Expert Systems With Applications 49 (2016) 123–135

Contents lists available at ScienceDirect

Expert Systems With Applications

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

Imperceptibility—Robustness tradeoff studies for ECG steganography using Continuous Ant Colony Optimization

Edward Jero S[a,*], Palaniappan Ramu[a], Ramakrishnan Swaminathan[b]

[a] Department of Engineering Design, Indian Institute of Technology Madras, Chennai, Tamil Nadu 600036, India
[b] Non Invasive Imaging and Diagnostics Laboratory, Biomedical Engineering Group, Department of Applied Mechanics, Indian Institute of Technology Madras, Chennai, Tamil Nadu 600036, India

ARTICLE INFO

Keyword:
ECG steganography
DWT–SVD watermarking
Continuous Ant Colony Optimization
Multiple scaling factors
Performance metrics

ABSTRACT

ECG Steganography ensures protection of patient data when ECG signals embedded with patient data are transmitted over the internet. Steganography algorithms strive to recover the embedded patient data entirely and to minimize the deterioration in the cover signal caused by the embedding. This paper presents a Continuous Ant Colony Optimization (CACO) based ECG Steganography scheme using Discrete Wavelet Transform and Singular Value Decomposition. Quantization techniques allow embedding the patient data into the ECG signal. The scaling factor in the quantization techniques governs the tradeoff between imperceptibility and robustness. The novelty of the proposed approach is to use CACO in ECG Steganography, to identify Multiple Scaling Factors (MSFs) that will provide a better tradeoff compared to uniform Single Scaling Factor (SSF). The optimal MSFs significantly improve the performance of ECG steganography which is measured by metrics such as Peak Signal to Noise Ratio, Percentage Residual Difference, Kullback–Leibler distance and Bit Error Rate. Performance of the proposed approach is demonstrated on the MIT-BIH database and the results validate that the tradeoff curve obtained through MSFs is better than the tradeoff curve obtained for any SSF. The results also advocate appropriate SSFs for target imperceptibility or robustness.

1. Introduction

Recent advances in medical devices enable ubiquitous patient monitoring. In order to achieve this, the acquired medical information along with patient data is sent to the physician/care giver through internet. It is essential to ensure the protection of patient data in such transfer (Al Ameen, Liu, & Kwak, 2012; Law, 1996). Data hiding schemes such as steganography can be used in such situations to shield the identity of the medical information. Watermarking techniques such as least significant bit and substitution schemes are used for hiding the data. The data to be protected is the watermark and the information that carries the watermark is referred to as cover signal. The success of steganography lies in maintaining the embedding induced deterioration of the signal to be minimal and also be robust to external attacks (Katzenbeisser & Petitcolas, 2000; Shih, 2007, chap. 4; Tareef & Al-Ani, 2015; Ziou & Jafari, 2014). In medical domain, steganography schemes protect patient data by hiding it inside their medical information (Zielinska, Mazurczyk, & Szczypiorski, 2014). In this paper, we are interested in hiding patient data into their ECG signals using steganography. Since watermarking leads to cover signal deterioration, steganography algorithms strive to modify the cover signal less such that diagnosability is not affected.

Among other methods, transform domain techniques are widely used in steganography. Steganography in transform domain consists of decomposing the cover signal and embedding the watermark in one or more frequency sub-bands. In ECG steganography, research in the past has focused on different transforms and watermarking techniques. Ibaida and Khalil (2013) performed ECG steganography using Discrete Wavelet Transform (DWT) and Least Significant Bits (LSB) algorithm. In addition, encryption and scrambling techniques were used to improve the security. Chen et al. (2014) compared the performance of Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and DWT using quantization based watermarking algorithm on ECG steganography. It was observed that DCT and DWT provide better results than DFT. A DWT and Singular Value Decomposition (SVD) based ECG steganography was proposed by Edward Jero, Ramu, and Ramakrishnan (2014). They converted the ECG signal into 2D matrix and the patient data was embedded into one of the DWT frequency sub-bands using SVD watermarking algorithm. Moreover,

---

* Corresponding author. Tel.: +91 44 2257 4738/ +91 9600047486.
E-mail addresses: edwardjero@gmail.com, edward_jero@yahoo.co.in (E.J. S), palramu@iitm.ac.in (P. Ramu), sramki@iitm.ac.in (R. Swaminathan).

http://dx.doi.org/10.1016/j.eswa.2015.12.010
0957-4174/

researchers have used steganography in medical images as well (Acharya, Niranjan, Iyengar, Kannathal, & Min, 2004; Giakoumaki, Pavlopoulos, & Koutsouris, 2006; Lei et al., 2014; Raul, Claudia, & Trinidad-Blas, 2007)

1.1. Related work

One of the widely used watermarking techniques is the quantization approach. In SVD based quantization, scaling factors play a vital role in minimizing the deterioration of the cover signal (Mishra, Agarwal, Sharma, & Bedi, 2014; Run, Horng, Lai, Kao, & Chen, 2012). In the context of using a single scaling factor, a low scaling factor provides better imperceptibility while high scaling factor provides better robustness against external attacks. Hence, scaling factor governs the tradeoff between imperceptibility and robustness. Thus, it plays a vital role in determining the quality of the watermarked signal. However, it is easier to decipher the uniform scaling factor in the event of hack. Multiple Scaling Factors (MSFs) (Mishra et al., 2014; Run et al., 2012) are a better choice in such situations but require optimization techniques to find them. Ali and Ahn (2015) show that the algorithm can fail in Mishra et al. (2014). But they use a very less scaling factor range (0.005–0.06) and compare the extracted watermark using correlation. Patient data retrieval which is the focus of this paper is measured using Bit Error Rate.

