Expert Systems with Applications 41 (2014) 3178–3188

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Reversible watermarking scheme for medical image based on differential evolution

Baiying Lei [a], Ee-Leng Tan [b], Siping Chen [a], Dong Ni [a,*], Tianfu Wang [a,*], Haijun Lei [c]

[a] Department of Biomedical Engineering, School of Medicine, Shenzhen University, National-Regional Key Technology Engineering Laboratory for Medical Ultrasound, Guangdong Key Laboratory for Biomedical Measurements and Ultrasound Imaging, Nanhai Ave 3688, Shenzhen, Guangdong 518060, China
[b] School of Electrical and Electronic Engineering, Nanyang Technological University, 639798, Singapore
[c] College of Computer Science and Technology, Shenzhen University, Nanhai Ave 3688, Shenzhen, Guangdong 518060, China

ARTICLE INFO

Keywords:
Reversible watermarking
Differential evolution
Medical image
Recursive dither modulation

ABSTRACT

Currently, most medical images are stored and exchanged with little or no security; hence it is important to provide protection for the intellectual property of these images in a secured environment. In this paper, a new and reversible watermarking method is proposed to address this security issue. Specifically, signature information and textual data are inserted into the original medical images based on recursive dither modulation (RDM) algorithm after wavelet transform and singular value decomposition (SVD). In addition, differential evolution (DE) is applied to design the quantization steps (QSs) optimally for controlling the strength of the watermark. Using these specially designed hybrid techniques, the proposed watermarking technique obtains good imperceptibility and high robustness. Experimental results indicate that the proposed method is not only highly competitive, but also outperforms the existing methods.

1. Introduction

With the rapid development of telediagnosis, telesurgery as well as hospital information system, medical images have become one of the most important tools in helping physicians to determine suitable diagnostic procedures (Das & Kundu, 2012; Giakoumaki, Pavlopoulos, & Koutsouris, 2006; Kong & Feng, 2001; Li & Kim, 2013). Medical images are also essential in evaluating patients' recovery from their treatment (Das & Kundu, 2012; Deng, Chen, Zeng, Zhang, & Mao, 2013; Giakoumaki et al., 2006; Kong & Feng, 2001). However, the sharing, handling, and processing of medical images can lead to security, confidentiality, copyright forgery, and integrity issues. Therefore, it is essential to provide security solutions for medical images to prevent any misuse or violation. To address the security issues related to medical images, Podilchuk and Delp proposed an effective and promising solution using a watermarking technique (Podilchuk & Delp, 2001). Watermarks such as patient-ID, tag, label, trademark, logo or signature is embedded into the multimedia object by changing the pixel gray level values of image without any perceptible changes on the host image (Giakoumaki et al., 2006; Kong & Feng, 2001). In fact, reversible watermarking technique or lossless method (Celik, Sharma, & Tekalp, 2006) is especially useful for medical images as it is possible to recover the original image without any distortion at the receiver side.

To allow doctors to make an accurate diagnosis using medical images, even very small distortion should be avoided in medical applications. Reversible watermarking methods not only meet the watermarking requirements of robustness, imperceptibility and capacity, they also can retrieve the host signal without distortion. Therefore, these methods have been widely applied in the literature (Alattar, 2004; An et al., 2012; Arsalan, Malik, & Khan, 2012; Coatrieux, Le Guillou, Cauvin, & Roux, 2009; Coatrieux, Lecornu, Sankur, & Roux, 2006; Coatrieux, Pan, Cuppens-Boulahia, Cuppens, & Roux, 2013; Deng et al., 2013; Farfoura et al., 2012; Kamran, Khan., & Malik, 2014; Ni, Shi, Ansari, & Su, 2006; Shi & Xiao, 2013; Shih & Wu, 2005; Tian, 2003; Zhang, Bao, Wang, & Xu, 2013) for both copyright protection and tampering authentication in the recent decade. Due to the algebraic or geometric properties of reversible watermarking, it is especially suitable for medical images (Arsalan et al., 2012; Coatrieux et al., 2009; Coatrieux et al., 2013; Farfoura et al., 2012; Shih & Wu, 2005). Difference expansion (Alattar, 2004), sorting and prediction (Sachnev, Kim, Nam, Suresh, & Shi, 2009), histogram modification (An et al., 2012; Coatrieux et al., 2013), lossless compression (Celik, Sharma, Tekalp, & Saber, 2005; De Vleeschouwer, Delaigle, & Macq, 2003), prediction-error histogram (Zhang et al., 2013) and hybrid methods (Kamran et al., 2014) are the most popular algorithms to realize the reversibility of watermarking algorithm. Although there are some existing work (Arsalan et al., 2012; Coatrieux

* Corresponding authors. Tel.: +86 755 26534314; fax: +86 755 26534940.
E-mail addresses: nidong@szu.edu.cn (D. Ni), tfwang@szu.edu.cn (T. Wang).

0957-4174/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2013.11.019

et al., 2009) on the discussed topic of medical images, reversible watermarking of medical images using recursive dither modulation (RDM) still remains uninvestigated.

It is known that larger quantization steps (QSs) lead to higher robustness, but more distortion on the host images will be introduced due to the larger QSs. On the other hand, smaller QSs result in higher transparency but often lead to lower robustness (Chen & Wornell, 2001). Different medical images have different spectral components resulting in different tolerance to distortion, thus single QS would not be applicable for all host medical images. To mitigate this problem, one popular way is to insert multiple watermarks in the host image. Another way is to find the optimized solutions by trial and error. However, without any specific consideration of spectral properties of the host signals, the empirically value may lead to undesirable QS. To address this issue, a myriad of methods in the recent literature have been proposed to optimize the parameters to meet the conflicting watermarking requirements using artificial intelligence (AI) techniques (Aslantas, 2009; Aslantas, Ozer, & Ozturk, 2009; Fındık, Babaoğlu, & Ülker, 2011; Kumsawat, Attakitmongcol, & Srikaew, 2005; Liu & Tan, 2002; Run, Horng, Lai, Kao, & Chen, 2012). This balance is achieved by formulating the watermarking algorithm as an optimization function. Consequently, many intelligent techniques such as differential evolution (DE) (Ali & Ahn, 2014; Aslantas, 2009; Lei, Soon, & Tan, 2013b), constrained clonal selection algorithm (Aslantas et al., 2009), particle swarm optimization (PSO) (Lei, Song, & Rahman, 2012a; Lei, Song, & Rahman, 2013a; Run et al., 2012), and genetic algorithm (GA) (Kumsawat et al., 2005) were proposed to resolve this optimization problem effectively.

We have witnessed another trend which introduces fast intelligent watermarking scheme to reduce the computational cost in these AI based schemes (Vellasques, Sabourin, & Granger, 2013). Since the schemes in transform domain are more robust to attacks, these classes of AI techniques are usually applied in transform domain such as discrete wavelet transform (DWT) (Aslantas, 2009), integer wavelet transform (IWT) (Arsalan et al., 2012; Lee, Yoo, & Kalker, 2007), lifting wavelet transform (LWT) (Lei, Soon, Zhou, Li, & Lei, 2012b; Lei et al., 2013b), discrete cosine transform (DCT) (Aslantas et al., 2009; Lei, Soon, & Li, 2011), and singular value decomposition (SVD) (Run et al., 2012) rather than in spatial domain (Liu & Tan, 2002). An alternative method to improve the robustness of watermarking involves the PSO method, but it is found to be inferior to SVD-based methods. Besides, there are no security measure adopted in both DCT–SVD and DWT–SVD methods, and thus security is still a great concern for this scheme. Furthermore, the performance of existing methods (Aslantas, 2009; Kumsawat et al., 2005) with genetic algorithm is still not optimal and should be investigated further.

Striking a balance between conflicting requirements is highly dependent on the automatic selection of the important controlling parameters such as QS, threshold, scaling factor and watermarking strength. It is very common that intelligent algorithms (Aslantas, 2009; Aslantas et al., 2009; Kumsawat et al., 2005; Liu & Tan, 2002; Run et al., 2012) are utilized to obtain desirable performance by optimizing one or two parameters. However, the tradeoff among the three contradictory requirements: robustness, imperceptibility and capacity are rarely investigated. Moreover, it is reported that DE (Storn & Price, 1997) can find optimal solutions over a specified range simultaneously, and hence the best solution is achieved appropriately. In view of this, the learning abilities of DE should be exploited for QS selection, which provide two-fold benefits too. First, the selection of proper QSs is able to adaptively control watermark and achieves better imperceptibility. Second, DE is able to select QSs that provide enhanced detection (under various attacks) even without the knowledge of watermark and attack parameters.

