Contents lists available at ScienceDirect

Biomedical Signal Processing and Control

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

# An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation

Y. Gangadhar[a,*], V.S. Giridhar Akula[b], P. Chenna Reddy[c]

[a] *Jawaharlal Nehru Technological University, Hyderabad, India*
[b] *Bandari Srinivas Institute of Technology, Hyderabad, India*
[c] *Jawaharlal Nehru Technological University, Ananthapuramu, India*

ARTICLE INFO

*Article history:*
Received 12 October 2017
Received in revised form 3 February 2018
Accepted 11 February 2018

*Keywords:*
Watermarking
Scalability
Particle swarm optimization
Authentication
Normalized coefficient

ABSTRACT

The importance of digital images in the field of health care made major impact in the recent years. There is need for protecting the medical images from unauthorized usage and watermarking serves well in this situations. Digital medical Image watermarking is the procedure of protecting the medical image content by inserting the watermark into it. The major objective of the image watermarking technique is to develop an algorithm with high imperceptibility. To achieve this, this paper proposed the image watermarking algorithm in wavelet transformation (IDWT) using the singular value decomposition (SVD) and particle swarm optimization (PSO). The improved DWT is applied to the medical image to retrieve the invariant wavelet domain. The watermark is inserted in to the selected region by modifying the values of the coefficients in the image using threshold function. The scaling factors are optimized using the PSO algorithm. The performance of the proposed model is evaluated using the existing schemes similar to the properties of the proposed model. The normalized coefficient (NC) and Peak Signal to Noise Ratio (PSNR) is considered to evaluate the similarity between the medical image and watermarked medical image. The proposed algorithm showed improved performance in terms of imperceptibility and robustness.

## 1. Introduction

The advancement in the digital era leads to the utilization of huge multimedia contents in the recent years [1–5]. This development in the digital technology also brings some issues regarding the distribution and unauthorized access of the multimedia content. To overcome these issues, digital watermarking has been introduced. The watermarking procedure is responsible for hiding the information in terms of watermark into the multimedia [59]. In general, inserting of watermarking causes degradation of image quality. This degradation is not visible to the human eye. Furthermore, the watermarked images are affected with distortions caused by active or passive attacks [35]. The watermark procedure must be robust against all the attacks. The robustness in the watermarking denotes the idea of extracting the watermark after the attacks are employed. According to the visibility, domain and permanency, the watermarking procedures are classified in to different types.

As per the visibility is concerned, the digital watermarking is classified into visible watermarking [60] and invisible watermarking [61]. In the visible watermarking procedure, the owner of the multimedia content is easily recognized. The main theme of the visible watermarking procedure is immediate recognition of the owner's identity in the multimedia content. The major drawback of the visible watermarking is that it can be easily tampered by the attackers using the image processing mechanisms [62]. In the invisible watermarking, the watermark is inserted in the multimedia at unknown places that are unnoticeable. The properties of the inserted watermark are similar to the original images. Therefore, it is difficult to identify the watermark in the original image.

In terms of domain, the watermarked techniques are classified into two types called as spatial domain and frequency domain. The spatial domain procedures are the oldest techniques that consider the modification of pixels in the image to the insertion of watermark. The commonly used approaches are spectrum [1] and least significant bit [2]. The advantages of spatial domain techniques are easy implementation procedure and low computation cost. However, the spatial domain techniques are not robust against all type of attacks. The frequency domain techniques are used to insert the watermark by transforming the original image with the help of

[*] Corresponding author.
*E-mail address:* ygangaphd@gmail.com (Y. Gangadhar).

https://doi.org/10.1016/j.bspc.2018.02.007
1746-8094/© 2018 Elsevier Ltd. All rights reserved.

discrete wavelet transform [3,4], Ridgelet transform [5,6], discrete cosine transform [7,8], discrete Hadamard transform [9,10], and discrete Fourier transform [11,12]. After that the watermark insertion procedure is applied. These techniques are widely acceptable and more robust against all type of attacks.

While permanency is concern, the invisible watermarking approaches are divided into three types, such as fragile watermarking [13,14], semi-fragile watermarking [15,16] and robust watermarking [17,18]. Fragile watermarking techniques are developed for identification of tampers in the watermarked images. These techniques are guaranteed the authenticity and integrity [65]. Semi-fragile watermarking techniques are the combination of both fragile and robust watermarking approaches. These techniques are robust against some attacks [63] and fragile against other attacks [64]. Robust watermarking techniques are developed to handle all type of attacks that are caused to tamper the watermarked images. The major types of attacks are compression, noise addition, filtering, image compression, geometric transformation and many more. The main theme of these techniques is to identify the origin of the attacks. The robust watermarking techniques are rich in providing the authenticity and verification of the images.