Loukhaoukha, Chouinard, and Taieb (2011) proposed Lifted Wavelet Transform (LWT) and SVD based image watermarking method. They used Multi Objective Ant Colony Optimization (MOACO) to determine the MSFs. It was observed that the robustness of the watermark improved without losing its transparency. Run et al. (2012) compared the performance of SVD based watermarking technique with DCT and DWT for copyright protection. They embedded the watermark into the principle components of cover image to improve the reliability. Then, the optimized MSFs were computed using Particle Swarm Optimization algorithm. DWT–SVD image watermarking using Firefly algorithm (FA) was introduced by Mishra et al. (2014). The fitness function of FA algorithm was a linear combination of imperceptibility and robustness. They report that the proposed approach is capable of identifying optimal MSFs such that the performance is better than existing methods. Ali and Ahn (2014) developed DWT–SVD watermarking algorithm with self-adaptive differential evolution (DE) to improve the performance of image watermarking. The scaling factors were optimized using self adaptive DE algorithm to yield highest possible robustness and better imperceptibility.

1.2. Research focus and contribution

In this study, the focus is to hide patient data in ECG signal with minimal deterioration to the signal. We use DWT to decompose the cover signal. SVD and quantization approach is used for watermark embedding. An optimization problem is formulated and solved using Continuous Ant Colony Optimization (CACO) algorithm to obtain MSFs. These MSFs when used in quantization provide superior imperceptibility and robustness of watermark than any Single Scaling Factor (SSF). One of the important outcomes of the study is a tradeoff curve between imperceptibility and robustness as a function of watermark size for different SSFs. If one wants to use a SSF for ECG type signals, this tradeoff curve can be utilized to pick up the appropriate scaling factor to achieve the respective imperceptibility and robustness.

Rest of the paper is organized as follows: In Section 2, the materials and methods discuss the database, CACO, DWT–SVD based ECG steganography and the proposed method. The results are discussed in detail in Section 3. The overall summary of the proposed research work is presented in Section 4.

2. Materials and methods

In this section we discuss the ECG database, preprocessing of ECG signal and patient data followed by DWT–SVD watermark embedding and extraction algorithms. CACO methodology is discussed as well.

2.1. Preprocessing of ECG signal and patient data

Important characteristic points of ECG signal are QRS complex, P, T and U waves. The rapid depolarization of right and left ventricle of heart is represented using QRS complex. Depolarization of atria and repolarization of ventricle are denoted by P and T waves, respectively. Repolarization of interventricular septum is referred as U wave (Li, Zheng, & Tai, 1995). These characteristic points play a vital role in characterizing an ECG signal. This study uses normal ECG signals from the MIT-BIH normal sinus rhythm database (Goldberger et al., 2000; Moody & Mark, 1990). The sampling frequency is 128 Hz and gain is 200. The proposed ECG steganography algorithm uses 2D ECG matrix as cover signal. In order to construct the 2D ECG image, 1D ECG signal is preprocessed using Pan–Tompkin's QRS detection algorithm (Pan & Tompkins, 1985). To achieve this, a 1D ECG signal is filtered through bandpass filters. The filtered signal is subjected to differentiation, squaring and moving average integration. Differentiation provides the QRS complex slope information. Squaring restricts false positives caused by T waves. The slope and width of QRS complex information are calculated using moving average integrator. The maximum slope of each QRS complex or peak of the R wave is referred as fiducial point. An ECG cycle consists of 64 samples each on both sides of the fiducial points of the signal which is referred as ECG train (Clifford, 2002, 2008,). Thus, the 1D ECG signal can be reconstructed using these fiducial points. There is negligible data loss during this conversion process.

The alphanumeric patient data such as name, age, location and registration number are converted into ASCII values followed by the conversion to binary stream which is referred as watermark. The reverse is performed to reconstruct the patient data after the retrieval process.

2.2. DWT–SVD watermark embedding and extraction

DWT is a time-frequency analysis that can be used to study an image/signal in different frequency bands with different resolution. This feature can be used to identify the least significant frequency sub-band of a signal. The characteristic points of ECG signal such as QRS complex, P and T waves lie in low frequency sub-bands. Hence, high frequency sub-band is the logical choice to embed the watermark to preserve diagnosability information. The advantage of DWT is that the original signal can be reconstructed by applying inverse DWT transform on frequency bands.

SVD is a matrix factorization technique and widely used in dimension reduction applications such as data compression. In the context of steganography, it is used to embed secret data. In 2D ECG steganography (Edward Jero et al., 2014), the singular values (SVs) of cover image is replaced by SVs of the secret data. However, there is a limit to the size of the watermark in this approach. SVD of a matrix A is mathematically represented as, $A = USV^T$; where U is the singular vectors of AA^T; S is the diagonal matrix containing singular values ordered in ascending order as $\{\sigma_1 > \sigma_2 > \sigma_3 > \ldots > \sigma_n\}$. V is the singular vectors of A^TA. $U^TU = V^TV = I$, where, I is an identity matrix.

2.2.1. Watermark embedding algorithm

In this section, we describe the algorithm to embed the SVs of patient data into the SVs of cover image.