Healthcare Image Watermarking Scheme Based on Human Visual Model and Back-Propagation Network

Der-Chyuan Lou, Ming-Chiang Hu, and Jiang-Lung Liu

Department of Electrical Engineering, Chung Cheng Institute of Technology, National Defense University

ABSTRACT

In this paper proposed a new healthcare image watermarking scheme based on human visual model and back-propagation network technique. The human visual model which is characterized by properties like luminance, frequency, and texture sensitivities was utilized to generate the suitable strength of an embedded watermark. In addition, the back-propagation network technique was employed to obtain the local characteristic of an image. Experimental results showed that the embedded watermark proposed healthcare image that could survive several kinds of image-processing attacks and the JPEG lossy compression. The proposed image watermarking scheme can be used on the Internet to reduce difficulties that medical personnel may encounter.

Keywords: Healthcare image, back-propagation network, digital watermarking, human visual model, image protection.

倒傳遞類神經網路應用於適應性醫學影像藏密技術

婁德權 胡明強 劉江龍

國防大學中正理工學院電機工程學系

摘　　要

本文提出將倒傳遞類神經網路演算法應用於人類視覺系統對於影像特性的估測，來提高數位浮水印印在醫學影像嵌入的強固性。在本文所提出視覺模式中的敏感度估測之方法，使用三種參數作為代表：亮度敏感度(luminance sensitivity)、頻率敏感度(frequency sensitivity)、對比度敏感度(contrast sensitivity) 。三個參數值將作為倒傳遞類神經網路之輸入資料，用以計算適應性數位浮水印或資訊隱藏量強度係數值，並將估測的結果應用在藏密技術的適應性權值。從實驗結果證明，本文所提出方法被能抵抗各種幾何攻擊及 JPEG 壓縮攻擊，來提高數位浮水印在醫學影像嵌入的強固性，使醫學影像在經網際網路傳遞後，能快速處理醫學影像及正確的判讀，可提高其醫護人員的服務品質。

關鍵字：醫學影像，倒傳遞網路，數位浮水印，人類視覺系統，影像保護

文稿收件日期 97.6.20; 文稿修正後接受日期 97.10.9
Manuscript received June 20, 2008; revised October 9,2008

I. INTRODUCTION

An increasing number of hospital institutions are now using information technology to improve work efficiency, a result of the changing healthcare needs and rapid development of information technology. Through the development and management of health information, we can better safe-keep public health and create new healthcare opportunities.

With the advancement of digital imaging in recent years, MRI, CT, and digital angiography have become new favorites in medical care practices. The imaging technology can not provide fast and accurate examination results, but it can assist surgeons in the precise positioning of surgery sites, avoiding unnecessary harms to healthy tissues and evaluating post-operative results. With no doubt, medical imaging equipment has taken on a crucial role in diagnosis and treatment of diseases. The image guidance system will surely bring a new wave of change in clinical practices [1].

In 2006, Lu [2] proposed a dynamic workflow Management system in biomedical research. The convergence of life sciences, healthcare, and information technology has been is required to create revolutionary discovery of new treatments and the practice of medicine. Thus, clinical records of patients contain may many categories and huge amount of data. Medical institutes only keep a part of unusual or important records. When litigation occurs, the records may turn out to be insufficient. Therefore, digitalization is now becoming popular, and information security is now given a more serious concern.

One method of embedding a watermark enduringly is the imperceptible digital watermarking method. By carrying some information about the ownership and identification of the intellectual property, the continuation of the watermark is almost imperceptible by human visual system (HVS). Information related with all intellectual possessions on documents available or disseminated on network surroundings have to be protected alongside piracy and malevolent manipulation. Even though encryption technique is possible to provide protected deliverance of precious information by deterring counterfeiters from hijacking the copyrighted information, it fails to organize the sharing of the prohibited copies of the unique work after decryption by the certified recipients. Imperceptible digital watermarking schemes could be applied to confirm the image legality and proposition of the sharing of its acceptable copies.

Digital watermarking technique has four main applications, including copyright protection, traitor tracking, copy protection, and image authentication [3-8]. Even though there are noticeable differences between usages and applications, a good watermarking technique must possess some common characteristics such as robustness, imperceptibility, security, and reliability.

The watermarking techniques proposed in the literature fall in two categories: spatial-domain methods and transform-domain methods. The spatial-domain technique processes the location and luminance of the image pixel directly. The simplest method is the least-significant-bit (LSB) substitution method which replaces the low-order bits of pixels of the cover image with the watermark bits.

In 2000, Lee and Chen [8] proposed a k-bits (k=3) LSB-based data hiding scheme, which computes the difference of contiguous pixels to obtain the hiding capacity of each pixel. In 2000, Wu and Tsai [9] utilized the image difference of pixel values to embed converted data into a grayscale wrap image. In 2001, Chang and Hwang [10] used the human visual system (HVS) and the active LSB to perform data hiding. In 2001, Wang et al. [11] proposed an LSB-based image hiding method that uses the hereditary algorithm to discover the most favorable bisection function solution for k-bits LSB substitution. In 2003, Chang et al. [12] used a dynamic programming approach to find an optimal LSB data hiding method. In general, these methods in the spatial domain can offer high hiding-capacity and keep image quality.