The main goal of this paper is to design a recursive DM (RDM) based watermarking system to effectively prevent the illegal use of the medical images without affecting its visual quality. The proposed heuristic watermarking method incorporates the wavelet transform including DWT, IWT, LWT, SVD, RDM, DE and scrambling to achieve optimal performance. The singular values (SVs) of the low frequency wavelet transform coefficient are utilized to insert watermarks using optimized QSs determined by the DE heuristic algorithm. The main contributions of this work are as follows:

(1) Both signature and logo data as watermark are inserted by recursive dither modulation algorithm to achieve reversibility with good performance.
(2) Uniquely designed fitness function for DE optimization to consider all conflicting requirements rather than one or two requirements only and makes the system more adjustable. Therefore, the balance of robustness, capacity and imperceptibility is achieved by the designed parameters appropriately.
(3) Hybrid SVD and transform domain watermarking methods (i.e. lifting, discrete and integer wavelet) with comprehensive analysis and experiments to demonstrate the effectiveness of the proposed scheme.
(4) Watermarking medical image with consideration of encryption in the medical application to address the security issue of the application without encryption. A detailed security analysis for the adopted security measure is provided too.

The organization of this paper is as follows. Section 2 provides a general overview of the related work. Section 3 discusses the proposed methodology in detail. Our experiments and discussion for validating the performance of our proposed method are provided in Section 4. Finally, we conclude our paper in Section 5.

2. Related work

Digital medical images in hospital information system as well as picture archiving and communication systems that have been widely transmitted over internet can be illegally modified or duplicated (Arsalan et al., 2012; Coatrieux et al., 2009; Dandapat, Chutatape, & Krishnan, 2004; Das & Kundu, 2012; Kong & Feng, 2001). Watermarking has been commonly applied to prevent illegal manipulation and access to the medical content without the permission of owner. The most popular methods in the field of watermarking include spread spectrum (SS) such as additive and multiplicative SS (Altun, Orsdemir, Sharma, & Bocko, 2009; An et al., 2012; Sachnev et al., 2009) and quantization technique such as quantization index modulation (QIM) (Chen & Wornell, 2001; Kalantari & Ahadi, 2010; Ko, Chen, Shieh, Hsin, & Sung, 2012) and dither modulation (DM). Although the SS technique is more robust against forced removal manipulations compared to the quantization method, this method performs badly in the presence of additive white Gaussian, speckle, and pepper & salt noise. In the traditional SS scheme, the interference effect of the original signal often leads to degradation of the decoding performance which is highly undesirable. There has been several attempts to solve this deficiency to embed the watermark in the logarithm domain (Kalantari & Ahadi, 2010).

One of the first few development of reversible watermarking was discussed in Tian (2003), and several enhanced implementations are found in Coltuc (2011), Coltuc (2012) and Sachnev et al. (2009). For instance, Sachnev et al. inserted the watermark by utilizing the prediction errors (Sachnev et al., 2009). A prediction based algorithm embedded the watermark by exploiting the expanding difference between the pixel in question and the

prediction context rather than inserting it in the current pixel (Coltuc, 2011). More and more researchers have put an important emphasis on the reversibility as well. For example, Ko et al. (2012) proposed the nested QIM-based method for reversible watermarking, which is targeted for the healthcare information management systems. However, important properties of watermarking algorithm such as the robustness and imperceptibility are not addressed in this scheme, and thus it is not conclusive that the Ko's watermarking method is suitable for medical application.

To restore the medical image after extracting the watermark, Arsalan et al. (2012) proposed a reversible watermarking method in medical and defense imagery with the combination of IWT and GA. It is reported that the intelligent method such as GA, PSO and DE (Ali & Ahn, 2014; Aslantas, 2009; Kumsawat et al., 2005; Lei et al., 2013b; Run et al., 2012) can improve the imperceptibility. The reversible watermarking is realized by histogram modification. GA algorithm has learning ability for intelligent threshold selection, which controls the companding procedure and the effective payload. The experimental results demonstrate that both imperceptibility and robustness are achieved simultaneously for a series of natural images and medical images. However, there is no security feature in this method. In Tian (2003), with the expansion of pair-wise pixel difference, reversible watermarking was proposed, which has high capacity and quality too. The watermark was embedded in the selected expansion between the pixel pair of the host images. Moreover, the location maps integrating with watermark were hidden by locating the expanded difference. However, significant distortion will arise if there is no enough space for location map. As a result, balance between the imperceptibility and capacity should be made to ensure enough space for location map. Similarly, in Shih and Wu (2005), a region-of-interest (ROI) based medical image watermarking with the GA optimization, which shows relatively high effectiveness for copyright protection.

Another popular class of reversible watermarking algorithm is based on the hybrid IWT (Alattar, 2004; Arsalan et al., 2012; Das & Kundu, 2012; Khan et al., 2012; Ni et al., 2006). This class of watermarking algorithm inserts data into IWT coefficients at middle or high frequencies. To achieve reversible watermarking application, companding IWT coefficients in the selected function are capitalized on. The compression and expansion approach is employed to minimize the distortion between the host and watermarked medical image. For instance, in (Das & Kundu, 2012), medical data protection issue is effectively solved by watermarking in the contourlet transform domain, which is especially robust to JPEG and JPEG 2000 compression. It is claimed that security, authentication, access control, archiving, and retrieval can be also addressed simultaneously. This algorithm achieved relatively high robustness, imperceptibility and capacity, and security is further improved with the popular advanced encryption system (AES) encryption technique. However, one of the key parameters (i.e. scaling factor) of this algorithm is just experimentally defined rather than automatically optimized. One of the biggest drawbacks of the watermarking method in contourlet transform is non-reversibility, which makes this method unsuitable for protection and authentication of medical images.

Most existing watermarking methods use intelligent approach to obtain a good tradeoff between imperceptibly and capacity (An et al., 2012; Arsalan et al., 2012; Aslantas et al., 2009; Kumsawat et al., 2005; Shih & Wu, 2005; Wang, Lin, & Yang, 2011). For instance, IWT domain based adaptive data hiding scheme is proposed to protect medical images [2]. This hiding technique based on the IWT technique is explored to embed multiple watermarks in the wavelet coefficients by decomposing the cover object. The threshold for each block is adaptively determined using iterative optimization method in the compression and expansion process, and hence avoids the pre- and post-processing of the histogram. In this sense, the advantage of this method lies in maintaining the distortion as small as possible in the histogram processing. Meanwhile, the disadvantage of the technique is low transparency value with the embedding capacity, and is only applicable for color images.

3. Proposed method

3.1. Differential evolution

The following steps illustrates the DE process in detail (Storn & Price, 1997):

Initialization: Define the fitness function, population size, mutation and cross rate, maximum iteration number, and optimized parameters randomly within the boundary constraints. Iterate the first generation by random selection.

Mutation: Adjust the pixel values based on each target vector, a mutant vector is generated according to:

$$v_1(i,G+1) = x(r_1,G) + F \times (x(r_2,G) - x(r_3,G) + x(r_5,G) - x(r_4,G)), \quad (1)$$

where $x_{i,G}$, $i = 1,2,3,\ldots,D$ is initial parameter vectors, i, r_1, r_2, r_3, r_4 and r_5 are mutually different indexes selected from the current generation, $F \in [0,2]$ is a convergence parameter improving the convergence rate, and D is population size.

Crossover: By considering the elements of mutated and target vector, the trial vector $u(i,G+1)$ is denoted as:

$$u(j,i,G+1) = \begin{cases} v(j,i,G+1), & \text{if } (randb(j) \leqslant CR) \text{ or } j = rnbr(i), \\ x(j,i,G+1), & \text{if } (randb(j) > CR) \text{ and } j \neq rnbr(i), \end{cases} \quad (2)$$

where $j = 1,2,\ldots,P$, $randb(j) \in [0,1]$ is a uniform random number generator in the jth evaluation, $CR \in [0,1]$ denotes the crossover constant parameter which is decided by the user.

