdots \\ E(x,y) \\ \vdots \\ E(X,Y) \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ x^A & x^{A-1}y & \dots & y & 1 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ X^A & X^{A-1}Y & \dots & Y & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ \vdots \\ P_N \end{bmatrix}, \tag{2}$$

where A is the order of the polynomial, N is the number of terms, $X \times Y$ is the image size, and (x, y) is the pixel coordinate. $\vec{P}$ can be calculated by Eq. 3.

$$\vec{P} = (S^T DS)^{-1}(S^T D)\vec{I}, \tag{3}$$

where $\vec{I}$ is the intensity vector generated by transforming the original image to a vector, and D is the diagonal weight matrix defined as

$$D = \begin{bmatrix} D(1,1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & D(X,Y) \end{bmatrix} \tag{4}$$

This matrix defines whether a pixel will be used in surface fitting process or not. The elements in the diagonal of the matrix correspond to pixels in the original image by order. The elements that correspond to the wanted pixels are set to 1, while the elements that correspond to the unwanted pixels are set to 0.

Unwanted pixels for surface fitting include optic disk, fovea, blood vessles, and lesions. To determine the unwanted pixels, upper bound and lower bound are calculated. Each single band image is smoothed by low pass filtering. Then, a low frequency image is subtracted from the original image to obtain a high frequency image. The upper bound is then calculated by adding the low frequency image, $I_L(x, y)$, by the standard deviation of the high frequency image, $I_H(x, y)$, as described by Eq. 5.

$$UB(x,y) = I_L(x,y) + \sqrt{\frac{1}{mn}\sum_{\forall(x,y)}(I_H(x,y) - \bar{I}_H)^2}, \tag{5}$$

where $UB(x, y)$ denotes the upper bound at pixel (x, y). I_H denotes the statistic mean of $I_H(x, y)$. In the same way, the lower bound is calculated by subtracting the low frequency image by the standard deviation of the high frequency image as described by Eq. 6.

$$LB(x,y) = I_L(x,y) - \sqrt{\frac{1}{mn}\sum_{\forall(x,y)}(I_H(x,y) - \bar{I}_H)^2}, \tag{6}$$

where $LB(x, y)$ denotes the lower bound. The upper bound and the lower bound are used to determine the diagonal weight matrix as Eq. 7.

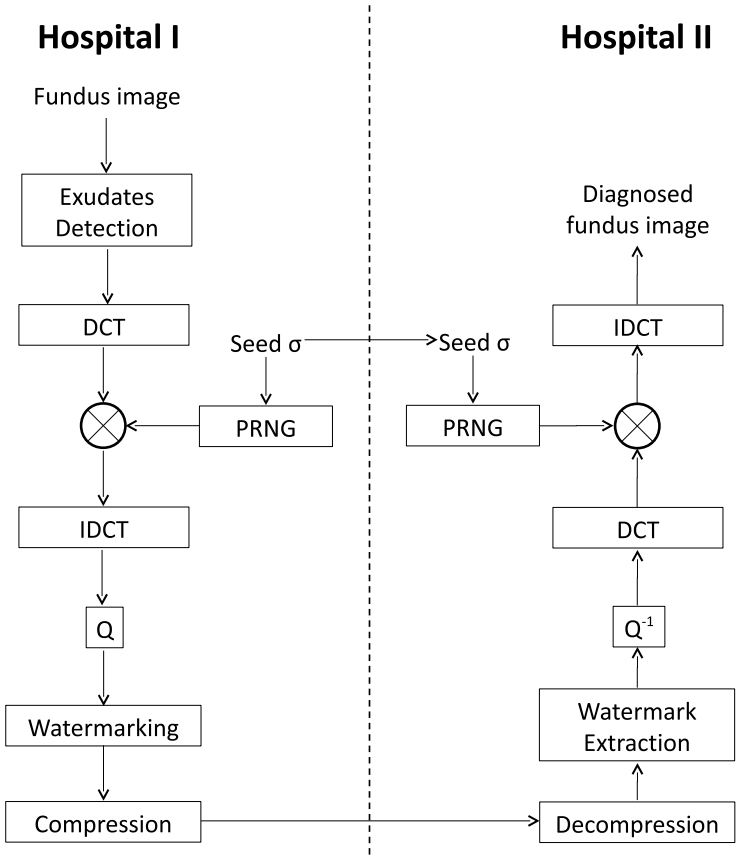


Fig.3: *Proposed copyright- and privacy-protected diabetic retinopathy diagnosis network (DCT: discrete cosine transform, PRNG: pseudo random number generator, IDCT: inverse discrete cosine transform, Q: quantization, Q^{-1}: inverse quantization).*

$$D(x,y) = \begin{cases} 0, UB(x,y) < I(x,y) \\ 0, I(x,y) < LB(x,y) \\ 1, LB(x,y) \leq I(x,y) \leq UB(x,y) \end{cases}. \quad (7)$$

Figure 5 shows an example of unwanted pixels detected by using upper/lower bounds. Figure 6 shows the result of illumination estimation. By using this method, there are two parameters needed to be controlled: filter mask and order of polynomial [15].

After illumination estimation process, exudates and other lesions are detected using level-set evolution without re-initialization [16]. Sensitivity, specificity, PPV, accuracy, and MP described by Eqs. (8), (9), (10), (11), and (12), respectively, are used to evaluate the effectiveness of the DR diagnosis method.

$$Sensitivity = TP/(TP + FN); \quad (8)$$

$$Specificity = TN/(TN + FP); \quad (9)$$

$$PPV = TP/(TP + FP); \quad (10)$$

$$Accuracy = (TP+TN)/(TP+TN+FP+FN); \quad (11)$$

$$MP = FP/(TP + TN + FP + FN), \quad (12)$$

where true positive (TP) is the number of lesion pixels correctly detected, true negative (TN) is the number of non-lesion pixels correctly identified as non-lesion pixels, false positive (FP) is the number of non-lesion pixels wrongly detected as lesion pixels, and false negative (FN) is the number of lesion pixels that cannot be detected. Sensitivity is the probability that the proposed method can classify the pixels of lesions as lesions. Specificity is the probability that the proposed method can classify the pixels of non-lesions as non-lesions. PPV is the probability that the pixels classified as lesions are really lesions. Specificity and accuracy are not very meaningful because the true negative value is always very high. Specificity and accuracy are always close to 100% regardless of the detection method.

3.2 Proposed Encryption Method

Each component of the color fundus image is processed independently. From now, only one color band of the image is considered for easy explanation. The algorithm for image encryption is as follows:

(1) Transform the image $f(x, y)$ by using DCT.
(2) Generate a random sign matrix R which consists of $+1$ and -1 randomly with the same size as the