Since 1990, the machine learning approaches and artificial intelligence mechanisms such as neuro computing, fuzzy techniques and evolutionary algorithms are playing predominant role in solving real time problems in the applications. In this category, some of the algorithms [41,42,56,57] like Genetic algorithm (GA), Ant Colony Optimization algorithm (ACO), Firefly algorithm and Particle Swarm Optimization algorithm (PSO) made numerous contributions to the watermarking field. In [58], the watermarking scheme was developed based on multiple scaling factors using the GA approach. Particle swarm optimization (PSO) is an efficient and easy optimization mechanism when compared to the other evolutionary approaches. This optimization mechanism is widely used in different domains as well as in watermarking [19–21], Apart from the PSO advantages, it has some drawbacks that the global convergence of the algorithm not satisfactory in all times. It is due to the population diversity evolved from the solution set [22].

To address the issues of multi scaling factors in watermarking, this paper proposed the image watermarking algorithm in wavelet transformation (IDWT) using the singular value decomposition (SVD) and particle swarm optimization (PSO). The improved DWT is applied to the medical image to retrieve the invariant wavelet domain. Then, the low frequency sub-band is selected and divided in to four non-overlapping blocks. The suitable region is selected from the blocks using the entropy for watermark insertion. The watermark is inserted in to the selected region by modifying the values of the coefficients in the image using threshold function. The scaling factors are optimized using the PSO algorithm. The performance of the proposed model is evaluated using the existing schemes similar to the properties of the proposed model. The Normalized Coefficient (NC) and Peak Signal to Noise Ratio (PSNR) are considered to evaluate the similarity between the original image and watermarked image. The attacks are employed to test the robustness of the proposed approach. The novelty of the proposed watermarking approach represented as follows:

i) The proposed watermarking scheme utilized improved discrete wavelet transformation (IDWT) referred from Li et al. [23] to retrieve the invariant wavelet domain.
ii) The entropy mechanism is used to identify the suitable region for insertion of watermark. This will improve the imperceptibility and robustness of the watermarking procedure.
iii) The application of SVD in other domains like DWT, DCT and DFT improves the watermarking procedure. Therefore, SVD is applied to the invariant wavelet domain.
iv) The scaling factors such as PSNR and NC are considered for evaluation of the proposed method and the PSO is employed to optimize the scaling factors.

The rest of the paper is organized as follows: Section 2 deals with the related work regarding the different approaches employed medical image watermarking. Section 3 deals with preliminaries used in the paper. Section 4 explains about the proposed watermarking algorithm. Section 5 evaluates the experimental results and finally Section 6 concludes the research work.

## 2. Related work

This section deals with the existing watermarking approaches based on singular value decomposition (SVD) along with artificial intelligence based watermarking approaches are explained. In [44], the authors proposed watermarking approach based on the combination of SVD and discrete wavelet transformation (DWT). After the transformation is applied to the host image, the image is divided in to LL, LH, HL, HH sub-bands. The SVD is applied to the original image to replace with the SVD values of the watermark. In [45], Liu and Tan developed the watermarking scheme based on SVD in spatial domain. The authors made the changes to original image singular values with the values of singular matrix generated with the watermark image. In [46], a robust watermarking scheme was proposed for multimedia content. The host image is decomposed in to four equal sub-bands and then SVD is applied to two of the selected sub-bands. U and S matrices are used to insert the watermark. They followed the quantization for watermark insertion.

In [47], the author proposed a method to store the information of patients in to the medical images. They employed the reversible watermarking approach for inserting the patient's information (text data) into medical image with high security. The high secured practices such as error detection rate, RS codes and hamming codes are used to protect the patient's data within the image. But, the quality of the image will be reduced after the insertion of the watermark. Tricheli et al. [48] proposed the encryption method for preserving the patient's data which is of 170 characters. The characters are converted in to binary format and then applied the private key encryption method for scrambling the data bits. In this approach, the authors considered the region of interest (ROI) and region of non interest (RONI) by creating the virtual border inside the image. The RoI is within the virtual border and RoNI is the outside the virtual border. The encrypted data is inserted in to the RoNI to preserve the original content unaltered.

Giakuomaki et al. [49], proposed the Haar wavelet transformation by combining with quantization parameters for providing authentication and security through digital watermarking. The authors made an attempt to insert the digital signature of the doctors and the patient's information as the caption to the digital signature. This will provide the authentication of the patient's data and is easy to find out the tampering of the images [50–54]. Dandapat et al. [55] developed embedding technique using the DWT method for inserting the medical data in to the images. The authors employed the diagnostic distortion measure to divide the image in to two sets, such as least sensitive region and high sensitive region. The least sensitive region is selected for inserting the medical data.

## 3. Preliminaries used in the algorithm

This section deals with the concepts that are used to transform the medical image in to wavelet transformation and then selects the blocks for watermark insertion.