Selection: To determine whether or not it should become a member of generation $G+1$, there is a comparison between the trial vector and the target vector using the greedy criterion as below:

$$x(i,G+1) = \begin{cases} u(i,G+1), & \text{if } f[u(i,G+1)] \leqslant f[x(i,G)], \\ x(i,G), & \text{otherwise}, \end{cases} \quad (3)$$

where $f[\bullet]$ is the objective function. Object value is evaluated for each corresponding vector. The new chromosomes are recombined using the crossover rate.

The above steps are repeated until a predefined condition is satisfied, or a predefined number of iterations are reached.

3.2. Watermark embedding

Fig. 1 illustrates the block diagram of the proposed watermark embedding procedure, which is presented in detail as below:

Step 1. The original image (I) is divided into sub-blocks B^k, where $k = 1,2,\ldots,N$, $N = W_w \times W_h$, W_w and W_h are the width and height of the watermark, respectively.

Step 2. To enhance the security of the proposed watermarking system, scrambling algorithm is applied to both meaningful signature and logo data first. In our watermark insertion approach, the space relationship of the pixel bit sequence of watermark image (W) is first dispelled and scrambled to generate the shuffled sequence (E) by a secret key (K).

Since the chaotic signal generally has good invariance to disturbance (Wu & Guan, 2007) due to the low correlation between the initial parameters, it has been widely utilized

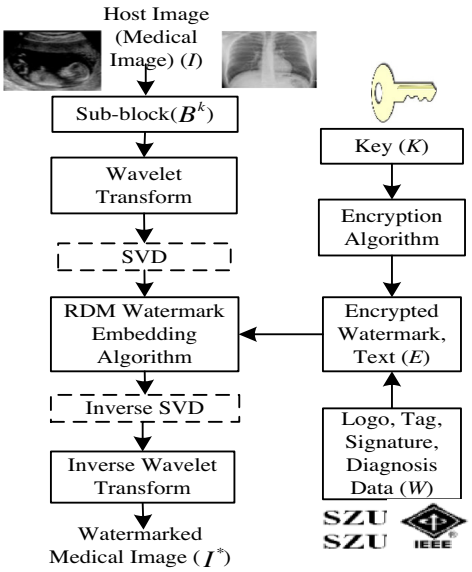

Fig. 1. Block diagram of the proposed watermarking scheme.

for improving the security performance. The chaotic map, piece-wise affine Markov (PWAM) map (Kocarev, Galias, & Lian, 2009; Wu & Guan, 2007) is selected in our scheme to achieve the scrambling goal, which is defined as:

$$x(k+1)=\begin{cases} B(-x(k)+C\times \mathrm{sgn}[x(k)]), & \text{for} \quad |x(k)|\geqslant C,\\ B(x(k)-2C\times \mathrm{sgn}[x(k)]), & \text{for} \quad |x(k)|<C, \end{cases} \tag{4}$$

where sgn[•] is the sign operator, $C=1$, $k=1,2,\ldots,N$, and N is the length of watermark. The initial condition and parameter B are important parameters for generating the encryption signal. The PWAM map (in the real number domain) is normalized to $[-1,1]$, and then mapped to a binary signal $\{0,1\}$ by thresholding. The exclusive OR method is applied to the binary signal generated by PWAM map and watermark image (W) to produce the final encrypted sequence (E).

Step 3. Two-level wavelet transform is applied to each sub-block. We select coefficients in the low frequency part to enhance robustness against additive noise, filtering, and JPEG compression.

Step 4. Perform SVD on the low frequency wavelet coefficient of each block to generate SVs (S^k).

Step 5. Watermark bits are embedded by quantization using the RDM approach, that is, only the first SVs of wavelet approximate coefficients are selected to be quantized since the first SVs are more robust to geometric distortion.

Differing from traditional DM based watermarking method (Chen & Wornell, 2001), the proposed watermarking method is reversible, and hence signals can be recovered completely. The proposed method starts with the embedding using the following normalization:

$$S_N^k=\|S^k\|, \tag{5}$$

where S^k is the first SVs in kth block, $\|\bullet\|$ can be L_1, L_2 or L_∞ normalization operation depending on the properties of the host image.

Let $S_a^k=floor(S_N^k/\Delta^k)$, where $floor(\bullet)$ is rounding toward the negative infinity and Δ^k is QS. The first SVs are modified by the value of the shuffled message:

$$S_w^k=\begin{cases} S_a^k+1-\mathrm{mod}(S_a^k,2), & \text{for} \quad E(i,j)=1,\\ S_a^k+1-\mathrm{mod}\left((S_a^k+1),2\right) & \text{for} \quad E(i,j)=0, \end{cases} \tag{6}$$

where mod(•) is modulation operation. SVs are further updated to retrieve the host signal as shown in the following:

$$S_w^k=\Delta^k\times S_w^k+\Delta^k/2, \tag{7}$$

$$S_w^{k*}=S^k\times S_w^k/S_N^k. \tag{8}$$

Step 6: Apply SVD calculations to obtain updated SVs for the host signals.

Step 7: The IWT is performed to obtain the watermarked host medical images (I^*).

The above mentioned process is the traditional DM quantization process (DM(•)), which is a nonlinear process. Let I_n, K_n, W_n, F_n, Δ_n, Q_m, and $O_{m,n-1}$ denote the input host image, secret key, watermark, quantization output, QS, quantization error and output watermarked image, at the n_{th} stage of m-level RDM, respectively. Fig. 2 shows the diagram of the RDM process for watermarking, and RDM can be described with the following equations:

$$F_n=\mathrm{DM}(I_{n-1}), \tag{9}$$

$$I_n=I_{n-1}-F_n, \tag{10}$$

$$O_{m,n-1}=F_n+V_{m,n}=F_n+I_n/\Delta_m, \tag{11}$$

$$O_{m,0}=F_1+\frac{I_m-F_m}{\prod_{i=1}^{m}\left(\sum_{j=i}^{m}\Delta_j\right)}+\sum_{r=2}^{m}\frac{F_r}{\prod_{i=1}^{r-1}\left(\sum_{j=i}^{m}\Delta_j\right)}. \tag{12}$$

3.3. Watermark extraction

Generally, watermark extraction procedure is the reverse of the watermark embedding and the steps of the procedure are described as below:

Step 1: The watermarked host medical image (I^*) is partitioned into sub-blocks B^{*k}, where $k=1,2,\ldots,W_w\times W_h$.

Step 2: Two-level wavelet transform is performed to each sub-block B^{**k}. The approximate coefficients are selected for SVD calculation.

Step 3: Perform SVD on the low frequency of each block to generate SVs (S^{**k}).

Step 4: The SVs (S^{**k}) is then normalized according to:

$$S_N^{**k}=\|S^{**k}\|. \tag{13}$$

Let $S_a^{**k}=floor(S_N^{**k}/\Delta^k)$, and the shuffled message is extracted with the following rule:

$$E*(i,j)=\begin{cases} 0, & \text{for} \quad \mathrm{mod}(S_w^{k*},2)=0,\\ 1, & \text{for} \quad \mathrm{mod}(S_w^{k*},2)=1. \end{cases} \tag{14}$$

Step 5: The final watermark is obtained by reshuffling the extracted shuffled message.

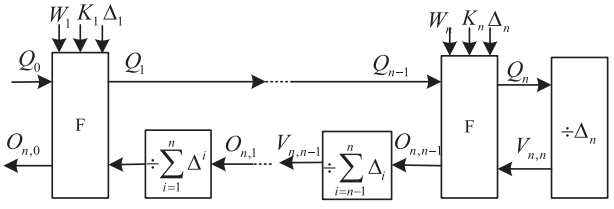

Fig. 2. RDM with n DM operations for watermarking.