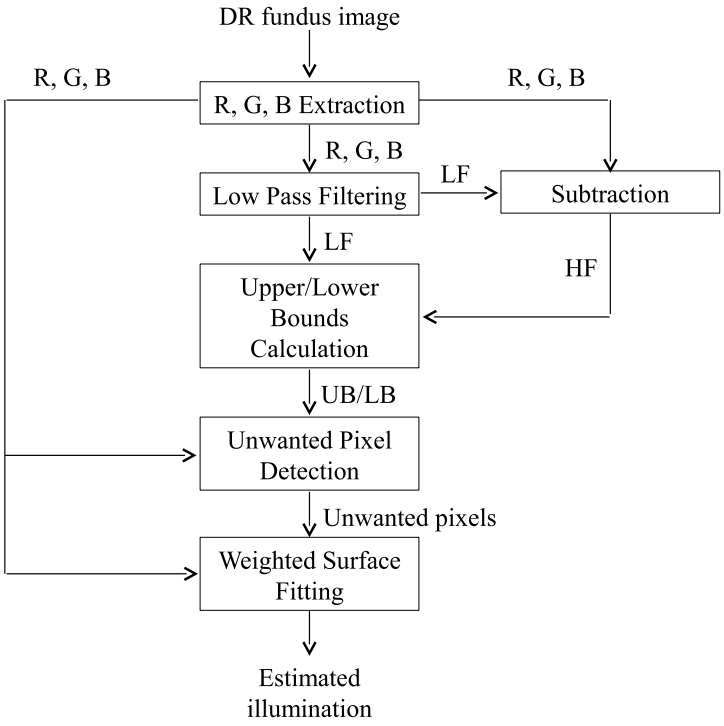
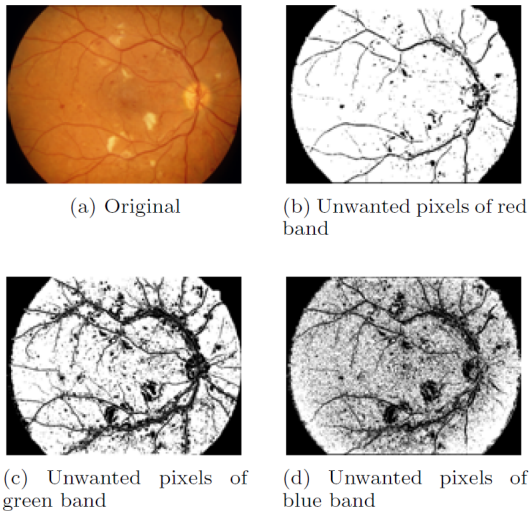
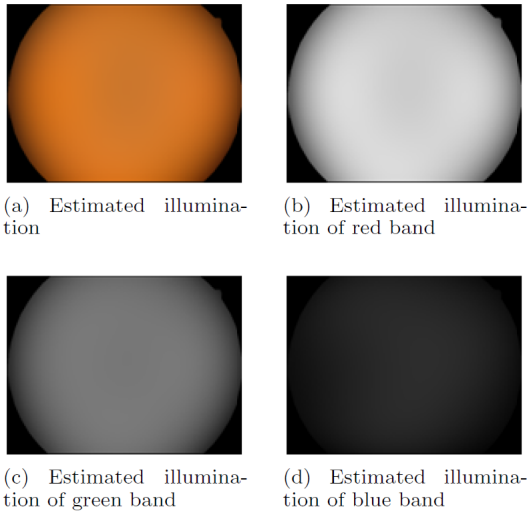


Fig.4: *Block diagram for illumination estimation [15] (DR: diabetic retinopathy, LF: low frequency, HF: high frequency, UB: upper bound, LB: lower bound).*



(a) Original (b) Unwanted pixels of red band (c) Unwanted pixels of green band (d) Unwanted pixels of blue band

Fig.5: *Unwanted pixels detected by using upper/lower bounds*



(a) Estimated illumination (b) Estimated illumination of red band (c) Estimated illumination of green band (d) Estimated illumination of blue band

Fig.6: *Estimated illumination*

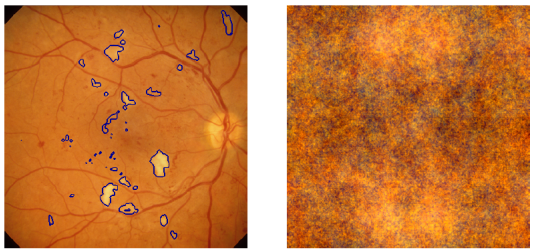
image $f(x, y)$. A seed σ for pseudo random number generator (PRNG) is input for image encryption and is sent to another user as the decryption key.

(3) Multiply DCT coefficients $F(u, v)$ of image $f(x, y)$ with the random matrix R pixel-wise.

(4) Apply inverse discrete cosine transform (IDCT) to the sign-scrambled coefficients $F'(u, v)$.

In this framework, 2D DCT and 1D DCT sign scrambling are proposed for image encryption.

For 2D DCT, the diagnosed fundus image is transformed to a frequency domain by using 2D DCT. Let $F(u, v)$ be the $X \times Y$-sized discrete cosine transformed (DCTed) coefficients of $X \times Y$-sized diagnosed fundus image $f(x, y)$, where $x = 0, 1, \ldots, X - 1$, $y = 0, 1, \ldots, Y - 1$, $u = 0, 1, \ldots, X - 1$, and $v = 0, 1, \ldots, Y - 1$;



(a) Diagnosed (b) Encrypted

Fig.7: *Diagnosed fundus image and encrypted diagnosed fundus image using 2D DCT sign scrambling.*

$$F(u,v) = \sum_{x=0}^{X-1}\sum_{y=0}^{Y-1} f(x,y)\cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right)\dots \cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right). \quad (13)$$

DCTed coefficients $F(u,v)$ can also be expressed in the polar form as

$$F(u,v) = |F(u,v)|S_{DCT}(u,v), \quad (14)$$

where $|F(u,v)|$ and $S_{DCT}(u,v)$ denote the amplitude and sign components of $F(u,v)$, respectively.

By applying sign scrambling encryption, the encrypted coefficients can be formulated as

$$F'(u,v) = |F(u,v)|S_{DCT}(u,v)R(u,v), \quad (15)$$

where $R(u,v)$ denotes a random sign matrix with $X \times Y$ in size which consists of $+1$ and -1. Apply IDCT to $F'(u,v)$ to obtain:

$$f'(x,y) = \sum_{u=0}^{X-1}\sum_{v=0}^{Y-1} \alpha(u)\alpha(v)F'(u,v)\dots \cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right)\cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right), \quad (16)$$

where

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{X}}, u = 0 \\ \sqrt{\frac{2}{X}}, u = 1,2,\dots,X-1, \end{cases} \quad (17)$$

$$\alpha(v) = \begin{cases} \frac{1}{\sqrt{Y}}, v = 0 \\ \sqrt{\frac{2}{Y}}, v = 1,2,\dots,Y-1, \end{cases} \quad (18)$$

and $f'(x,y)$ denotes the visually encrypted diagnosed fundus image. Figures 7 (a) and (b) show a diagnosed fundus image and the related encrypted image, respectively.

It is necessary to check the IR of the encrypted image. Eq. (19) defines the IR.

$$\text{IR} = \max\left(f'(x,y)\right) - \min\left(f'(x,y)\right). \quad (19)$$

To store the images into 8 bits per pixel (bpp) images, a simple linear quantization (LQ) is used to quantize the image $f'(x,y)$ by taking into account the entire IR. $f'(x,y)$ is quantized as

$$f'_{id}(x,y) = \left(\frac{f'(x,y) - \min(f'(x,y))}{s}\right), \quad (20)$$

$$s = \frac{\max(f'(x,y)) - \min(f'(x,y))}{2^n - 1}. \quad (21)$$

$f'_{id}(x,y)$ is the index image which ranges in $[0, 2^n - 1]$, i.e., the number of quantization levels is equal to 2^n. To obtain quantized image $f'_{LQ}(x,y)$, the inverse quantization with constant step size s and bias constant $\min(f'(x,y))$ are applied to $f'_{id}(x,y)$ as

$$f'_{LQ}(x,y) = sf'_{id}(x,y) + \min(f'(x,y)). \quad (22)$$

For image decryption, firstly the quantized image $f'_{LQ}(x,y)$ is transformed using 2D DCT as shown in Eq. (23).

$$F'_{LQ}(u,v) = \sum_{x=0}^{X-1}\sum_{y=0}^{Y-1} f'_{LQ}(x,y)\cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right)\dots \cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right), \quad (23)$$

where $F'_{LQ}(u,v)$ denotes the encrypted coefficients with quantization effects. Then, the random sign matrix R is multiplied pixel-wise with the coefficients $F'_{LQ}(u,v)$ as

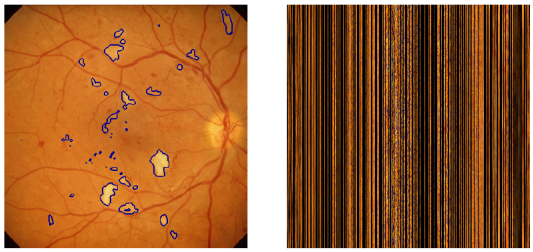
$$F_{LQ}(u,v) = F'_{LQ}(u,v)R(u,v), \quad (24)$$

where $F_{LQ}(u,v)$ denotes the decrypted coefficients with quantization effects. Finally, 2D IDCT is applied to the coefficients $F_{LQ}(u,v)$ as

$$f_{LQ}(x,y) = \sum_{u=0}^{X-1}\sum_{v=0}^{Y-1} \alpha(u)\alpha(v)F_{LQ}(u,v)\dots \cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right)\cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right), \quad (25)$$

where $f_{LQ}(x,y)$ denotes the decrypted diagnosed fundus image with quantization effects. It is noted that if the quantization is not applied, $f_{LQ}(x,y) = f(x,y)$. Anyway, other quantization methods can be used in order to minimize quantization errors.