Transform-domain methods [4, 7, 13-20] modulate the transformed coefficients of the host image with the watermark information. The watermark is hidden in the low-frequency or middle-frequency coefficients of the protected image because the high-frequency coefficients are more likely to be suppressed by compression. Therefore, how to select the best frequency portions of an image to hide watermark is very important. In general, compared with spatial-domain methods, transform-domain methods have several advantages. First, they are more robust than the spatial-domain methods for attackers to extract and alter the watermark since the watermark is irregularly distributed all over the host image. Second, everyone can select certain bands that possess perceptually significant features to embed a watermark. Third, by modifying transform-domain

coefficients, the visual artifacts of the watermarked image can be reduced even though the watermark is introduced into the selected coefficients.

In 1995, Zhao and Koch [13] proposed a watermarking scheme based on discrete cosine transform (DCT). In their approach, an image is segmented into 8 by 8 blocks first, and then each block is transformed into 64 DCT coefficients. In the 64 DCT coefficients, three coefficients are selected from a predefined set of eight coefficients to cover the low-frequency and medium-frequency bands of the image block. In general, high frequency coefficients will be truncated and low frequency coefficients can survive after image compressing. Hence, altering only the low frequency components will make the watermark more resilient to attacks. However, as only 3/64 of the coefficients are used to embed the watermark, the amount of watermark information that can be embedded is limited.

In 1997, Cox et al. [4] proposed a famous spread-spectrum watermarking scheme. They used a spread-spectrum-like method to insert watermark into the perceptually most significant spectral components of an image. The watermark is a sequence of real numbers $X = \{x_1, \ldots, x_n\}$ with a normal distribution N(0, 1) that has zero mean and a variance of one. The watermark X is inserted into the original image $V=\{v_1, \ldots, v_n\}$ to produce the watermarked image V'. The embedding process of watermark can be described as one of the following equations:

$$v_i' = v_i + \alpha x_i, \quad (1)$$

$$v_i' = v_i(1 + \alpha x_i), \quad (2)$$

$$v_i' = v_i + e^{\alpha x_i}, \quad (3)$$

where v_i refers to the selected DCT coefficient of image V, and α is the strength weight of the watermark X. The Eq. (1) may not be suitable when v_i varies violently. The other two equations, Eq. (2) and Eq. (3), are more adaptive to the variation of v_i. However, how to select the strength weight α had not been discussed and the length n of the watermark is static in Cox et al.'s scheme. Applying the knowledge of human visual model to the watermarking schemes, Cox et al.'s scheme can be improved by introducing the adaptive strength value α_i for different spectrum component v_i s. It means that the strength weight α can be adjusted by using the human visual model to determine the bound of watermark strength. This allows us to provide the maximum strength watermark on the considerations of imperceptibility and robustness.

In 1999, Hsu and Wu [14] proposed another block-wise DCT-based watermarking scheme which uses a recognizable binary pattern to be the watermark. The watermark is permutated first, and then shuffled into every image block according to the variances of the image blocks. However, as only a single bit of the coefficients is used to embed the watermark, the amount of watermark information that can be embedded is also limited.

In 2002, Chang et al. [17] proposed a Fuzzy-ART based digital watermarking scheme to improve the robustness of Hsu and Wu method [14]. Chang et al. applied fuzzy technology on watermarking, Mei [20] proposed decision of image watermarking strength. He applied artificial neural-networks technology on watermarking in different blocks to adjust each embedded volume, and this created a solution watermarking for robustness. However, the human visual characteristics such as texture, brightness, and others have not been explored in the methods used by Chang et al. [17] and Mei [20].

In this paper, a block-wise DCT domain watermarking scheme is proposed. In the proposed approach, we use the human visual model and back-propagation network adaptive resonance theory (BPN-ART) to train each host image independently and to identify good-locations for watermark insertion according to the user-specified parameters. This provides a suitable power subject to the imperceptibility constraint. Thus, the clustering result would be very different from image to image, which leads to a diversity of embedding strengths. Therefore, the attackers cannot counterfeit watermark by simply replacing a similar block from a watermarked image [20]. A formal analysis of the proposed watermarking scheme resistance against the counterfeiting attack is provided at the end of this paper.

The rest of this paper is organized as follows. Section II describes the proposed watermarking scheme. Several experiments are drawn in Section III to demonstrate the superior robustness of the proposed watermarking scheme against common image processing attacks. A formal robustness analysis against counterfeiting attacks is also given. Section IV concludes this paper.

II. The Proposed Watermarking Scheme

In the section, we propose a back-propagation network algorithm and DCT-based adaptive digital

watermarking scheme. The human visual model and BPN-ART algorithm used in the proposed watermarking scheme are first introduced.

2.1 Resolving the Human Visual Model

The human visual model used by the proposed scheme is characterized by three properties: luminance, frequency, and texture sensitivities. The sensitivity of the human visual model and membership function mapping input/output variables to HVS set are shown in Table 1 and Fig. 1, respectively.

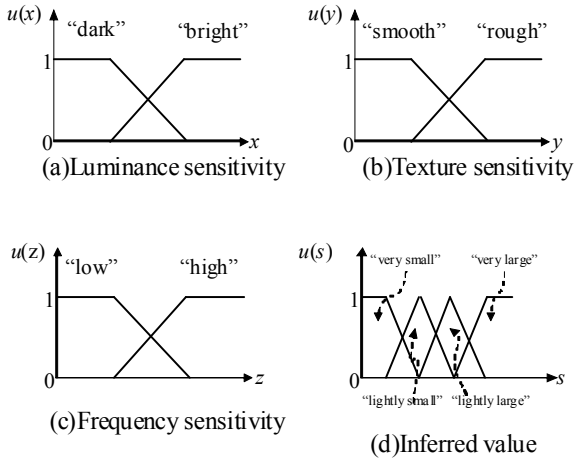


Fig. 1. The membership function mapping input/output variables to HVS set.

