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