For the last method using 1D DCT, Let $F_c(x,v)$ be the $X \times Y$-sized column-wise 1D discrete cosine transformed (DCTed) coefficients of the diagnosed



(a) Diagnosed (b) Encrypted

Fig.8: *Diagnosed fundus image and encrypted diagnosed fundus image using 1D DCT sign scrambling.*

fundus image $f(x, y)$, where $x = 0, 1, \ldots, X-1$, $y = 0, 1, \ldots, Y-1$, and $v = 0, 1, \ldots, Y-1$;

$$F_c(x, v) = \sum_{y=0}^{Y-1} f(x, y) \cos\left(\frac{\pi}{Y}\left(y + \frac{1}{2}\right) v\right). \quad (26)$$

DCT coefficients $F_c(x, v)$ can also be expressed in the polar form as

$$F_c(x, v) = |F_c(x, v)| S_c(x, v), \quad (27)$$

where $|F_c(x, v)|$ and $S_c(x, v)$ denote the amplitude and sign components of $F_c(x, v)$, respectively.

To encrypt the image $f(x, y)$, the coefficients, $|F_c(x, v)|$ is multiplied with $R(x, v)$ as

$$F'_c(x, v) = |F_c(x, v)| S_c(x, v) R(x, v), \quad (28)$$

Apply 1D IDCT to $F'_c(x, v)$ to obtain

$$f'_c(x, y) = \sum_{v=0}^{Y-1} \alpha(v) F'_c(x, v) \cos\left(\frac{\pi}{Y}\left(y + \frac{1}{2}\right) v\right), \quad (29)$$

where $f'_c(x, y)$ denotes the visually encrypted diagnosed fundus image, and

$$\alpha(v) = \begin{cases} \sqrt{\frac{1}{Y}}, v = 0 \\ \sqrt{\frac{2}{Y}}, v = 1, 2, \ldots, Y-1. \end{cases} \quad (30)$$

Figures 8 (a) and (b) show a diagnosed fundus image and the related encrypted image, respectively. It is seen that the visual encryption performance of 1D DCT-based method is as good as that of 2D DCT-based method.

It is noted that for 1D DCT, quantization and the similar decryption method are also applied.

3.3 Security Analysis

Comparing security of encryption algorithms is not an easy task. It depends on skills and levels of attackers. One important aspect of security analysis of encryption is key space size. For both 2D DCT and 1D DCT sign scrambling, assume that the attacker applies brute-force attack. To guess the random sign matrix R, the number of possible ways in generating the matrix called encryption key space size, S_k, is:

$$S_k = 2^{XY}. \quad (31)$$

It is clearly seen that the key space size depends on the image size. Since medical images normally have quite big sizes, this key space size is big enough to this kind of attack. For example, suppose that the fundus image size $XY = 1024 \times 1024$ pixels. In this case, the key space $S_k = 2^{1024 \times 1024}$ which is much bigger than that of an AES-like cipher with a 256-bit key ($S_k = 2^{256}$).

From an experiment (see Figs. 9 and 10), 1%, 5%, and 10% wrong bits for the decryption make decrypted images have lower quality with respect to original images. In security aspect, with these numbers, it seems that the proposed encryption methods are still sensitive. However, for 30% and 40% wrong bits for the decryption, the results show that the decrypted images are unrecognizable. It would need about 60% to 70% correct decryption bits to obtain recognizable images. For an 1024×1024-pixel image with the key space $2^{1024 \times 1024}$, to get 60% to 70% correct decryption bits from guessing, it is still not an easy task.

3.4 Complexity Analysis

Even though low complexity is not a major requirement of the proposed network, this section compares the complexity of both encryption methods. The difference between methods is the dimension of image transformation. The complexity of 2D DCT for an $X \times Y$ sized image is $O((XY)^2)$ or $O((XY \log_2 (XY))$ with fast algorithm, whereas that of 1D DCT is $O((X^2)Y)$ or $O((X \log_2 X)Y)$ with fast algorithm. It is clearly seen that 1D DCT outperforms 2D DCT in terms of complexity.

4. EXPERIMENTAL RESULTS

The experiment is divided into two parts: DR diagnosis performance and copyright and privacy protection performance. Eight 32-bit color fundus images from REVIEW databases [17] and eighty nine 24-bit color fundus images with 1500×1152 pixels in size from DIARETDB1 database [18] are used in the experiments.

4.1 DR Diagnosis Performance

In this part, eighty nine 24-bit color fundus images with 1500×1152 pixels in size from DIARETDB1 database are used to evaluate the exudate detection performance. Forty seven images contain exudates, but the rest images do not. The database includes

Table 1: *Exudate detection results from forty seven images that contain hard exudates.*

Method	Average sensitivity (%)	Average specificity (%)	Average PPV (%)	Average MP (%)
Sopharak et al. [19]	43.48	99.31	25.48	0.68
Ravishankar et al. [9]	58.21	98.09	13.37	1.90
Welter et al. [20]	66.00	98.64	19.45	1.34
Welfer et al. [21]	70.48	98.84	21.32	1.10
Kande et al. [22]	86.00	98.00	-	-
Sae-Tang et al. [15]	89.38	99.08	80.74	0.81

Table 2: *Exudate detection results from forty two images that do not contain hard exudates.*

Method	Average specificity (%)	Average MP (%)
Sopharak et al. [19]	99.28	0.71
Ravishankar et al. [9]	97.53	2.47
Welter et al. [20]	99.22	0.77
Welfer et al. [21]	98.74	1.20
Kande et al. [22]	-	-
Sae-Tang et al. [15]	99.48	0.52

manually labeled images that are used as a ground truth in the experiment. Table 1 and 2 show the experimental results. The method used in this paper is compared with the methods proposed by Soparak et al. [19], Ravishankar et al. [9], Walter et al. [20], Welfer et al. [21], and Kande et al. [22]. All compared methods are based on mathematical morphology and were validated using DIARETDB1 database. Welfer et al. [21] used the contrast enhancement before detecting exudates. The method improved the sensitivity of exudate detection, but it also increases FP causing low PPV. Kande et al. [22] used local contrast enhancement, but it introduces noises to images. For images containing hard exudates, the method used in this paper achieves higher average PPV than those of other methods. For images without hard exudates, the method achieves the highest average specificity and the lowest average MP compared to other methods. It shows that the method significantly reduces FP in detecting exudates and simultaneously keeps high sensitivity in detecting exudates. This is because of the effective illumination estimation.

4.2 Copyright and Privacy Protection Performance

The proposed encryption methods are compared with JPEG 2000-based DWT sign scrambling [6], 2D DFT AOI [4], 1D DFT AOI [5], 2D DCT AOI [5], and 1D DCT AOI [5] which were proposed for copyright- and privacy-protected image trading systems in which a trusted third party (TTP) can process images using visual scrambled images. Even though the application is different from the proposed application, these encryption methods could also be applied to the proposed network. Figures 11, 12, and 13 show the proposed copyright- and privacy-protected DR diagnosis network using the compared encryption methods.

4.2.1 Visual Encryption Performance

The original fundus images and the lesion-marked fundus images are encrypted by several methods as shown in Figs. 14, 15, 16, and 17. The results show that the proposed 1D DCT sign scrambling and 2D DCT sign scrambling methods perfectly visually encrypt the original fundus images and the lesion-marked fundus images, while other methods encrypt the images imperfectly especially for the lesion-marked fundus images. Among several methods, JPEG 2000-based DWT sign scrambling [6] is the worst encryption method. 2D DFT AOI and 2D DCT AOI are better than 1D DFT AOI and 1D DCT AOI.