Table 1. Sensitivity of the human visual model.

Sensitivity	Minimum		Maximum	
Luminance	highest bright	lowest bright	lowest dark	highest dark
Frequency	supreme	second	median	lowest
Contrast	highest	second	low	lowest

All the DC components of DCT blocks of an image are used as the luminance sensitivity. The JPEG quantization table is used as the frequency sensitivity. The DCT coefficients are then quantized by using the frequency sensitivity, and the number of non-zero coefficients serves as the texture sensitivity. Detailed description of the adopted human visual model is stated below.

(1). The luminance sensitivity: The luminance sensitivity L_k is estimated by the following equation:

$$L_k = \frac{X_{DC,k}}{\overline{X}_{DC}}, \tag{4}$$

where X_{DC}, k denotes the DC coefficient of the k_{th} block, and $\overline{X}_{DC}$ is the mean value of all blocks' DC coefficients.

(2). The frequency sensitivity: The JPEG quantization table Q(x, y) is used as the frequency sensitivity, which is shown in Fig. 2.

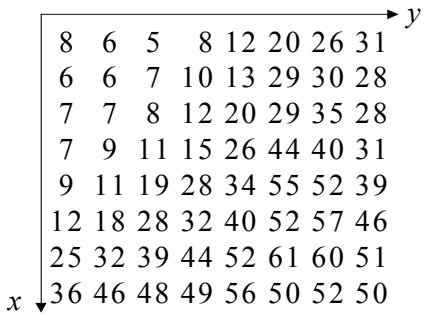


Fig. 2. The frequency sensitivity.

(3). The contrast sensitivity: The pixel in the image block, minimum difference of largest and gray steps value of gray steps value, The contrast sensitivity can be described in the following equation:

$$Contrast = \max(z_{ij}) - min(z_{ij}),$$
$$\text{for } i, j = \{0,1,2,3\} \tag{5}$$

2.2 The Back-Propagation Network Algorithm

The topological structure of the neural network architecture and the flowchart of back-propagation network algorithm are shown in Fig. 3 and Fig. 4, respectively.

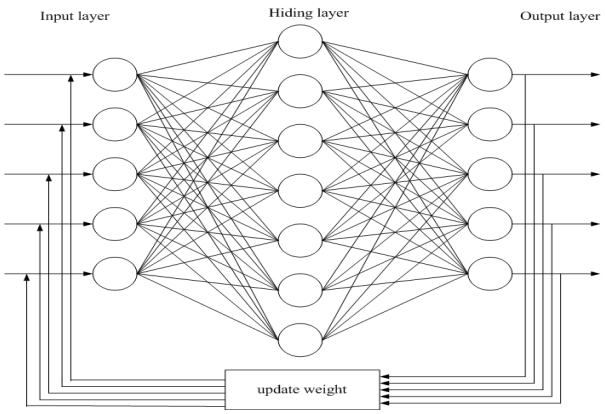


Fig. 3. Topological structure of the neural network architecture.

In order to solve the problem that the watermark or the information floats to hide quantity in the adaptability of the systematic way of human vision, the interface of intelligence based on BPN

relation, this chapter puts forward the following basic rule inference knowledge:

(1). If the image is highest dark, highest smooth, and lowest, it is too little to hide the quantity of entering information.
(2). If the image is highest dark, highest smooth, and median, it is slightly little to hide the quantity of entering information.
(3). If the image is highest dark, median smooth, and lowest, it is slightly little to hide the quantity of entering information.
(4). If the image is highest dark, median rough and median, it is little to hide the quantity of entering information.
(5). If the image is lowest bright, lowest rough and second, it is little to hide the quantity of entering information.
(6). If the image is lowest dark, highest rough and second, it is slightly large to hide the quantity of entering information.
(7). If the image is lowest bright, highest rough and second, the quantity of entering is information message slightly little to hide.
(8). If the image is lowest bright, highest rough, and supreme, it is slightly large to hide the quantity of entering information.
(9). If the image is highest bright, rough and supreme, it is slightly large to hide the quantity of entering information.
(10). If the image is highest bright, highest rough, and supreme, it is extremely large to hide the quantity of entering information.

In the neural inference system, the systematic knowledge of human vision on the foundation can treatment course of the neural inference system.

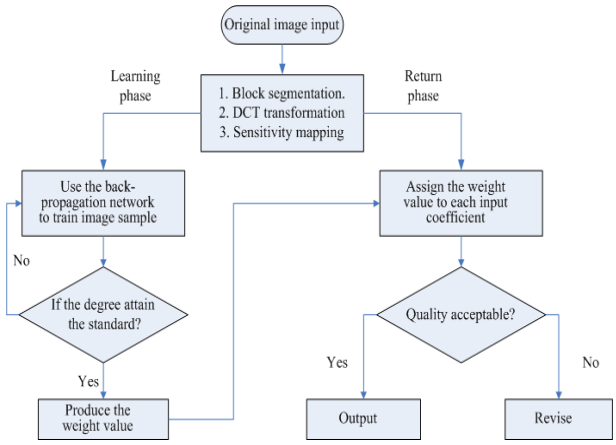


Fig. 4. The flowchart of the back-propagation network processes.