Fig. 3 shows the watermark extraction procedure by n inverse DM operations. The original watermark image can be extracted from the watermarked image based on the nested inverse DM using the following expressions:

$$F_n = \mathrm{IDM}(O_{m,n-1}), \tag{15}$$

$$V_{m,n} = O_{m-1,n} - F_n, \tag{16}$$

$$T_{m,n-1} = T_{m,n} + F_n, \tag{17}$$

$$T_{m,0} = F_1 + T_{m,1} = F_1 + \cdots + F_n + T_{m,m} = \sum_{r=1}^{m} F_r + T_{m,m} = Q_0. \tag{18}$$

3.4. Design of objective function

The main task of intelligent approach is to optimize the system performance by trading off between robustness, capacity, and imperceptibility. To achieve this goal, an optimal balance is obtained by optimizing these three requirements using the objective function:

$$\mathit{fitness} = f(\text{impercetibility, robustness, capacity}). \tag{19}$$

Assuming A and A' are the host and watermarked medical images, respectively, the structural similarity index measure (SSIM) based on three comparisons, luminance $l(A,A')$, contrast $c(A,A')$, and structure $s(A,A')$ are selected for the measure of imperceptibility (Sheikh, Wang, Bovik, & Simoncelli, 2002). SSIM is defined as:

$$\mathrm{SSIM}(A,A') = [l(A,A')]^{\alpha}[c(A,A')]^{\beta}[s(A,A')]^{\gamma}, \tag{20}$$

where $\alpha > 0$, $\beta > 0$, and $\gamma > 0$ are the parameters that are used to vary the contributions of the three elements in SSIM. A single value within [0,1] is obtained with mean SSIM (MSSIM) to describe the similarity of the host and watermarked images:

$$\mathrm{MSSIM} = \frac{1}{N_B}\sum_{j=1}^{N_B}\mathrm{SSIM}(A_j, A'_j), \tag{21}$$

where N_B is the total number of blocks in the host image.

Normalized cross correlation coefficient (NC) is an effective way to measure the robustness (Run et al., 2012), and NC is used to evaluate the robustness of the proposed watermarking method. NC is computed as:

$$NC(W,W') = \frac{\sum_{i=1}^{W_w}\sum_{j=1}^{W_h} W(i,j)\times W'(i,j)}{\sum_{i=1}^{W_w}\sum_{j=1}^{W_h} W'^2(i,j)\sum_{i=1}^{W_w}\sum_{j=1}^{W_h} W^2(i,j)}, \tag{22}$$

where W and W' are the host and detected watermarks, respectively. Common signal manipulation attacks of watermarks including JPEG compression (JG), rescaling (RS), cropping (CP), adding Gaussian noise (GN), low pass filtering (LF), median filtering (MF), rotation (RT) and adding salt & pepper noise (SN) are integrated into the DE optimization process. Moreover, the mean of NC values (MNC) of all selected attacks in our scheme is adopted in the objective function, which is denoted as

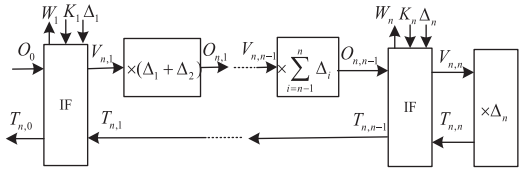

Fig. 3. Watermark extraction by RDM using n inverse QIM operations.

$$\mathrm{MNC} = \frac{1}{R}\sum_{i=1}^{R} w_i \times NC_i, \tag{23}$$

where R represents the total number of attacks.

The capacity of the watermarking algorithm, which is the total number of bits that can be inserted into the host image, is another important assessment of watermark methods. In our method, capacity is computed as:

$$NP = \frac{\text{Total number of watermark bits}}{\text{Total number of host image bits}}. \tag{24}$$

Finally, the objective function is designed as

$$\mathit{fitness} = \max(k_1\mathrm{MSSIM} + k_2(1-NP) + k_3\mathrm{MNC}), \tag{25}$$

where k_1, k_2 and k_3 are the weighting factors are computed as

$$k_1 = \frac{(1-NP)\times\mathrm{MNC}}{\mathrm{MSSIM} + (1-NP)\times\mathrm{MNC} + (1-NP)\times\mathrm{MSSIM}}, \tag{26}$$

$$k_2 = \frac{\mathrm{MSSIM}\times\mathrm{MNC}}{\mathrm{MSSIM} + (1-NP)\times\mathrm{MNC} + (1-NP)\times\mathrm{MSSIM}}, \tag{27}$$

$$k_3 = \frac{(1-NP)\times\mathrm{MSSIM}}{\mathrm{MSSIM} + (1-NP)\times\mathrm{MNC} + (1-NP)\times\mathrm{MSSIM}}. \tag{28}$$

It should be noted that $k_1 + k_2 + k_3 = 1$, and by substituting k_1, k_2, and k_3 into the fitness function, we can rewrite the fitness function as:

$$\mathit{fitness} = \frac{3\times\mathrm{MSSIM}\times(1-NP)\times\mathrm{MNC}}{\mathrm{MSSIM} + (1-NP)\times\mathrm{MNC} + (1-NP)\times\mathrm{MSSIM}}. \tag{29}$$

The metrics selected here can converge to a saturated value using DE algorithm. Fig. 4 shows the DE algorithm applied in the proposed watermarking approach.

It can be observed that the fitness function is constrained to [0,1]. Fitness function can be designed with integration of more fidelity, capacity, and robustness metrics. Moreover, weighting factors should be used to control the emphasis of these metrics since different metrics play different roles.

3.5. Security of the proposed method

The security issue of the proposed recursive watermarking can be addressed using the scrambling method (Elshoura & Megherbi, 2013), as shown in Table 1. Both the secret message and authentication logo are embedded in the host medical signal. Besides, this is a blind watermarking method without involving original host signal in the extraction step.

In a single precision computer, the probability of estimating one bit of watermark is:

$$P(\text{estimating one bit}) = 1/2^{32}. \tag{30}$$

In the block-based scheme, the intruder often needs to figure out the block if he/she wants to hack into the scheme and modify the secret information. Assuming the size of image is $N_A \times N_A$, where N_A is an even number, the block can be estimated with the following probability:

$$P(\text{estimating the block size}) = 1/\log_2\left(\frac{N_A}{2}\right), \tag{31}$$

$$P(\text{estimating watermark bit and block size}) = \left(\frac{1}{2^{32}}\right)^{\log_2\left(\frac{N_A}{2}\right)}. \tag{32}$$

To further improve the security of the proposed method, encryption approach or chaos based scrambling is often used. These approaches are adopted in both the watermark and hidden

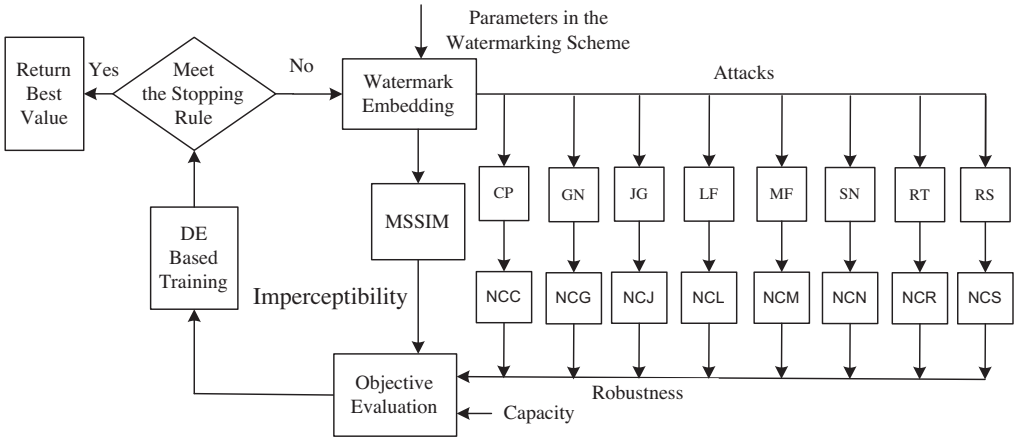

Fig. 4. DE algorithm applied in the proposed watermarking algorithm.

Table 1
Scrambling algorithm.

Begin
1:Generate a vector of random integers with the length same as the number of blocks in the scrambled image
2: Index the image blocks to be scrambled in an ascending order
3: Scanning the whole image from the left top to the right bottom corner
4: Switch each block based on its order, the block number is saved in the randomly generated vector. The vector's index is the 5: same as the block index
6: Rearrange the blocks to obtain a scrambled image
End

image block before inserting into the host image. Supposing N_b is the total blocks, the probability of estimating the scrambling parameters (Elshoura & Megherbi, 2013) are as below:

$$T = \prod_{x=0}^{N_b/2-1} (N_b - 2x - 1), \tag{33}$$

$$P(\text{estimating watermark bit, block size and scrambling algorithm}) = \left((1/2^{32})^{\log_2\left(\frac{N_A}{2}\right)}\right)^T. \tag{34}$$

Supposing the intruder acquires some knowledge of the proposed method out of the thousands of watermarking and information hiding algorithms available in the market, it is clear that the attempt to detect and extract the hidden images from the carrier is very challenging for a hacker without knowing the arbitrary weights, order of the watermarked images, block size, and scrambling mapping parameters (Elshoura & Megherbi, 2013). Even with the fastest computer working in a nanosecond clock cycle, the estimate of the weights and scrambling mapping is very time-consuming and may require years to finish.