4.2.2 Image Quality

Tables 3 and 4 compare IRs of encrypted diagnosed fundus images "HRIS001" and "HRIS003," respectively. Between two proposed methods, 2D DCT sign scrambling gives narrower IRs than those of 1D DCT sign scrambling for every color band of images. From this fact, by applying LQ to the encrypted images, 2D DCT sign scrambling method has a possibility to achieve better image quality. For JPEG 2000-based DWT sign scrambling method, the IRs are not defined, because the scrambled DWT coefficients are encoded, and by using the proprietary JPEG 2000 decoder, the original images are recovered for lossless compression, viz., quantization is not required. Therefore, infinite PSNRs are obtained. However, this method will not be considered anymore in the rest experiments because of its bad visual encryption performance. For AOI methods, 2D DFT AOI and 2D DCT AOI methods give wide IRs, while 1D DFT AOI and 1D DCT AOI methods give much lower IRs than those of 2D transform methods. However, they are worse than the proposed methods. Besides IRs of images, the distribution of pixel intensities are also an important factor of image quality. Consequently, the image quality is evaluated by peak signal-to-noise ratio (PSNR). The PSNRs of decrypted images with respect to the original diagnosed fundus images are calculated. From Tables 5 and 6, the proposed methods give the highest PSNRs than the conventional methods. 2D DCT sign scrambling method gives higher PSNRs than those of 1D DCT sign scrambling. 1D DFT AOI method and 1D DCT AOI method give higher PSNRs than those of 2D DFT AOI method and 2D DCT AOI method. Figures 18 and 19 show the decrypted images. Even though 2D DCT sign scrambling gives higher PSNRs than those of 1D DCT sign scrambling, the image visual quality for 1D DCT sign scrambling method is also good. Therefore, 1D DCT sign scrambling method can be considered in case that the complexity of the system is concerned.

Table 3: *Intensity range of encrypted diagnosed fundus image "HRIS001."*

	Red	Green	Blue
2D DCT sign scrambling	[49.4, 351.2]	[−2.5, 219.3]	[−55.4, 110.2]
1D DCT sign scrambling	[−414.1, 420.3]	[−245.6, 264.2]	[−176.0, 160.7]
JPEG 2000-based DWT sign scrambling [6]	N/A	N/A	N/A
2D DFT AOI [4]	[130.9, 7688.7]	[53.4, 5068.4]	[4.4, 3651.8]
1D DFT AOI [5]	[82.9, 1203.7]	[22.1, 746.7]	[−13.7, 538.9]
2D DCT AOI [5]	[95.0, 8434.1]	[31.7, 5725.7]	[−6.1, 4046.6]
1D DCT AOI [5]	[75.8, 1186.5]	[15.3, 740.4]	[−25, 532.4]

Table 4: *Intensity range of encrypted diagnosed fundus image "HRIS003."*

	Red	Green	Blue
2D DCT sign scrambling	[−112.5, 369.3]	[−75.0, 174.3]	[−147.6, 160.0]
1D DCT sign scrambling	[−407.1, 449.6]	[−215.8, 217.6]	[−260.6, 237.5]
JPEG 2000-based DWT sign scrambling [6]	N/A	N/A	N/A
2D DFT AOI [4]	[24.1, 1242.2]	[0.4, 6070.3]	[−7.3, 8260.3]
1D DFT AOI [5]	[−66.5, 1387.8]	[−11.0, 715.2]	[−62.0, 896.5]
2D DCT AOI [5]	[−45.3, 1325.3]	[−38.3, 6621.9]	[−70.7, 8890.2]
1D DCT AOI [5]	[−66.7, 1386.7]	[−41.8, 739.1]	[−70.1, 913.6]

Table 5: *Peak signal-to-noise ratio of decrypted diagnosed fundus image "HRIS001" [dB].*

	Red	Green	Blue
2D DCT sign scrambling	62.2152	64.9031	67.4253
1D DCT sign scrambling	53.3933	57.6723	61.2826
JPEG 2000-based DWT sign scrambling [6]	Inf	Inf	Inf
2D DFT AOI [4]	34.1981	37.8061	40.5690
1D DFT AOI [5]	50.6424	54.1384	56.1575
2D DCT AOI [5]	33.3508	36.6959	39.6654
1D DCT AOI [5]	50.9035	54.6350	56.8893

Table 6: *Peak signal-to-noise ratio of decrypted diagnosed fundus image "HRIS003" [dB].*

	Red	Green	Blue
2D DCT sign scrambling	58.1709	63.9040	62.0651
1D DCT sign scrambling	53.1801	59.0853	57.8542
JPEG 2000-based DWT sign scrambling [6]	Inf	Inf	Inf
2D DFT AOI [4]	30.3778	36.2587	34.1194
1D DFT AOI [5]	48.7052	54.3634	51.9720
2D DCT AOI [5]	29.3981	35.2937	32.7385
1D DCT AOI [5]	48.6078	53.9613	51.9457

4.2.3 Watermarking Performance

Almost any arbitrary digital watermarking technique can be applied. This paper uses a simple non-blind additive digital watermarking technique in the discrete wavelet transformed (DWTed) domain, which is based on the essence of [23].

(A) Watermarking: The process of watermarking is as follows:
  (1) $X \times Y$-sized DWTed coefficients are divided into $X_B \times Y_B$-sized coefficient blocks where $X_B = Y_B = 8$ in the experiments. That is, the DWTed coefficients are divided into $K = XY/X_BY_B$ blocks.
  (2) A binary watermark sequence, $b = [b_1b_2b_3...b_K]$, is provided, where $b_k \in \{0, 1\}$, and $k = 1, 2, 3, ..., K$.
  (3) Each single bit of the watermark sequence, b_k, is represented by an M-sequence with the length L, and the length of M-sequences used in the experiments is the smallest, i.e., $L = 3$, where $L = B^P - 1$, $B = 2$, and $P = 2$, even longer sequences serve better correct watermark extracting rate. The M-sequences differ from each other for different single bits of the watermark. Therefore, two different M-sequences are prepared for $b_k \in \{0, 1\}$.
  (4) Each M-sequence is subsequently embedded to a divided block of DWTed coefficients by linearly scaling and adding it to three bottom-right coefficients of the block as

$$C'_{k,l} = \mathrm{sgn}\left(C_{k,l}\right)\left(|C_{k,l}| + \delta W_{b_k,l}\right), \quad (32)$$

  where $C'_{k,l}$ denotes the l-th watermarked DWTed coefficient in the k-th block, $C_{k,l}$ denotes the l-th original DWTed coefficient in the k-th block, δ is a scaling factor, and $W_{b_k,l} \in \{0, 1\}$ denotes the l-th element of the M-sequence for bit b_k, where $l = 1, 2, \ldots, L$. It is noted that all variables in Eq. (32) are integers.

(B) Watermark Extraction: The watermark is extracted from the DWTed coefficients by using a correlation-based detector as

$$b'_k = \arg \max_{b_k \in \{0,1\}} \sum_{l=1}^{L} \left(W_{b_k,l} - 0.5\right) ... \left(\frac{\left|\left|C''_{k,l}\right| - |C_{k,l}|\right|}{\delta} - 0.5\right), \quad (33)$$

where b'_k is an extracted watermark bit, and $\left|C''_{k,l}\right|$ denotes the l-th watermarked DWTed coefficient in the block. It is noted that $\left|C''_{k,l}\right|$ may be different from $\left|C'_{k,l}\right|$ because of clipping in JPEG 2000 decoding.

Table 7 shows PSNRs of watermarked diagnosed fundus images averaged by 97 images without compression effects, when δ is varied from 1 to 8 with stepping by 1. All methods are comparable in terms of watermarked image quality. However, these slight differences in PSNRs of watermarked images between methods are not significant, because the final image quality significantly depends on the encryption method, and from Table 5 and 6, it is clearly seen that the proposed methods give much higher PSNRs than those of other methods. For watermark extracting performance, all methods have achieved 100% correct watermark extracting rates using a correlation-based detector. It is noted that if the compression is lossless, the images can be recovered, because the watermark is extracted 100% correctly. It means that this watermarking method is very effective as reversible watermarking. Due to the fact that watermarking performance depends on the watermarking technique, optimization or other watermarking techniques such as [23–26] could be applied.

4.2.4 Compression Performance

Kakadu [27], a software to encode and decode JPEG 2000 images, is used in the experiments. It is noted that any image compression standard could be used in the proposed network instead of JPEG 2000.

Usually, compression and encryption are combined by firstly compressing the content and encrypting it subsequently. However, the encryption is performed independently from the compression process in the proposed network for flexibility in choosing the encryption method and the compression method. Therefore, it is necessary to confirm the compression performance when the encryption is done first. In this part, the compression performance is compared with and without the proposed encryption method and other encryption methods without considering watermarking process, where the diagnosed fundus image "HRIS001" with 446 kbytes is used in the experiment. The encrypted diagnosed fundus images are linearly quantized and then compressed using JPEG 2000. The compression bit rate is varied by 0.25, 0.5, 1, 2, 3, 4, and 5 bpp for lossy compression. Table 8 compares the compressed file sizes of the quantized encrypted diagnosed fundus images, while the file sizes of the quantized encrypted diagnosed fundus images are 446 kbytes. PSNRs of the compressed images are calculated with respect to the quantized images as shown in Table 9.