The topological structure of the neural network architecture is composed of three layers. [21,22] The first layer is to present the input variables of network. The processing units depend on problems. Each human visual feature vector has twelve elements to be the input variables in this study. The neurons in this layer use a linear transform function. The second layer, which is a hiding layer, serves to explain the interactions among input variables. There is no optimal method to decide the numbers of processing units of the hiding layer. The neurons in the hiding layer use a non-linear transform function. The value of the hiding layer in the study equals to 1 and the number of processing units is 15. The third layer is the output level that presents output variables of this network. The number of processing units of this layer also depends on problems. There are three kinds of human visual characteristics so that the output variable is 4. The neurons in the output layer also use a non-linear transform function. The neural network system can be designed according to the human visual characteristics for each of the watermark element.

2.3. The Proposed Watermark Embedding Process

Normally, a reasonable transaction is to embed the watermark in the middle-frequency band of images [18]. Hence, the proposed watermarking scheme only embeds the watermark information into the coefficients selected from the middle-frequency band (shown as Fig. 5) according to the cluster features. The adaptive watermark embedding process is illustrated in Fig. 6. The detailed steps of the proposed watermark embedding process are described as follows.

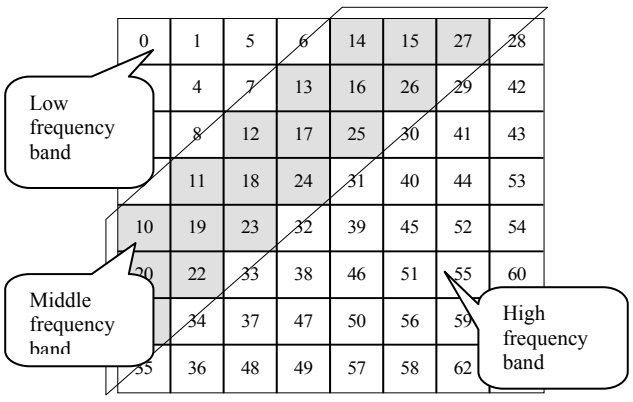


Fig. 5. Definition of the middle-frequency band.

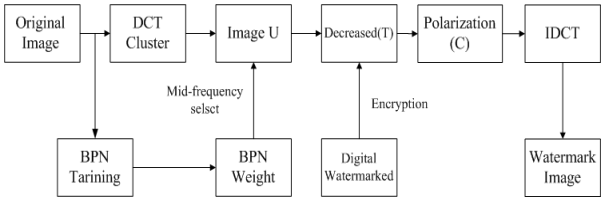


Fig. 6. The watermark embedding process.

(1). Divide the host image into non-overlapping 8×8 blocks (B_i) and transform each block to frequency coefficient by the DCT technique (U_i). The 8×8 blocks and transformation can be described in the following equation:

$$B = \sum_{i=1}^{k} B_i = B_1 \| B_2 \| ... \| B_k , \quad (6)$$

$$U = \mathrm{DCT}(B) = \mathrm{DCT}(B_1) \| \mathrm{DCT}(B_2) \| ... \| \mathrm{DCT}(B_k) = U_1 \| U_2 \| ... \| U_k \quad (7)$$

(2). Convert each DCT block (U_i) to the 1×64 array according to a raster scan. Each DCT block (U_i) expands each array to an array (U_{ni}) of dimension 1×128 with the element values lying between 0 and 1 to form the input training patterns for the BPN operation. The U_i and U_{ni} can be described in the following equation:

$$U_n = U_{n1} \| U_{n2} \| ... \| U_{nk} , \quad (8)$$

$$U_{ni} = (n_i, n_i^c) = (n_{i1}, n_{i2}, ..., n_{i64}, n_{i1}^{'}, n_{i2}^{'} ... n_{i64}^{'}) \quad (9)$$

where $1 \le i \le k$ and $n_{il}^{'} = 1 - n_{ik}$, for $k = 1, 2, ..., 64$.

(3). The back-propagation network algorithm (BPN) weight α_i can be described in the following equation:

$$\alpha_F = \alpha(B_i) = BPN(L_k, Q_k, C_k), \quad (10)$$

(4). Input all input arrays to the back-propagation network for classification. The back-propagation network algorithm function produces two outputs: a weight matrix (W_m) and a codebook (C_b). The (W_m, C_b) can be described in the following equation:

$$(W_m, C_b) = BPN(U_n, \alpha_F, \beta_F, \eta_F), \quad (11)$$

where α_F is the choice BPN parameter, β_F is the BPN learning rate, and η_F is the BPN vigilance parameter.

(5). Input vector U to normalize ζ The ζ is constant and greater than zero that $|U| = \varsigma$ for any input vectors. Select 64× ζ DCT coefficients from each candidate block *Ti*, where ζ . is the fraction of selected blocks. The selected coefficients form a decreased macro block D whose size is the same as that of encrypted watermark block, which can be described in the following equation:

$$D = \mathrm{Decreased}(T) = \mathrm{D}(T_1) \| \mathrm{D}(T_2) \| ... \| \mathrm{D}(T_k) = D_1 \| D_2 \| ... \| D_K . \quad (12)$$

(6). The embedding process can be modeled mathematically that localized gain factor an adjust the block DCT to coefficients sensitivity D^* and U^* instead of modifying the selected coefficients with a uniform gain factor globally. This can be described in the following equation:

$$U^* = K(I, W), \quad (13)$$

$$D^* = K(U, W) = K_1(D_1, W_1) \| K_2(R_2, W_{e2}) \| ... \| K_q(R_q, W_q) = D_1^* \| D_2^* \| ... \| D_q^* , \quad (14)$$

$$D_i^*(k,l) = D_i(k,l) \pm \alpha(i) |D_i(k,l)| \quad (15)$$

where K is the encryption key, I is the original image, W is the watermark information, $D_i(k,l)$ is the DCT coefficients value at match (k,l) of the decreased macro block D_i , and α_i is the embedding strength gain factor in the decreased block D_i .