In the third phase of enhancing security, the proposed method with the carrier image is obtained with independency of the proposed method. The same carrier is not required each time as the hidden information should be sent to the receiver. The carrier image is neither a part of the extraction algorithm, nor the needed one at the receiver. To avoid the same carrier, a new set of hidden data to reduce the risk that a carrier image with the contained hidden information is suspected to be attacked.

3.6. False positive probability

Generally, an image is regarded as watermarked if at least L number of bits of a watermark is extracted correctly in the block. The presence of a watermark in the original medical image is determined if at least one block of the host image is determined to be watermarked. In most cases, there is false positive error P_{fpp} of watermark detected from a non-watermarked image. The probability of false positive or negative error (Lei et al., 2013a) is defined using the Binomial distribution approximation as below:

$$P_{fpp} = \sum_{i=L}^{N} \binom{N}{i} (P_b)^i (1 - P_b)^{N-i}, \tag{35}$$

where N is the length of watermark image, P_b is the probability that a bit is falsely detected as a watermark bit, and L is the threshold used for determining the presence of a watermark. As the watermarks' pixel value is either 0 or 1, $P_b = 0.5$. The value of L is selected according to the desired probability of false positive error of the host signal, that is, L is a function of NC (e.g. $L = NC \times N$). From (35), it can be noted that the false positive error for a host signal depends on both the correlation detection threshold for L and N.

The curves of the false positive error vs. the watermark length of the proposed method are plotted in Fig. 5. It can be observed that the false positive error P_{fpp} is higher if the NC value is lower and watermark length is shorter. The average NC of our approach on the test data sets is more than 0.9 (see Table 2). From our experiments, P_{fpp} is found to be near zero (less than 10^{-8}) when NC is more than 0.9 and N is equal to 4096, which is far more than 100.

4. Experimental results and discussions

4.1. Experiment configuration

In our experiment, simulations are carried out to evaluate the effectiveness of the proposed reversible medical image watermarking method. Commonly used popular gray-level natural image (e.g. Lena and Baboon) are selected as reference images to compare the proposed method with existing watermarking methods. Three 512×512 medical images including X-ray, MRI, ultrasound (US) images, two 64×64 watermarks (one is text data for signature,

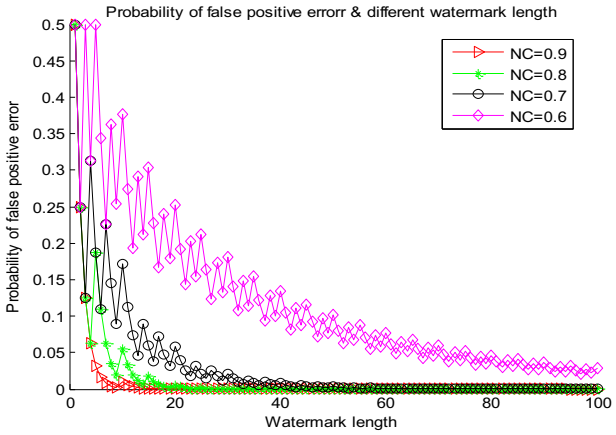

Fig. 5. False positive error vs. various different watermark lengths.

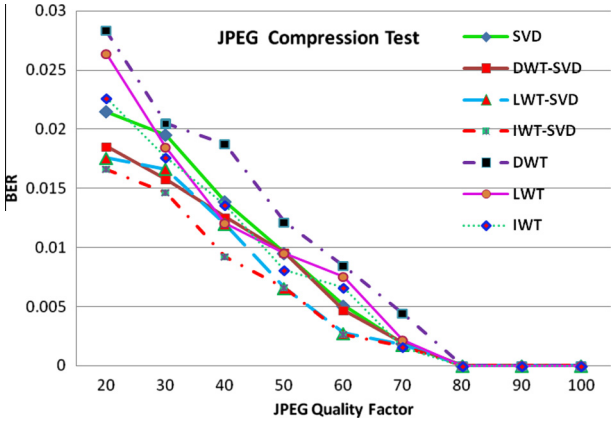

Fig. 7. JPEG compression results.

Table 2
Optimization results.

	Method	Fit	PSNR	MSSIM	NCA
XRAY	IWT	0.9723	48.28	0.9936	0.9719
	LWT	0.9672	47.96	0.9920	0.9652
	DWT	0.9657	47.88	0.9912	0.9662
	IWT–SVD	0.9791	48.39	0.9934	0.9738
	LWT–SVD	0.9708	48.06	0.9924	0.9623
	DWT–SVD	0.9703	48.03	0.9924	0.9615
	SVD	0.9694	48.03	0.9621	0.9604
US	IWT	0.9746	48.12	0.9931	0.9675
	LWT	0.9728	48.21	0.9925	0.9587
	DWT	0.9716	48.03	0.9918	0.9578
	IWT–SVD	0.9749	48.35	0.993	0.9679
	LWT–SVD	0.9704	48.47	0.9934	0.9612
	DWT–SVD	0.9701	48.43	0.9934	0.9608
	SVD	0.9688	48.42	0.9935	0.9588
MRI	IWT	0.9722	48.02	0.9912	0.9542
	LWT	0.9622	47.91	0.9908	0.9436
	DWT	0.9589	47.23	0.9902	0.9428
	IWT–SVD	0.9746	48.31	0.992	0.968
	LWT–SVD	0.9657	47.94	0.992	0.9549
	DWT–SVD	0.9636	48.08	0.9917	0.9513
	SVD	0.9615	47.99	0.9915	0.9499

another one is logo) are used in our simulations, which are shown in Fig. 6 (noted that the images shown here are resized). The performance evaluation of the watermark methods includes the important metrics such as robustness, imperceptibility, reversibility, capacity, and complexity. Bits per pixel (bpp) (bit of message per pixel in an image) is adopted to represent the capacity rate. PSNR and MSSIM are utilized to represent imperceptibility, while *NC* and BER are used to measure robustness.

Generally, reversibility is defined as the completely recovery of the host images and watermarks in a secured situation. It can be seen from the RDM method achieves reversibility in the proposed method. The maximum generation (G) is 80. The DE optimization parameters are empirically chosen as $CR = 0.4$, $F = 0.2$, $D = 30$. The

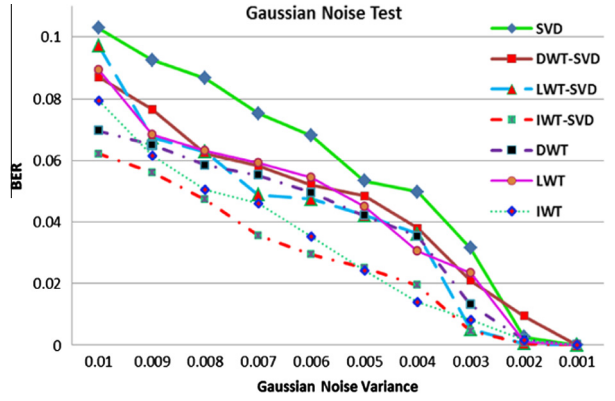

Fig. 8. Gaussian noise attack results.

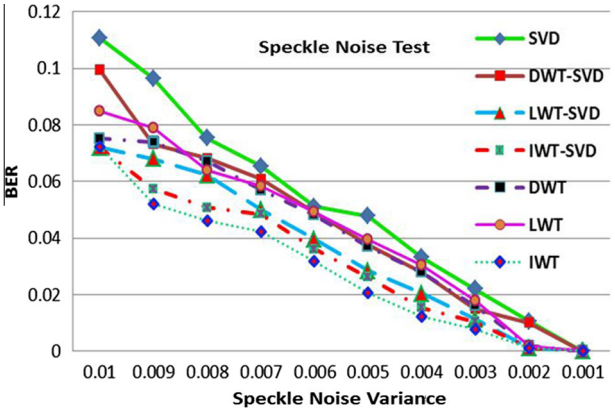

Fig. 9. Speckle noise attack results.

weighting factors are also determined based on numerous experimental and validated empirically as $w_i = 1$, which is closely related to the tradeoff among the contradictory requirements.