From the results, all encryption methods degrade the compression performance. Comparing the proposed methods to other methods, 1D DFT AOI and 1D DCT AOI are better than the proposed methods in terms of compression performance. However, these methods are worse in terms of visual encryption performance (see Section 4.2.1) which is more important for privacy protected network. 2D DFT AOI and 2D DCT AOI are better than the proposed methods in terms of compression performance, when the compression is lossy. However, they are worse than the proposed methods in terms of visual encryption performance (see Section 4.2.1) and much worse in terms of image quality (see Section 4.2.2). In addition, for lossless compression, the proposed methods are comparable with them. It is expected that the compression is lossless in practical terms, since high quality images are required for DR diagnosis. Therefore, the proposed methods are the better choices.

Table 10 concludes the effectiveness of the proposed encryption methods and the conventional encryption methods. Symbols "×," "Δ," "◯," and "◎" mean "bad," "fair," "good," and "excellent," respectively.

5. CONCLUSIONS

The paper has proposed a copyright- and privacy-protected DR diagnosis network. In the network, DR lesions are automatically detected from a fundus image by firstly estimating the non-uniform illumination of the image, and then the lesions are detected from the balanced image by using level-set evolution without re-initialization. The lesions are subsequently marked by using contours. The lesion-marked fundus image is subsequently shared for intra or inter hospital network diagnosis with copyright and privacy protection. Watermarking technique is used for image copyright protection, and visual encryption is used for privacy protection. 2D DCT sign scrambling and 1D DCT sign scrambling have been proposed for privacy protection. The proposed encryption methods are effective for strong-edge images that is suitable for lesion-marked fundus images, while random sign-based JPEG 2000, DFT AOIs, and DCT AOIs encrypt the images imperfectly. Moreover, the proposed methods are better in terms of image quality. Eventhough 2D DCT sign scrambling method is the best in terms of image quality, the proposed 1D DCT sign scrambling could be used instead of 2D DCT sign scrambling in cases that the complexity is concerned. In addition, the proposed encryption methods could be applied for general images and other applications, and other encryption methods that encrypt images containing strong edges perfectly could be applied to the proposed network. All methods are comparable in terms of watermarked image quality. For watermark extracting performance, all methods have achieved 100% correct watermark extracting rates using a correlation-based detector.

References

[1] G. G. Yen and W. F. Leong, "A sorting system for hierarchical grading of diabetic fundus images: A preliminary study," *IEEE Trans. Inf.*

Table 7: *Averaged peak signal-to-noise ratios of watermarked diagnosed fundus images [dB].*

δ	1	2	3	4	5	6	7	8
2D DCT sign scrambling	64.3396	60.9186	58.5993	56.8373	55.1256	53.7174	52.5801	51.5593
1D DCT sign scrambling	64.3865	61.1529	58.8164	57.0382	55.3445	53.9888	52.8151	51.8253
2D DFT AOI [4]	65.1744	61.8779	59.4572	57.6995	56.0046	54.6690	53.5241	52.5157
1D DFT AOI [5]	65.5210	62.4001	59.9945	58.2029	56.5058	55.1782	54.0052	52.9781
2D DCT AOI [5]	63.8137	60.8935	58.4202	56.7237	54.9686	53.6312	52.4312	51.4703
1D DCT AOI [5]	63.9598	60.8524	58.5301	56.7642	55.0644	53.7950	52.6293	51.6443

Table 8: *Compressed file sizes of encrypted diagnosed fundus images for "HRIS001" [kbytes].*

Bit rate [bit per pixel]	0.25	0.5	1	2	3	4	5	Lossless
original	4.69	9.36	18.5	37.2	55.7	75.2	92.6	211
2D DCT sign scrambling	4.65	9.07	18.5	37.1	55.7	74.2	92.8	317
1D DCT sign scrambling	4.61	9.36	18.6	37.0	55.7	74.2	92.7	282
2D DFT AOI [4]	4.71	9.25	18.6	37.1	55.7	74.3	92.8	299
1D DFT AOI [5]	4.68	9.25	18.4	37.1	55.2	74.2	92.8	231
2D DCT AOI [5]	4.56	9.20	18.6	36.8	55.7	74.3	92.8	316
1D DCT AOI [5]	4.71	9.35	18.5	37.1	55.7	74.3	92.8	251

Table 9: *Peak signal-to-noise ratios of compressed encrypted diagnosed fundus images for "HRIS001" [dB].*

Bit rate [bit per pixel]	0.25	0.5	1	2	3	4	5	Lossless
original	25.5465	27.4390	29.4362	34.7269	38.6917	41.6652	43.7407	Inf
2D DCT sign scrambling	23.8068	24.5345	25.7157	27.5950	29.0822	29.9125	31.1130	Inf
1D DCT sign scrambling	16.1688	19.2890	22.4141	25.4751	30.0771	32.3156	34.2390	Inf
2D DFT AOI [4]	28.5696	29.2500	30.1917	31.3830	32.5048	33.5065	34.3004	Inf
1D DFT AOI [5]	30.6858	31.7375	33.8367	35.8697	38.2836	40.0649	41.5370	Inf
2D DCT AOI [5]	26.8727	27.6097	28.5678	29.7366	31.1661	31.9076	32.7252	Inf
1D DCT AOI [5]	28.6237	29.5979	31.6235	33.9189	35.8974	37.8213	39.5469	Inf

Table 10: *Conclusions of effectiveness of considered methods (P_1: 2D DCT sign scrambling (Proposed 1), P_2: 1D DCT sign scrambling (Proposed 2), C_1: JPEG 2000-based DWT sign scrambling [6] (Conventional 1), C_2: 2D DFT AOI [4] (Conventional 2), C_3: 1D DFT AOI [5] (Conventional 3), C_4:2D DCT AOI [5] (Conventional 4), C_5: 1D DCT AOI [5] (Conventional 5)).*

Requirement	P_1	P_2	C_1	C_2	C_3	C_4	C_5
Visual encryption performance	◎	◎	×	○	△	○	△
Image quality	◎	◎	◎	△	○	△	○
Watermarking performance	◎	◎	-	◎	◎	◎	◎
Compression performance	○	○	-	○	◎	○	◎
Complexity	○	◎	-	○	◎	○	◎

Technol. Biomed., vol. 12, no. 1, pp. 118–130, Jan. 2008.

[2] J. Nayak, P. S. Bhat, R. A. U., and M. S. Kumar, "Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes," *Journal of medical systems*, vol. 33, issue 3, pp. 163–171, Jun. 2009.

[3] M. Nergui, U. S. Acharya, U. R. Acharya, W. Yu, "Reliable and robust transmission and storage techniques for medical images with patient information," *Journal of Medical systems* vol. 34, issue 6, pp. 1129–1139, 2010.

[4] W. Sae-Tang, M. Fujiyoshi, and H. Kiya, "A Generation Method of Amplitude-Only Images with Low Intensity Ranges," *IEICE Trans. Fundamentals*, vol. E96-A, no. 6, pp. 1323–1330, Jun. 2013.

[5] W. Sae-Tang, S. LIU, M. FUJIYOSHI, and H. KIYA, "1D Frequency Transformation-Based Amplitude-Only Images for Copyright- and Privacy-Protection in Image Trading Systems," *ECTI-CIT*, vol. 8, no. 2, Nov. 2014.

[6] W. Sae-Tang, S. Liu, M. Fujiyoshi, and H. Kiya, "A copyright- and privacy-protected image trading system using fingerprinting in discrete wavelet domain with JPEG 2000," *IEICE Trans. Fundamentals*, vol. E97-A, no. 11, Nov. 2014.

[7] W. Sae-Tang, W. Chiracharit, and W. Kumwilaisak, "Exudates Detection in Fundus Images Using Non-uniform Illumination Background Subtraction," *Proc. IEEE TENCON2010*, Fukuoka, Japan, pp. 204–209, Nov. 21-24, 2010.

[8] [Online]. Available: http://www.mastereyeassociates.com/presbyopia.