(7). Enhancement of the pixels is accompanied by diffusing of the background pixels in the recovery process. The convergence of each DCT coefficient within each compact image block is computed by using a two-dimensional (2-D) pattern mask (C_i) . The polarization C_i can be described in the following equation:

$$C_i = C(D_1) \| C(D_2) \| ... , \quad (16)$$

$$C_i(k,l) = \begin{cases} 1, & \text{if } D_i(k,l) > \beta_i \\ 0, & \text{otherwise} \end{cases} , \quad (17)$$

where β_i is the average value of selected frequency coefficients .

(8). Modify frequency coefficients D^* , then match them into U to obtain U^*. The U^* can be described in the following equation:

$$U^* = D^* \| U_x , = D_1^* \| D_2^* \| ... \| U_1^* \| U_2^* \| ... \| U_k^* \quad (18)$$

where U_x is DCT coefficients that aren't

chosen for modulation.

(9). Perform an inverse block DCT (IDCT) to obtain the watermarked image, i.e.,

$$B^* = IDCT(B^*), \tag{19}$$

2.4 The Proposed Watermark Extraction Process

The watermark extraction process requires the original image. The adaptive watermark extraction process is illustrated in Fig. 7 and described as follows:

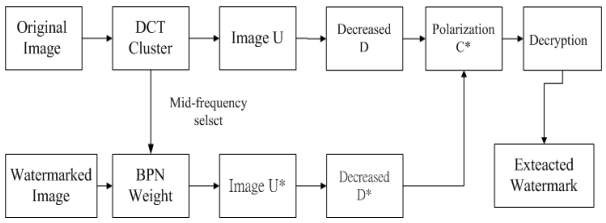


Fig. 7. The watermark extraction process.

(1). Partition the original image and the assumed image into non-overlapping 8×8 blocks and transform each block to frequency coefficients by the DCT technique. The 8×8 blocks and the transformation done can be described as the following equation:

$$B = \sum_{i=1}^{k} B_i = B_1 \| B_2 \| ... \| B_k \ , \tag{20}$$

$$B^{'} = \sum_{i=1}^{k} B_i^{'} = B_1^{'} \| B_2^{'} \| ... \| B_k^{'} \ , \tag{21}$$

$$\begin{aligned} U &= \mathrm{DCT}(B) \ , \\ &= \mathrm{DCT}(B_1) \| \mathrm{DCT}(B_2) \| ... \| \mathrm{DCT}(B_k) \\ &= U_1 \| U_2 \| ... \| U_k \ , \end{aligned} \tag{22}$$

$$\begin{aligned} U^{'} &= \mathrm{DCT}(B^{'}) \\ &= \mathrm{DCT}(B_1^{'}) \| \mathrm{DCT}(B_2^{'}) \| ... \| \mathrm{DCT}(B_k^{'}) \\ &= U_1^{'} \| U_2^{'} \| ... \| U_k^{'} \ , \end{aligned} \tag{23}$$

where B_i is the host image with non-overlapping 8×8 blocks, $B_i^{'}$ is the corrupted watermarked image with non-overlapping 8×8 blocks, U_i is the host image transformed in each block to frequency coefficient by the DCT technique, and $U_i^{'}$ is the corrupted watermarked image transformed in each block to frequency coefficient by the DCT technique.

(2). Expand each array to an array of dimension 1×128. The back-propagation network algorithm weight α_k with the element values can be described as Eq .(9) and Eq .(10)

(3). Extract the candidate blocks according to the location map of the selected blocks from the compact macro blocks, i.e.,

$$D = Decreased(T) \tag{24}$$

$$D^{'} = Decreased(T^{'}) \tag{25}$$

where T is the extracted host image, and from it, the decreased macro blocks (D) are formed. $T^{'}$ is the extracted corrupted watermarked, and from it, the decreased macro blocks ($D^{'}$) are formed.

(4). Produce the polarization pattern mask by subtracting the original compact image from the assumed compact image. Eq. (26) container is used to explain the proposed polarization pattern mask:

$$C_i^{'}(k,l) = \begin{cases} 1, & \text{if } D_i^{'}(k,l) - D_i(k,l) > 0 \\ 0, & \text{otherwise} \end{cases} . \tag{26}$$

(5). Extract the watermark by simple logical XOR (Exclusive-OR) operation. The simple logical XOR can be described as the following equation:

$$W^{'} = \mathrm{XOR}\ (C, C^{'}). \tag{27}$$

(6). Use the secret key to recover the watermark, i.e.,

$$W^{*} = Decrypt(W^{'}, K) \tag{28}$$

Generally, the visual quality of the embedded image can be measured by using the peak signal to noise ratio (PSNR) which is defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \ (\mathrm{dB}), \tag{29}$$

where MSE is the mean square error between the original image X and the target image X' and this error is defined as:

$$MSE = \frac{1}{M} \sum_{i=1}^{M} (X_i - X_i')^2 , \tag{30}$$

where M denotes the number of pixels in each image.[23]