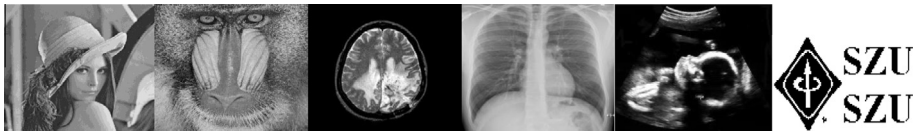

Fig. 6. Host medical images and watermarks.

4.2. Performance results

Table 2 gives the fitness value (Fit), PSNR value, and average *NC* value of all attacks (NCA) of the three representative host medical images. Wavelet based methods, pure SVD and hybrid SVD and wavelet methods are also included in this comparison. While the results in Table 2 reveal these methods demonstrate good results as well as a good balance of imperceptibility and robustness, it is found that the SVD method has the worst performance among the seven methods. High PSNR, MSSIM, and NCA results shown in Table 2 demonstrate that the proposed method has a good balance of robustness and fidelity.

4.3. Effect of JPEG lossy compression

The plots of the BER value vs. JPEG quality factor after JPEG compression attack on the watermarked medical image are shown in Fig. 7. A high value of quality factor indicates low compression and vice versa. Hybrid wavelet based methods with SVD approach are generally more robust against JPEG attacks compared with that without SVD approach, and the proposed method can resist JPEG compression even at a very low quality factor (e.g. 20). It is noted that the BER value decreases as the JPEG quality increases, and the BER value approaches zero when JPEG quality factor is higher than 80.

4.4. Effect of additive noise

To evaluate the resistance of the watermarking methods to noise attacks, zero mean Gaussian and speckle noises of various variances are added to the host images. Figs. 8 and 9 show that the proposed watermarking method effectively resists Gaussian and speckle noises, and the IWT and IWT–SVD methods constantly outperform DWT and LWT methods in terms of the resistance against additive noise attack. It is noted that the robustness of the proposed method to Gaussian noise attacks is quite similar to the Speckle noise attacks. This is expected since there is not much difference between the distribution error probability of the Gaussian and speckle noise.

4.5. Robustness of watermarking method

The following attacks are applied to test the robustness of the watermarking method: (a) CP (5% signal is cropped randomly); (b) GN (5% Gaussian noise is added); (c) JG (JPEG compression with quality factor 70); (d) LF (3×3 Gaussian low pass filtering is applied); (e) MF (3×3 median filtering is added); (f) SN (5% salt & pepper noise is fedded); (g) RS (image size is enlarged to 2 and then reduced to the original size); (h) RT (rotate 5°). Fig. 10 shows the *NC* results after these attacks. It can be seen that methods based on IWT and SVD hybrid techniques have slightly better performance than non-hybrid techniques such as DWT and LWT. Due to the multiresolution properties of wavelets, the methods based on hybrid techniques managed to outperform the SVD technique. It can be seen that IWT–SVD method has the best performance among these methods, while DWT and LWT methods have very similar performance in terms of the *NC* results. Table 3 shows the *NC* results and extracted watermarks using the proposed method after the robustness test, and these results revealed the high robustness of the proposed method in resisting various attacks.

Table 3
Robustness test results.

Attacks	Original watermark	CP	GN
Extracted logo			
Extracted signature			
NC	1	0.9867	0.984
Attacks	JG	LF	MF
Extracted signature			
Extracted logo			
NC	0.9984	0.9638	0.9853
Attacks	SN	RS	RZ
Extracted signature			
Extracted logo			
NC	0.9602	0.9884	0.9570

4.6. DE optimization results

Fig. 11 shows the converged values of the fitness (objective) value, QS, MSSIM and *NC* results, which relates to the best or optimal values based on the input images and parameters. It is observed that the balance of the robustness and imperceptibility is obtained from the convergence results. It is obvious that the DE

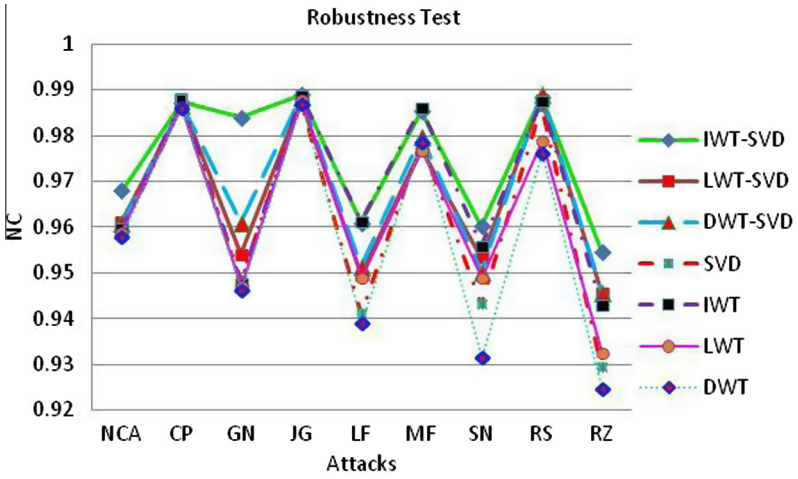

Fig. 10. Performance comparison of different methods.

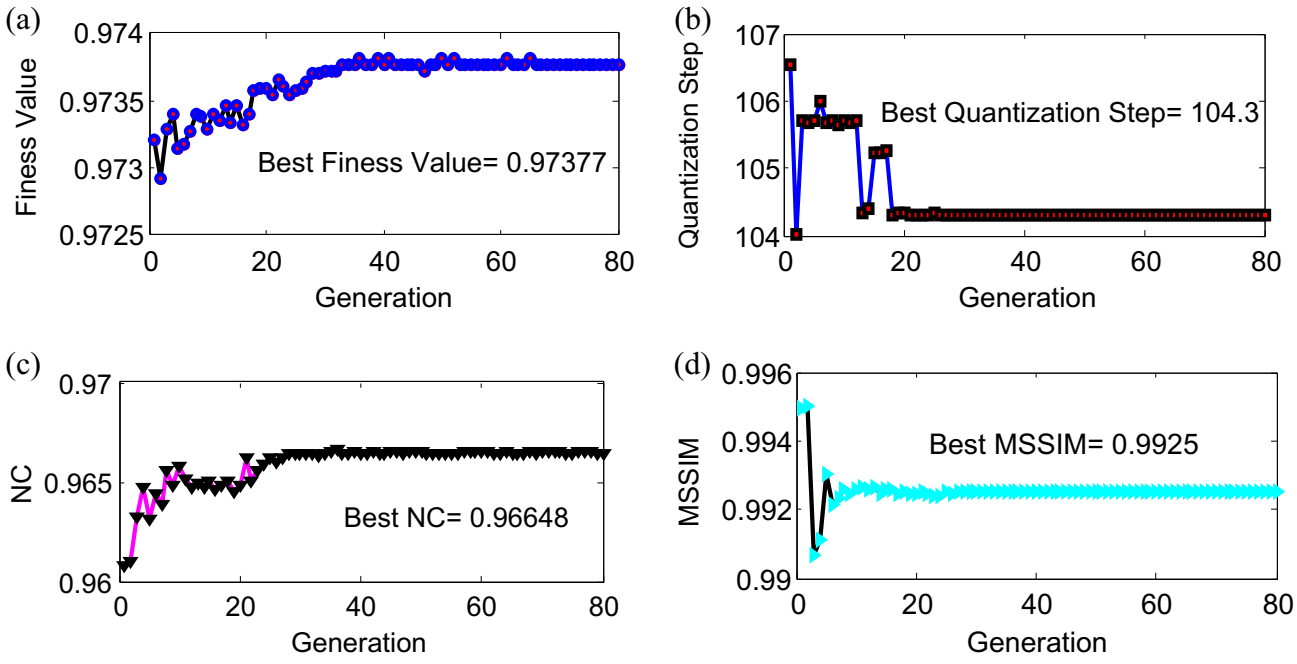

Fig. 11. DE optimization results; (a) objective value results; (b) quantization steps results; (c) MSSIM results; (d) *NC* results.

Table 4
Comparison results (PSNR).