[9] S. Ravishankar, A. Jain, and A. Mittal, "Automated feature extraction for early detection of diabetic retinopathy in fundus images," *Proc. IEEE CVPR*, Miami, FL, 2009.

[10] H. Narasimha-Iyer, A. Can, B. Roysam, Charles V. Stewart, Howard L. Tanenbaum, A. Majerovics, and H. Singh, "Robust detection and classification of longitudinal changes in color retinal fundus images for monitoring diabetic retinopathy," *IEEE Trans. Biomed. Eng.*, vol. 53, no. 6, pp. 1084–1098, Jun. 2006.

[11] H. Narasimha-Iyer, A. Can, B. Roysam, Howard L. Tanenbaum, and A. Majerovics, "Integrated analysis of vascular and nonvascular changes

from color retinal fundus image sequences," *IEEE Trans. Biomed. Eng.*, vol. 54, no. 8, pp. 1436–1445, Aug. 2007.

[12] A. Sopharak, B. Uyyanonvara, and S. Barman, "Automatic exudate detection from non-dilated diabetic retinopathy retinal images using fuzzy c-means clustering," *Sensors*, pp. 2148–2161, 2009.

[13] M. Foracchia, E. Grisan, and A. Ruggeri, "Luminosity and contrast normalization in retinal images," *Medical Image Analysis*, vol. 3, no. 9, pp. 179–190, 2005.

[14] E. Grisan, A. Giani, E. Ceseracciu, and A. Ruggeri, "Model-based Illumination Correction in Retinal Images," *IEEE Int. Sym. on Biomed. Imag.*, pp. 984–987, Apr. 2006.

[15] W. Sae-Tang, W. Chiracharit, S. Kiattisin, and W. Kumwilaisak, "Non-Uniform Illumination Estimation in Fundus Images Using Bounded Surface Fitting," *The international journal on applied biomedical engineering (IJABME)*, vol. 5, no. 1, pp. 37–45, 2012.

[16] C. Li, C. Xu, C. Gui, and M. D. Fox, "Level-set evolution without re-initialization: A new variational formulation," *IEEE CVPR'05*, 2005.

[17] University of LINCOLN, Department of Computing and Informatics (MHAC MC3201), Retinal Vessel Image set for Estimation of Widths (REVIEW) databases, [Online]. Available: http://aldiri.info.

[18] T. Kauppi, V. Kalesnykiene, J-K. Kamarainen, L. Lensu, I. Sorri, A. Raninen, et al. DIARETDB1: diabetic retinopathy database and evaluation protocol. In: Medical image understanding and analysis (MIUA), pp. 61–65, 2007.

[19] A. Sopharak, B. Uyyanonvara, S. Barman, S. Vongkittirux, and N. Wongkamchang, "Fine exudate detection using morphological reconstruction enhancement," *The international journal on applied biomedical engineering (IJABME)*, vol. 1, no. 1, pp. 45–50, 2010.

[20] T. Walter, J. C. Klein, P. Massin, and A. Erginay, "A contribution of image processing to the diagnosis of diabetic retinopathy-detection of exudates in color fundus images of the human retina," *IEEE Trans. Med. Imag.*, vol. 21, no. 10, pp. 1236–1243, Oct. 2002.

[21] D. Welfer, J. Scharcanski, and D. R. Marinho, "A coarse-to-fine strategy for automatically detecting exudates in color eye fundus images," *Computerized Medical Imaging and Graphics*, pp. 228-235, 2010.

[22] G. Kande, P. Subbaiah, and T. Savithri, "Segmentation of exudates and optic disk in retinal images," *IEEE Sixth Indian Conference on Computer Vision, Graphic & Image Processing*, 2008.

[23] S. Pereira, S. Voloshynoskiy, and T. Pun, "Optimal transform domain watermark embedding via linear programing," *Signal Processing 81*, pp. 1251–1260, 2001.

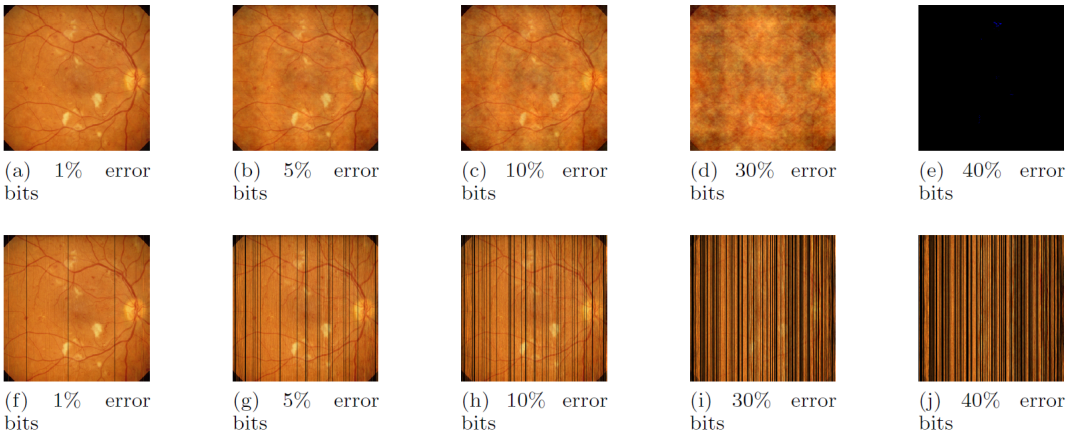
[24] H. Inoue, A. Miyazaki, and T. katsura, "An image watermarking method based on the wavelet transform," *Proc. IEEE ICIP*, pp. 296–300, 1999.

[25] Z. Zhang, Q. Sun, and W. Wong, "A novel lossy-to-lossless watermarking scheme for JPEG2000 images," *Proc. IEEE ICIP*, pp. 573–576, 2004.

[26] Y. Chen and H. Huang, "A progressive image watermarking scheme for JPEG2000," *Proc. IEEE IIH-MSP*, pp. 230–233, 2012.

[27] D. Taubman, "Kakadu software-a comprehensive framework for JPEG2000," 2005.

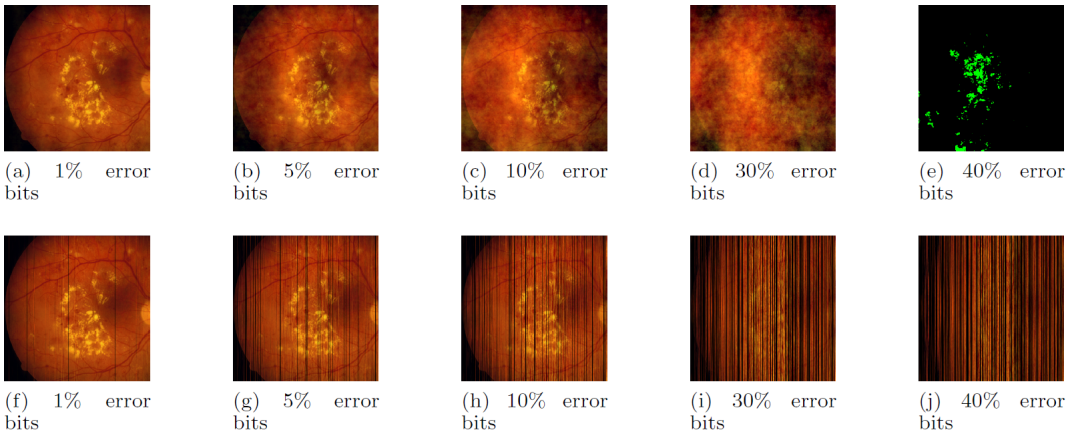
Wannida Sae-Tang received her B.Eng. degree in Electronic and Telecommunication Engineering with the first class honors and her M.Eng. degree in Electrical Engineering from King Mongkut's University of Technology Thonburi, Thailand in 2007 and 2011, respectively, and her Ph.D. degree in Information and Communication Systems from Tokyo Metropolitan University, Japan in 2014 with Tokyo metropolitan governmental Asian human resources fund. From 2007 to 2009, she was an IC packaging design engineer of New product design and research and development team at United Test and Assembly Center Thai Ltd. She is currently a lecturer of The Sirindthorn International Thai-German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, Thailand. Her research interests include image processing and multimedia communication. She received the Best Paper Award of the IEICE/ITE/KSBE IWAIT in 2014.