III. THE EXPERIMENTAL RESULTS

To evaluate the performance of the proposed watermarking scheme, the proposed watermarking scheme was tested in four medical images of 512×512 sizes with difference texture complexity to be the original images (shown as Fig. 8.). The

medical images were applied through DICOM outcome. The source was provided by Dr. Chen, Zong-Zhe, Department of Medical Imaging Technology, Shu Zen College of Medicine and Management. A binary random sequence generated by MATLAB 7.0. The was binary image ("CCIT" and "中") was taken as the watermark and was embedded it in the original healthcare color image shown in Fig. 8. The test healthcare images were estimated by the human visual model and the extracted features are clustered by the back-propagation network algorithm described in Section 2. The watermarked image was attacked by various image-processing operations including cropping, compression, Gaussian noise adding, scale, and sharpening. The performances of the proposed watermarking scheme were also compared with Cox et al.'s scheme [4]. Besides offering the assessment value using PSNR to do the image [23] this paper offers NC value to ensure that several watermarks coming in are getting stronger. The details of the experiments are described in the following subsections:

3.1 Cropping Attack

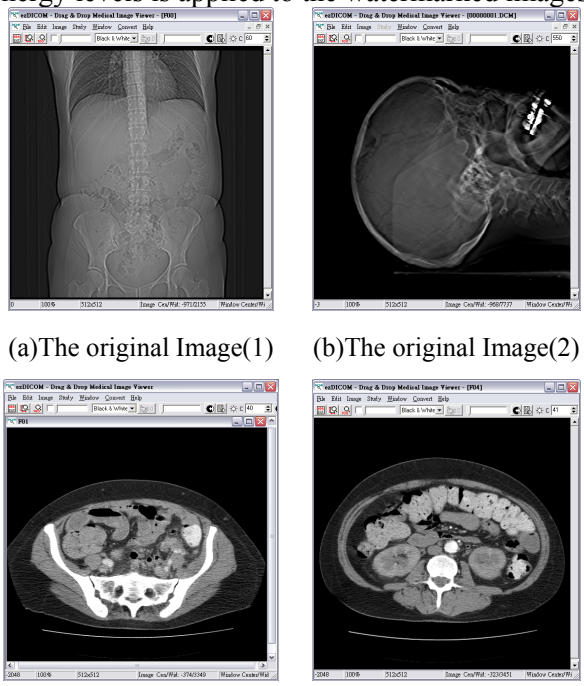
Cropping is the easiest operation among popular image manipulations. In this paper, each watermarked image is subjected to a wide range of cropping ratios. Fig. 9 is an example of the cropped image. The experimental results are shown in Table 2. It has been found that the watermark can survive large cropping ratio in all seven types (left 1/2, right 1/2, upper 1/2, lower 1/2, center part with 1/16, center part with 1/8, and center part with 1/4) of test images. This can be explained by the fact that the selected blocks are distributed all over the image and the cropped area may contain only a fraction of embedded information. The risk of losing large amount of information may happen only if the selected blocks are concentrated in some areas of the watermarked image.

3.2 Compression Attack

Being the most classical and ubiquitous image processing attack, JPEG compression with various compression ratios is applied to the watermarked images. Fig. 10 shows a JPEG-compressed image. The experimental results are shown in Fig. 11. The superior performance is due to the appropriate choice of watermark insertion regions coupled with the adaptive embedding strength.

3.3 Additive Guassian Noise Attack

In this set of tests, Guassian noise of different energy levels is applied to the watermarked images,



(a)The original Image(1) (b)The original Image(2)

©The original Image(3) (d)The original Image(2)

The watermark is "中"

The watermark is "CCIT"

Fig. 8. The experimental original healthcare X-ray images using DICOM and watermarking.

so as to test the robustness against additive Gaussian noise attacks. The watermarked images are added in 0%, 5%, 10%, 15% and 20% Gaussian noise. Fig. 10 shows a Gaussian-noise added image. The experimental results are shown in Table 3.

3.4 Additive Guassian Noise Attack

In this set of tests, Guassian noise of different energy levels is applied to the watermarked images, so as to test the robustness against additive Gaussian noise attacks. The watermarked images are added in 0%, 5%, 10%, 15% and 20% Gaussian noise. Fig. 10 shows a Gaussian-noise added image. The experimental results are shown in Table 3.

3.5 Sharpening and scale Attack

The watermarked image is sharpened for the 4th and scale attack. The watermark is then extracted from the corrupted image. Fig. 10 shows a sharpened image. The experimental results are shown in Table 4. It is clear that the detection

response of the proposed scheme outperforms Cox et al.'s scheme [4].