	Kumsawat et al. (2005)	DWT–SVD	LWT–SVD	IWT–SVD	SVD	DWT	LWT	IWT
XRAY	42.25	48.02	48.06	48.39	47.89	46.58	47.11	48.56
US	42.12	48.35	48.47	48.43	47.91	46.63	47.46	48.69
MRI	41.32	48.31	47.94	48.08	47.95	46.96	47.63	48.78

Table 5
Comparison results (MSSIM).

	Kumsawat et al. (2005)	DWT–SVD	LWT–SVD	IWT–SVD	SVD	DWT	LWT	IWT
XRAY	0.9687	0.9924	0.9924	0.9934	0.9848	0.9917	0.9947	0.9981
US	0.9815	0.9934	0.9934	0.993	0.9825	0.9926	0.9959	0.9968
MRI	0.9724	0.9917	0.992	0.992	0.9812	0.9812	0.9948	0.9975

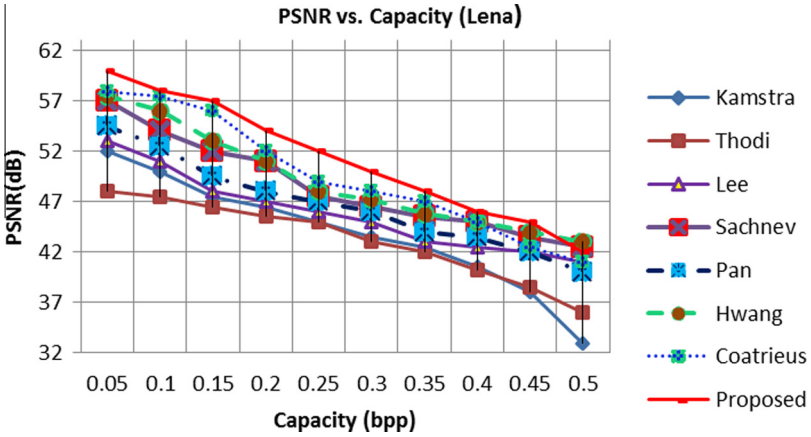

Fig. 12. Algorithm comparison results using Lena image.

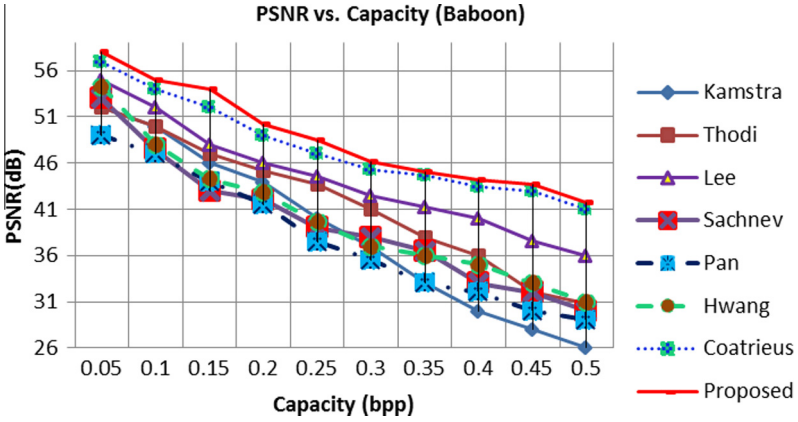

Fig. 13. Algorithm comparison results using Baboon image.

optimization can be successfully applied for the medical image watermarking for the parameter optimization.

4.7. Algorithm comparison results

To further validate the proposed method, we compared our method with the one discussed in Kumsawat et al. (2005). Kumsawat's method uses GA for optimization in the multi-wavelet transform domain, and possesses many similarities with the proposed method such as wavelet and AI technique. Despite the similarities, our proposed method consistently outperforms Kumsawat's method in terms of PSNR and MSSIM results, as shown in Tables 4 and 5.

A comparative analysis of several reversible watermarking methods in Coatrieux et al. (2013), Hwang, Kim, Sachnev, and Joo (2010), Kamstra and Heijmans (2005), Pan, Coatrieux, Cuppens, Cuppens, and Roux (2010) and Sachnev et al. (2009) and the proposed hybrid method is performed using natural images (e.g. Lena and Baboon). The PSNR values of these watermaking methods using Lena and Baboon images are shown in Figs. 12 and 13, respectively. Only IWT–SVD method result is shown in both figures (i.e. the proposed method) since the wavelet based and SVD combination methods obtain very similar results. The results obtained from natural images are similar to those from the medical images. It is noted that the image quality is better preserved with the same capacity rate compared to literature (Coatrieux et al., 2013; Hwang et al., 2010; Kamstra & Heijmans, 2005; Pan et al., 2010; Sachnev et al., 2009). In addition, the proposed method can achieve a compromise from 0.05 bpp/48 dB, 0.5 bpp/33 dB for Lena image, and 0.05 bpp/48 dB, 0.5 bpp/28 dB for Baboon image. Generally, there is a similarity of performance between the proposed method and that in Coatrieux et al. (2013), but the proposed method has slightly higher capacities for highest PSNR values. The higher bpp will cause a higher watermark strength, and thus lead to faster distortion when more sub-band are adopted.

The reversible watermarking schemes presented in Hwang et al. (2010) and Pan et al. (2010) are non-blind approaches where the original medical images are required to extract the watermark. However, the technique in Hwang et al. (2010) and Pan et al. (2010) is less secure as compared to the proposed method since only proposed method requires the secret key for watermark extraction. Because medical images are highly confidential, sensitive and critical in nature, the watermark sequence is scrambled prior to the insertion process to further enhance the security of the proposed method. Moreover, the watermarking capacity of the proposed method is higher than most of the existing methods (Coatrieux et al., 2013; Hwang et al., 2010; Kamstra & Heijmans, 2005; Pan et al., 2010; Sachnev et al., 2009).

5. Conclusions

In this article, a robust and reversible watermarking scheme that embeds/extracts watermarks blindly using RDM scheme and DE optimization is proposed. The proposed method inserts double watermarks into the original host images by recursively modifying the SVs of different blocks. Furthermore, DE is utilized to optimize the QSs for controlling watermark strength with the specially designed fitness function. Overall, the proposed method demonstrates a good balance of robustness, imperceptibility, and capacity as compared to many existing methods. Our experimental results show the superiority of combination of wavelet algorithm with SVD technique as compared to non-hybrid SVD or wavelet algorithm in terms of PSNR and MSSIM. It is also demonstrated that the proposed scheme achieves superior results using DE algorithm compared with the optimization method using GA algorithm.

The main practical application for the watermarking medical image is to protect and authenticate the medical documents in the telemedicine, telediagnosis and other related medical system. The proposed watermarking technique addresses the issue of copy protection and intellectual protection of medical images as well. The evolutional and intelligent algorithm used in the proposed technique can provide adjustable robustness, quality and capacity level by adjusting the fitness function.

Future research directions are mainly concentrated on speedup of the watermarking method by fast and efficient intelligent algorithms. This work is generalized and can be extended to other media such as medical audio, video, 3D, vector map, sensor data and other image media (satellite image, biometrical image and document image). Moreover, the reversible watermarking scheme can be applied in a more wide area such E-government system, wireless network, cloud system and medical related area. Watermarking for authentication purpose or multipurpose watermarking scheme for both copyright protection and authentication by the proposed watermarking method is a good future research direction too.

Acknowledgements

This work was supported partly by National Natural Science Foundation of China (Nos. 61101026, 61372006, 61031003 and 81270707), partly by Shenzhen Research Project (Nos. JCYJ20120613113419607, JCYJ20130329105033277 and JSE201109150013A), partly by Project on the Integration of Industry, Education and Research of Guangdong Province and Ministry of Education (No. 2012B091100495), partly by National

Natural Science Foundation of China Postdoc (No. 2013M540663), and partly by National Natural Science Foundation of Guangdong Province (No. S2013040014448).

References

Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing, 13*(8), 1147–1156.

Ali, M., & Ahn, C. W. (2014). An optimized watermarking technique based on self-adaptive de in DWT–SVD transform domain. *Signal Processing, 94*(1), 545–556.

Altun, H. O., Orsdemir, A., Sharma, G., & Bocko, M. F. (2009). Optimal spread spectrum watermark embedding via a multistep feasibility formulation. *IEEE Transactions on Image Processing, 18*(2), 371–387.