(a) 1% error bits (b) 5% error bits (c) 10% error bits (d) 30% error bits (e) 40% error bits

(f) 1% error bits (g) 5% error bits (h) 10% error bits (i) 30% error bits (j) 40% error bits

Fig.9: *Decrypted images of "HRIS001" for several percentages of error decryption bits. The upper row is for the proposed 2D DCT sign scrambling, and the lower row is for the proposed 1D DCT sign scrambling.*



(a) 1% error bits (b) 5% error bits (c) 10% error bits (d) 30% error bits (e) 40% error bits

(f) 1% error bits (g) 5% error bits (h) 10% error bits (i) 30% error bits (j) 40% error bits

Fig.10: *Decrypted images of "HRIS003" for several percentages of error decryption bits. The upper row is for the proposed 2D DCT sign scrambling, and the lower row is for the proposed 1D DCT sign scrambling.*

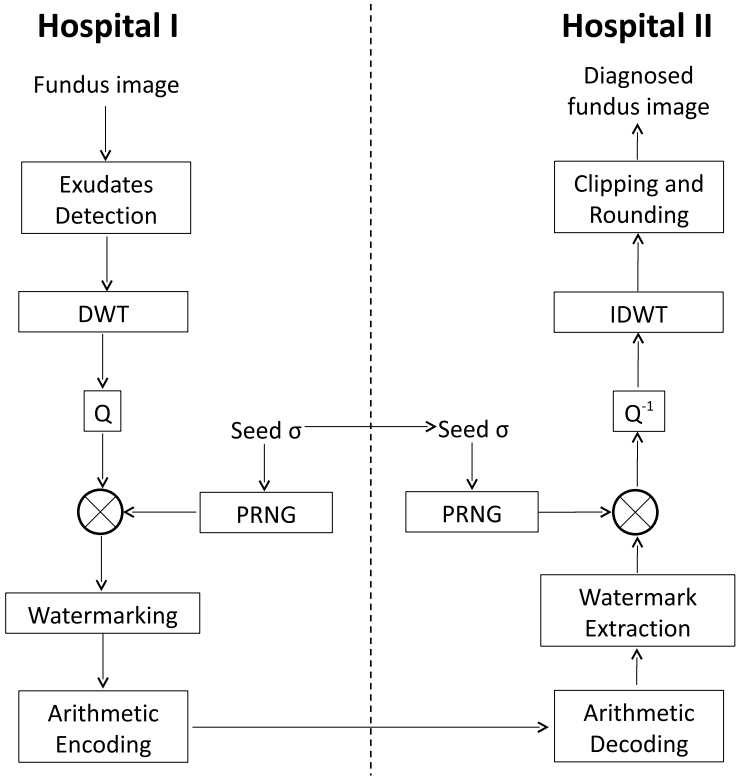


Fig.11: *Copyright- and privacy-protected diabetic retinopathy diagnosis network using JPEG 2000-based DWT sign scrambling (DWT: discrete wavelet transform, Q: quantization, PRNG: pseudo random number generator, Q^{-1}: inverse quantization, IDWT: inverse discrete wavelet transform) [6].*

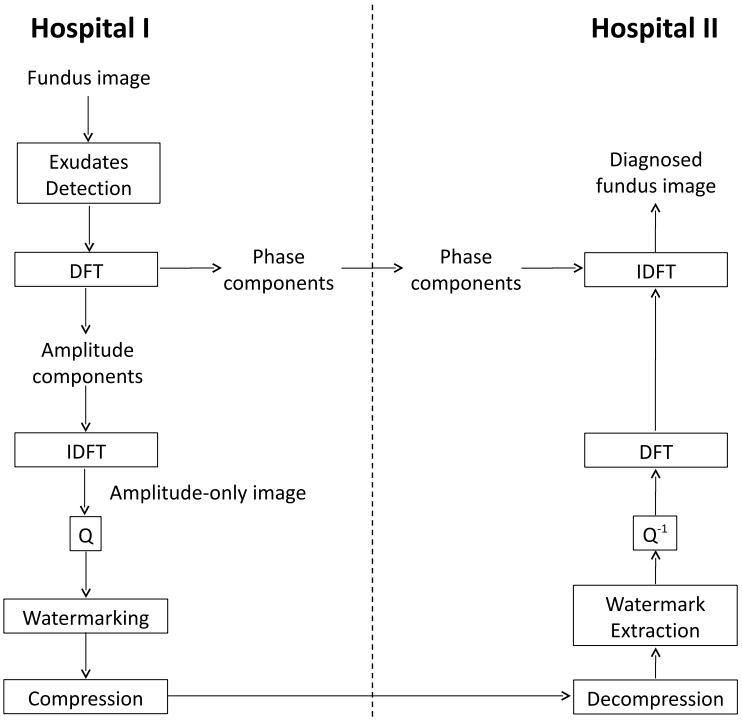


Fig.12: *Copyright- and privacy-protected diabetic retinopathy diagnosis network using DFT AOI (DFT: discrete Fourier transform, IDFT: inverse discrete Fourier transform, Q: quantization, Q^{-1}: inverse quantization) [4, 5].*

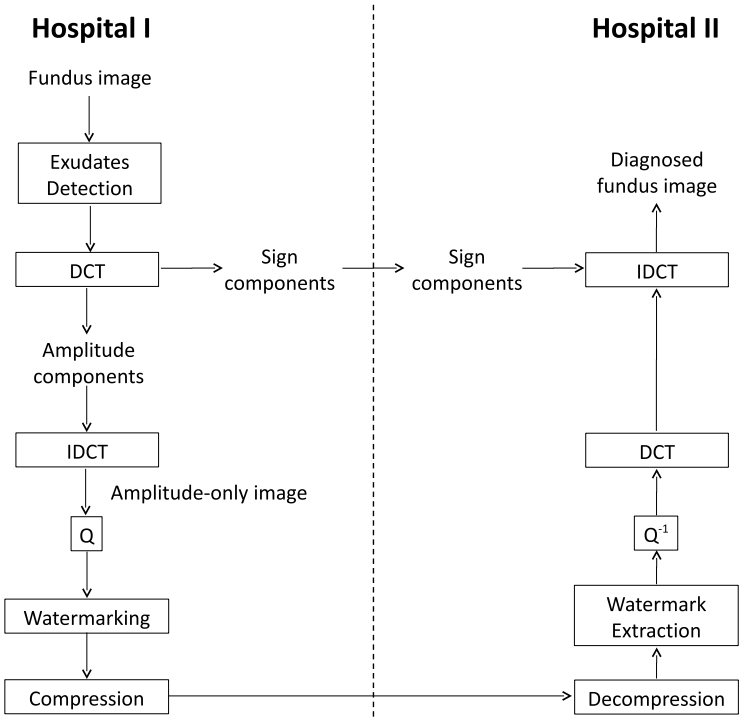
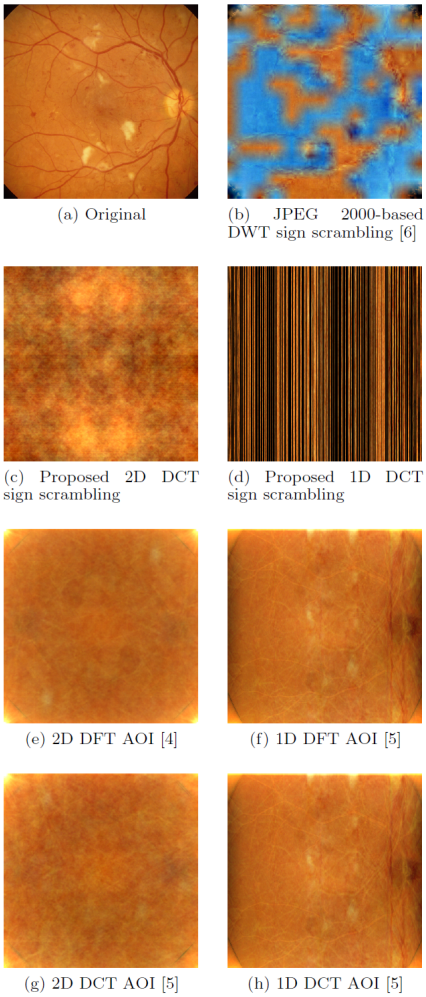