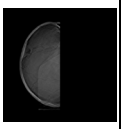
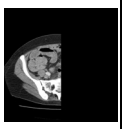
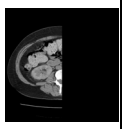
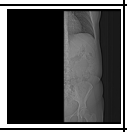
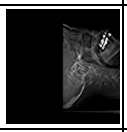
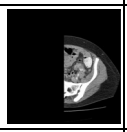
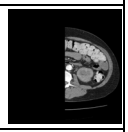
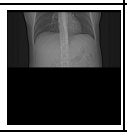
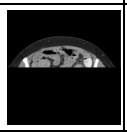
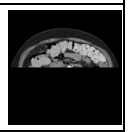
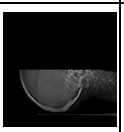
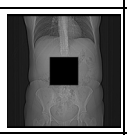
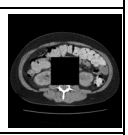
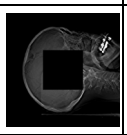
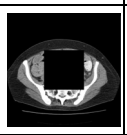
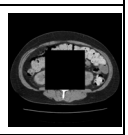
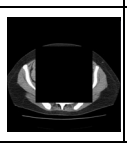
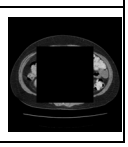
Cropping	Medical image(1)	Medical image(2)	Medical image(3)	Medical image(4)
Left 1/2				
Right 1/2				
Upper 1/2				
Lower 1/2				
Center part with 1/16				
Center part with 1/8				
Center part with 1/16				

Fig. 9. Illustration of cropping the attacked images.

Table 2. The PSNR and NC values of the extracted watermark by cropping the boarder of the watermarked images in different shape proportions.

Image(1)	Left 1/2	Right 1/2	Upper 1/2	Lower 1/2
PSNR (Cox)	19.39	17.25	18.43	16.87
PSNR (BPN)	24.03	21.53	22.93	21.07
NC (BPN)	0.729	0.703	0.727	0.693
Extracted watermark				
Image(2)	Left 1/2	Right 1/2	Upper 1/2	Lower 1/2
PSNR (Cox)	20.04	17.83	18.05	19.44
PSNR (BPN)	24.78	22.23	20.65	22.77
NC (BPN)	0.736	0.742	0.689	0.751
Extracted watermark				
Image(1)	Center part 1/16	Center part 1/8	Center part 1/4	
PSNR (Cox)	38.89	30.53	25.12	
PSNR (BPN)	42.36	35.25	30.12	
NC (BPN)	0.922	0.8371	0.773	
Extracted watermark				
Image(2)	Center part 1/16	Center part 1/8	Center part 1/4	
PSNR (Cox)	39.21	31.56	25.97	
PSNR (BPN)	43.41	36.19	29.96	
NC (BPN)	0.949	0.886	0.803	
Extracted watermark				

	Medical image(1)	Medical image(2)	Medical image(3)	Medical image(4)
JPEG compressed				
Scale				
Gaussian noise added				
Sharpened 4th				

Fig. 10. Illustration of the attacked images: JPEG compressed, scale, Gaussian noise added, and sharpened.

Table 3. The PSNR and NC values of the extracted watermark by adding the Gaussian-noise to the watermarked images.

Image(3)+CCIT	0%	5%	10%	15%	20%
PSNR (Cox)	46.831	43.62	41.738	38.044	35.3
PSNR (BPN)	55.92	51.27	46.715	41.48	40.65
Extracted watermark					
Image(4)+CCIT	0%	5%	10%	15%	20%
PSNR (Cox)	44.978	41.202	39.37	37.304	33.851
PSNR (BPN)	53.97	50.251	47.752	43.428	39.126
Extracted watermark					

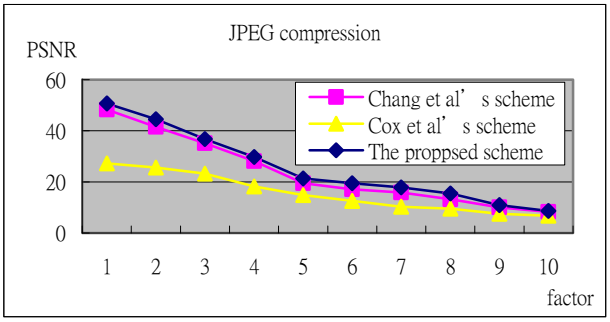


Fig. 11. Detection responses of the JPEG compression attack.

Table 4. The PSNR and NC values of the extracted watermark by scaling and sharpening of the watermarked images.

Scaling			Sharpening		
Image(3)+"中"	PSNR (Cox)	24.940	Image(3)+"中"	PSNR (Cox)	23.634
	PSNR (BPN)	29.43		PSNR (BPN)	27.85
	NC (BPN)			NC (NNS)	
Image(4)+"CCIT"	PSNR (Cox)	27.40	Image(4)+"CCIT"	PSNR (Cox)	25.05
	PSNR (BPN)	31.47		PSNR (BPN)	30.952
	NC (BPN)			NC (BPN)	

IV. CONCLUSIONS

With an aging population and changes in the health insurance system, countries around the globe have become more actively involved in medical technology innovation and development, utilizing information and communication technology to create an advanced e-medical service system. Information technology can allow fast processing of large quantity of data, offer energy savings, and contribute to environmental protection by eliminating too much paper work. Therefore, more and more industries have integrated with information technology to improve work efficiency. The healthcare industry has especially invested a large amount to manpower and equipment to design a clinical and operational information system to improve medical service quality. Thus, the security that medical imaging conveys in the network needs special attention.

In this paper, a novel healthcare image watermarking scheme based on the human visual model and back-propagation network technique is proposed. The human visual model is utilized to generate the suitable strength of embedded watermark and can be described in terms of three properties: luminance, frequency, and contrast sensitivities. The back-propagation network technique is employed to obtain the local characteristics of images. To test the robustness of the proposed watermarking scheme, several experiments have been conducted. Experimental results show that the proposed technique can survive several kinds of image processing attacks and the JPEG lossy compression. The experimental results were also compared with Cox et al.'s [4] watermarking schemes, and the results show that the proposed scheme outperforms Cox et al.'s [4] scheme against various attacks. The system can be used on the Internet and helps reduce the difficulty that any medical personnel encounter.