An, L., Gao, X., Li, X., Tao, D., Deng, C., & Li, J. (2012). Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Transactions on Image Processing, 21*(8), 3598–3611.

Arsalan, M., Malik, S. A., & Khan, A. (2012). Intelligent reversible watermarking in integer wavelet domain for medical images. *Journal of Systems and Software, 85*(4), 883–894.

Aslantas, V. (2009). An optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Optics Communications, 282*(5), 769–777.

Aslantas, V., Ozer, S., & Ozturk, S. (2009). Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. *Optics Communications, 282*(14), 2806–2817.

Celik, M. U., Sharma, G., & Tekalp, A. M. (2006). Lossless watermarking for image authentication: A new framework and an implementation. *IEEE Transactions on Image Processing, 15*(4), 1042–1049.

Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing, 14*(2), 253–266.

Chen, B., & Wornell, G. W. (2001). Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory, 47*(4), 1423–1443.

Coatrieux, G., Lecornu, L., Sankur, B., & Roux, C. (2006). A review of image watermarking applications in healthcare. In *Proceedings of international conference of the IEEE engineering in medicine and biology* (pp. 4691–4694).

Coatrieux, G., Le Guillou, C., Cauvin, J. M., & Roux, C. (2009). Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE Transactions on Information Technology in Biomedicine, 13*(2), 158–165.

Coatrieux, G., Pan, W., Cuppens-Boulahia, N., Cuppens, F., & Roux, C. (2013). Reversible watermarking based on invariant image classification and dynamic histogram shifting. *IEEE Transactions on Information Forensics and Security, 8*(1), 111–120.

Coltuc, D. (2011). Improved embedding for prediction-based reversible watermarking. *IEEE Transactions on Information Forensics and Security, 6*, 873–882.

Coltuc, D. (2012). Low distortion transform for reversible watermarking. *IEEE Transactions on Image Processing, 21*(1), 412–417.

Dandapat, S., Chutatape, O., & Krishnan, S. M. (2004). Perceptual model based data embedding in medical images. In *Proceedings of international conference on image processing* (pp. 2315–2318).

Das, S., & Kundu, M. K. (2012). Effective management of medical information through a novel blind watermarking technique. *Journal of Medical Systems, 36*(5), 3339–3351.

De Vleeschouwer, C., Delaigle, J. F., & Macq, B. (2003). Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Multimedia, 5*(1), 97–105.

Deng, X., Chen, Z., Zeng, F., Zhang, Y., & Mao, Y. (2013). Authentication and recovery of medical diagnostic image using dual reversible digital watermarking. *Journal of Nanoscience and Nanotechnology, 13*(3), 2099–2107.

Elshoura, S. M., & Megherbi, D. B. (2013). A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments. *Signal Processing: Image Communication, 28*(5), 531–552.

Farfoura, M. E., Horng, S.-J., Lai, J.-L., Run, R.-S., Chen, R.-J., & Khan, M. K. (2012). A blind reversible method for watermarking relational databases based on a time-stamping protocol. *Expert Systems with Applications, 39*(3), 3185–3196.

Fındık, O., Babaoğlu, İ., & Ülker, E. (2011). A color image watermarking scheme based on artificial immune recognition system. *Expert Systems with Applications, 38*(3), 1942–1946.

Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2006). Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine, 10*(4), 722–732.

Hwang, H. J., Kim, H. J., Sachnev, V., & Joo, S. H. (2010). Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting. *KSII Transactions on Internet and Information Systems, 4*(4), 655–670.

Kalantari, N. K., & Ahadi, S. M. (2010). A logarithmic quantization index modulation for perceptually better data hiding. *IEEE Transactions on Image Processing, 19*(6), 1504–1517.

Kamran Khan, A., & Malik, S. A. (2014). A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection. *Information Sciences, 256*, 162–183.

Kamstra, L., & Heijmans, H. J. A. M. (2005). Reversible data embedding into images using wavelet techniques and sorting. *IEEE Transactions on Image Processing, 14*(12), 2082–2090.

Khan, A., Malik, S. A., Ali, A., Chamlawi, R., Hussain, M., Mahmood, M. T., et al. (2012). Intelligent reversible watermarking and authentication: Hiding depth map information for 3D cameras. *Information Sciences, 216*, 155–175.

Ko, L. T., Chen, J. E., Shieh, Y. S., Hsin, H. C., & Sung, T. Y. (2012). Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems. *Computational and Mathematical Methods in Medicine*.

Kocarev, L., Galias, Z., & Lian, S. (2009). *Intelligent computing based on chaos*. Springer.

Kong, X., & Feng, R. (2001). Watermarking medical signals for telemedicine. *IEEE Transactions on Information Technology in Biomedicine, 5*(3), 195–201.

Kumsawat, P., Attakitmongcol, K., & Srikaew, A. (2005). A new approach for optimization in image watermarking by using genetic algorithms. *IEEE Transactions on Signal Processing, 53*(12), 4707–4719.

Lee, S., Yoo, C. D., & Kalker, T. (2007). Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Transactions on Information Forensics and Security, 2*(3), 321–330.

Lei, B., Song, I., & Rahman, S. A. (2012a). Optimal watermarking scheme for breath sound. In International joint conference on neural networks (IJCNN) (pp. 1–6).

Lei, B., Song, I., & Rahman, S. A. (2013a). Robust and secure watermarking scheme for breath sound. *Journal of Systems and Software, 86*(6), 1638–1649.

Lei, B. Y., Soon, I. Y., & Li, Z. (2011). Blind and robust audio watermarking scheme based on SVD–DCT. *Signal Processing, 91*(8), 1973–1984.

Lei, B., Soon, I. Y., & Tan, E. L. (2013b). Robust SVD-based audio watermarking scheme with differential evolution optimization. *IEEE Transactions on Audio, Speech, and Language Processing, 21*(11), 2368–2378.

Lei, B., Soon, I. Y., Zhou, F., Li, Z., & Lei, H. (2012b). A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. *Signal Processing, 92*(9), 1986–2001.

Li, X. W., & Kim, S. T. (2013). Optical 3D watermark based digital image watermarking for telemedicine. *Optics and Lasers in Engineering, 51*(12), 1310–1320.

Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia, 4*(1), 121–128.

Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(3), 354–361.

Pan, W., Coatrieux, G., Cuppens, N., Cuppens, F., & Roux, C. (2010). An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform. In *2010 Proceedings of international conference of the IEEE engineering in medicine and biology society* (pp. 4740–4743).

Podilchuk, C. I., & Delp, E. J. (2001). Digital watermarking: Algorithm and application. *IEEE Signal Processing Magazine, 18*(4), 33–46.

Run, R. S., Horng, S. J., Lai, J. L., Kao, T. W., & Chen, R. J. (2012). An improved SVD-based watermarking technique for copyright protection. *Expert Systems with Applications, 39*(1), 673–689.

Sachnev, V., Kim, H. J., Nam, J., Suresh, S., & Shi, Y. Q. (2009). Reversible watermarking algorithm using sorting and prediction. *IEEE Transactions on Circuits and Systems for Video Technology, 19*(7), 989–999.

Sheikh, H. R., Wang, Z., Bovik, A. C., & Simoncelli, E. P. (2002). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing, 13*(4), 600–612.

Shi, X., & Xiao, D. (2013). A reversible watermarking authentication scheme for wireless sensor networks. *Information Sciences, 240*, 173–183.

Shih, F. Y., & Wu, Y. T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences, 175*(3), 200–216.

Storn, R., & Price, K. (1997). Differential evolution – A simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization, 11*(4), 341–359.

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 13*(8), 890–896.

Vellasques, E., Sabourin, R., & Granger, E. (2013). Fast intelligent watermarking of heterogeneous image streams through mixture modeling of PSO populations. *Applied Soft Computing Journal, 13*(6), 3130–3148.

Wang, Y. R., Lin, W. H., & Yang, L. (2011). An intelligent watermarking method based on particle swarm optimization. *Expert Systems with Applications, 38*(7), 8024–8029.

Wu, X., & Guan, Z.-H. (2007). A novel digital watermark algorithm based on chaotic maps. *Physics Letters A, 365*(5–6), 403–406.

Zhang, Y., Bao, Y., Wang, Q., & Xu, H. (2013). Reversible watermarking algorithm of grid map based on prediction-error histogram. *Journal of Software, 8*(5), 1117–1123.