Fig.13: *Copyright- and privacy-protected diabetic retinopathy diagnosis network using DCT AOI (DCT: discrete cosine transform, IDCT: inverse discrete cosine transform, Q: quantization, Q^{-1}: inverse quantization) [5].*



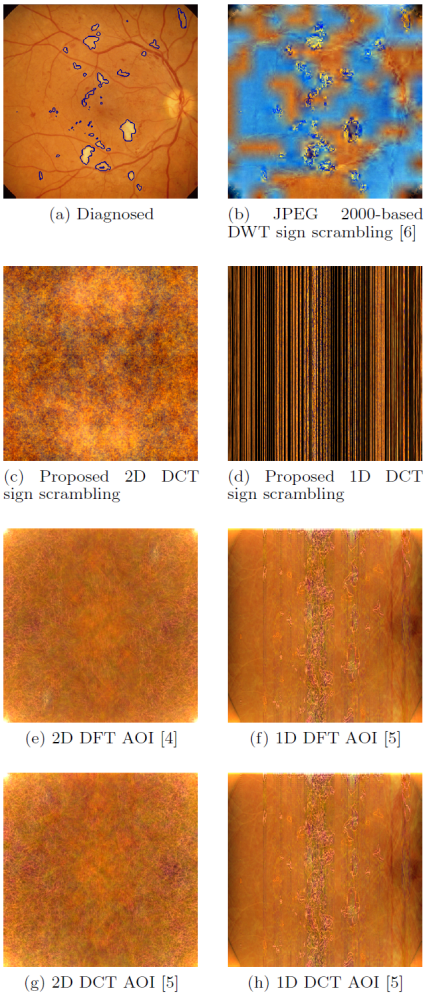
(a) Original (b) JPEG 2000-based DWT sign scrambling [6]

(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling

(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]

(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

Fig 14. Visually encrypted fundus image "HRIS001."



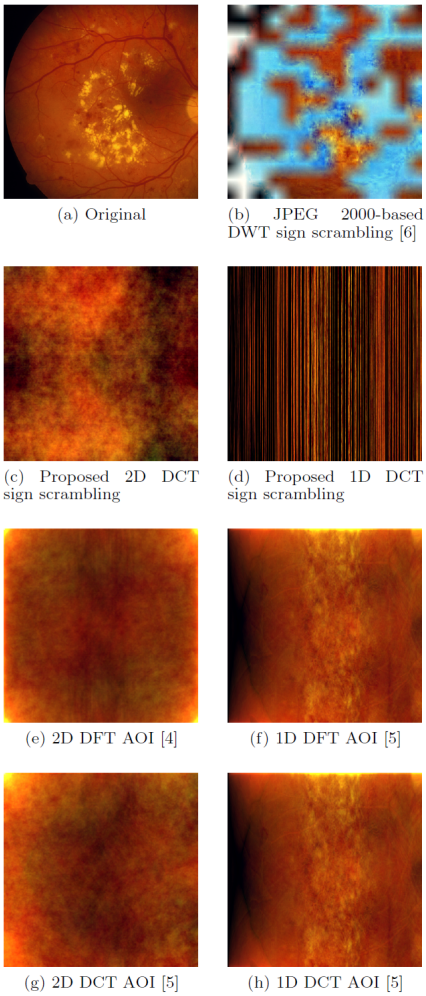
(a) Diagnosed (b) JPEG 2000-based DWT sign scrambling [6]

(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling

(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]

(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

Fig 15. Visually encrypted diagnosed fundus image "HRIS001."



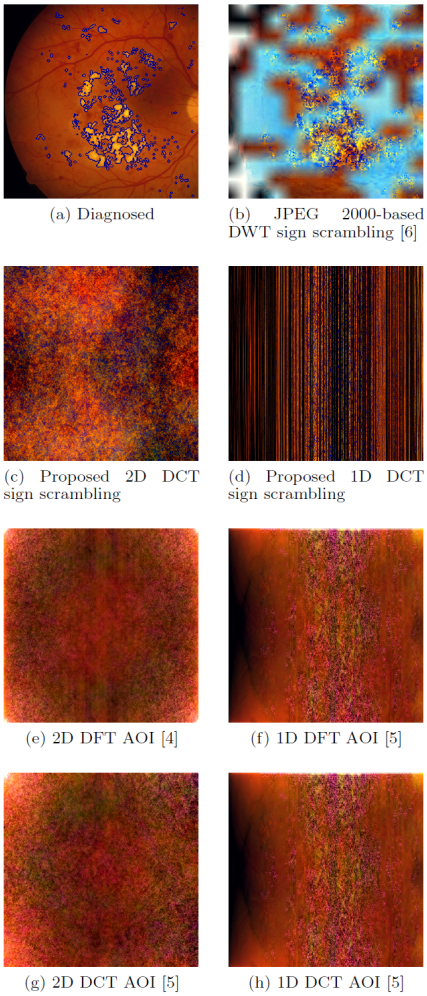
(a) Original (b) JPEG 2000-based DWT sign scrambling [6]

(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling

(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]

(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

Fig 16. Visually encrypted fundus image "HRIS003."



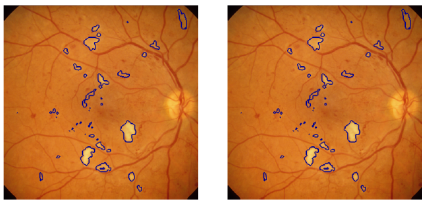
(a) Diagnosed (b) JPEG 2000-based DWT sign scrambling [6]

(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling

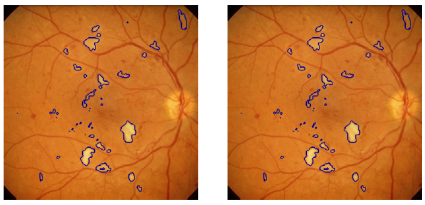
(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]

(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

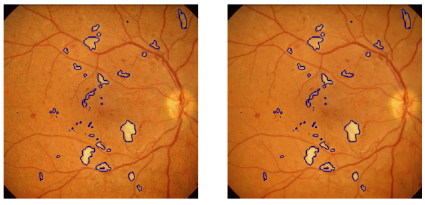
Fig 17. Visually encrypted diagnosed fundus image "HRIS003."



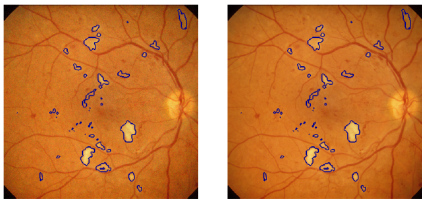
(a) Diagnosed (b) JPEG 2000-based DWT sign scrambling [6]



(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling

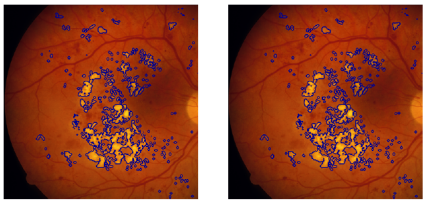


(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]

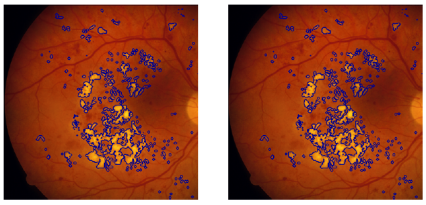


(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

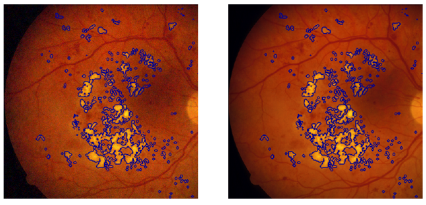
Fig 18. Decrypted diagnosed fundus image "HRIS001."



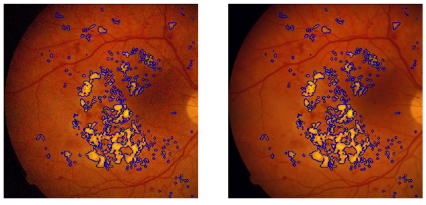
(a) Diagnosed (b) JPEG 2000-based DWT sign scrambling [6]



(c) Proposed 2D DCT sign scrambling (d) Proposed 1D DCT sign scrambling



(e) 2D DFT AOI [4] (f) 1D DFT AOI [5]



(g) 2D DCT AOI [5] (h) 1D DCT AOI [5]

Fig 19. Decrypted diagnosed fundus image "HRIS003."