ACKNOWLEDGMENTS

This work was supported partially by the National Science Council of Republic of China under grant NSC 97-2221-E-606-016-.

REFERENCES

[1] Hung, C., "The Trend of health Information and Communication Technology Development," Proc. 16th Annual International Wu Ho-Su Memorial Symposium on Health Information Technology, Taipei, 2008, pp. 2-5, 2008.

[2] Lu, C. H., Deng, Y. W., and Huang, S. C., "Dynamic Workflow Management System in Biomedical Research," Proc. IBM Greater China Group's Technical Conference, pp. 124-127, 2006.

[3] Luo, W., Heileman, G. L., and Pizano, C. E., "Fast and Robust Watermarking of JPEG Files," Proc. IEEE 5th Southwest Symp. Image Analysis and Interpretation, pp. 158-162, 2002.

[4] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia," J. IEEE Trans. Image Process, Vol. 6, No. 12, pp. 1673-1687, 1997.

[5] Rey, C., and Dujelay, J. L., "Blind Detection of Malicious Alterations on Still Images Using Robust Watermarks," Proc. IEE Secure Images and Image Authentication Colloquium, London, session 7, pp. 1-6, 2000.

[6] Dautzenberg, C., and Boland, F. M., "Watermarking Images," Dept. Electron. and Elect. Eng., Trinity College Dublin, Tech. Rep., 1994.

[7] Eggers, J. J., and Su, J. K., "A Blind Watermarking Scheme Based on Structured Codebooks," Proc. IEE Secure Images and Image Authentication Colloquium, London, session 4, pp. 1-21, 2000.

[8] Lee, Y. K., and Chen, L. H., "High Capacity Image Steganographic model," J. IEE Vision, Image, Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[9] Wu, D. C., and Tsai, W. H., "Spatial-domain Image Hiding Using an Image Differencing," J. IEE Vision, Image, Signal Processing, Vol. 147, No. 1, pp. 29-37, 2000.

[10] Chang, C. C., and Hwang, K. F., "Hiding Images using Dynamic Bit-replacement and Human Visual System," Distributed Multimedia Databases: Techniques and Applications, Chapter 16, Idea Group Publishing, USA, p. 190-205, 2001.

[11] Wang, R. Z., Lin, C. F., and Lin, J. C., "Image Hiding by Optimal LSB Substitution and Genetic Algorithm." J. Pattern Recognition, Vol. 34, pp. 671-683, 2001

[12] Chang, C. C., Hsiao, J. Y., and Chan, C. S., "Finding Optimal LSB Substitution in Image Hiding by Using Dynamic Programming Strategy, " J. Pattern Recognition, Vol. 36, pp. 1583-1595, 2003.

[13] Zhao, J., and Koch, E., "Embedding Robust Labels into Images for Copyright Protection. Proc. Int. Congress IPR for Specialized Information," Knowledge and New Technologies, Vienna, Austria, pp. 242-251, 1995.

[14] Hsu, C. T., and Wu, J. L., "Hidden Digital Watermarks in Images," J. IEEE Trans. Image Process, Vol. 8, No.1, pp. 58-68, 1999.

[15] Ruanaidh, J. K. O., Dowling, W. J., and Boland, F. M., "Watermarking Digital Images for Copyright Protection," J. IEE Proceeding Vision, Image, Signal Processing, Vol. 143, No. 4, pp. 250-256, 1996.

[16] Hu, M. C., Lou, D. C., and Chang, M. C., "Dual-wrapped Watermarking Scheme for Image copyright protection," J. Computers & Security, Vol. 26, No. 4, pp. 319-330, 2007.

[17] Chang, C. H., Ye, Z., and Zhang, M., "Fuzzy-ART Based Digital Watermarking Scheme," J. IEEE Trans. on Circuits and Systems for Video Technology, Vol. 15, No.1, pp. 65-81, 2002.

[18] Hu, M. C., Lou, D. C., and Tso, H. K., "Digital Watermarking Method Using Compression Concept and Coefficient Difference," J. The Imaging Science. Vol. 55, No. 3, pp. 155-163, 2007.

[19] Carpenter, G. A., Grossberg, S., and Rosen, D. B., "Fuzzy ART: An Adaptive Resonance Algorithm for Rapid, Stable Classification of Analog Patterns," Proc. Int. Joint Conf. Neural Networks, pp. 411-416, 1991.

[20] Mei, S. C., Li, R. H., Dang, H. M., and Wang, Y. K., "Decision of Image Watermarking Strength Based on Artificial Neural-Networks," Proc. of the 9th International Conference on Neural Information Processing, Singapore, pp. 2430-2434, 2005.

[21] Sarle, W. S., "Neural Networks and Statistical Models," Proc. 19th Annu. SAS User Group Int. Conf., pp. 1538-1550, 1995.

[22] Bender, W., Gruhl, D., Morimoto, N., and Lu, A., "Techniques for Data Hiding," J. IBM Syst., Vol. 35, No. 3&4, pp. 313-336, 1996.

[23] Lou, D. C., Hu, M. C., and Liu, C.L., "Multiple-layer Data Hiding Scheme for Medical images," J. Computer Standards & Interfaces, No: CSI-D-05-00026, 2008.