

An Improved Medical Image Watermarking Technique Based on Weber's Law Descriptors

KVSV Trinadh Reddy*, S. Narayana Reddy

Department of ECE, S.V. University College of Engineering, Andhra Pradesh 517501, India

Corresponding Author Email: trinadh.reddy@prepladder.com



<https://doi.org/10.18280/ts.380607>

ABSTRACT

Received: 12 August 2021

Accepted: 28 November 2021

Keywords:

watermarking, embedding capacity, medical image, blind watermarking, Weber's Local Descriptor (WLD), Arnold chaotic map

In distributed m-health communication, it is a major challenge to develop an efficient blind watermarking method to protect the confidential medical data of patients. This paper proposes an efficient blind watermarking for medical images, which boasts a very high embedding capacity, a good robustness, and a strong imperceptibility. Three techniques, namely, discrete cosine transform (DCT), Weber's descriptors (WDs), and Arnold chaotic map, were integrated to our method. Specifically, the Arnold chaotic map was used to scramble the watermark image. Then, the medical image was partitioned into non-overlapping blocks, and each block was subjected to DCT. After that, the scrambled watermark image data were embedded in the middle-band DCT coefficients of each block, such that two bits were embedded in each block. Simulation results show that the proposed watermarking method provides better imperceptibility, robustness, and computational complexity results with higher embedding capacity than the contrastive method.

1. INTRODUCTION

In the information era, a huge amount of data is transmitted online. The security of information and the protection of multimedia copyright become challenging problems. To cope with these challenges, digital watermarking and many other techniques have been developed. There are three fundamental requirements of digital watermarking: robustness, imperceptibility, and security (e.g., copyright, integrity, authenticity, and source traceability). However, the three requirements are conflicting. For example, a high robustness will sacrifice the perceptual transparency of the watermark, and vice versa. Watermarking protects the original data by embedding the information in multimedia.

Since the 1990s, digital watermarking has been growing rapidly. To protect the copyright of multimedia data, the technique is mainly applied in the following cases: intellectual property protection of multimedia, anti-counterfeiting of invoices in financial contracts, and the hidden recognition and tampering tips of videos/audios [1]. Basically, the watermarking process involves three steps: generation, embedding, and extraction.

Watermarking methods can be roughly divided into three types: robust watermarking, fragile watermarking, and semi-fragile watermarking [2]. The robust watermarking guarantees that the watermark image cannot be affected with any change on transformations [3]. The fragile watermarking allows the image to collapse with respect to any kind of transformations [4]. The semi-fragile watermarking endures minor alteration [5].

Recently, quantum image watermarking has attracted much attention [6-9]. The quantum image can be characterized with the colors of monochromatic electromagnetic waves. Watermarking can be done both in spatial and frequency domains. In the spatial domain, watermarking is achieved by operating directly on pixels. This reduces the computing cost,

but weakens robustness. In the frequency domain, the cover image is first converted from the spatial domain to the frequency domain through various transforms, such as discrete Fourier transform (DFT) [10], discrete cosine transform (DCT) [11], discrete wavelet transform (DWT) [12-14], and singular value decomposition (SVD) [15]. Frequency-domain watermarking is more computationally intensive but more robust than spatial-domain watermarking.

This paper combines DCT with Weber's descriptors (WDs) and Arnold chaotic map to improve the imperceptibility and robustness of image watermarking altogether. Specifically, the chaotic map was applied to the binary watermark image, and DCT was performed on the host image. The middle-band coefficients were considered for embedding the binary watermark image. The Arnold chaotic map was adopted to scramble the binary watermark image, and hence provides more protection.

The rest of the paper is organized as follows: Section 2 briefly reviews the relevant literature; Section 3 gives the basic preliminaries, and proposed an algorithm; Section 4 presents the comprehensive results; Section 5 compares the performance of the proposed algorithm with that of the related watermarking method; Section 6 concludes the research.

2. LITERATURE REVIEW

The existing watermarking techniques employ different algorithms. Embedding capacity is the most demanding function of these techniques. Zhang et al. [16] adopted a reversible watermarking method to improve the embedding capacity: a quadratic difference expansion is applied on adjacent pixels. This watermarking method not only doubles the embedding capacity, but also significantly improves the visual quality. Taha et al. [17] developed a perceptual mapping model by integrating integer-based lifting wavelet transform

into an adaptive watermarking algorithm. This algorithm can quickly embed and extract the watermark bits, and achieve a good imperceptibility. Ernawan and Kabir [18] presented a watermarking method, which modifies the selected DCT coefficients according to the features of human vision. For additional protection, an Arnold chaotic map was used to encrypt the watermark bits. This watermarking method achieves a good imperceptibility and a high robustness.

Sun et al. [19] designed an efficient and robust watermarking algorithm, which effectively employs multilayer back propagation (BP) feed-forward neural network in compressed domain. This algorithm trains the neural network with three layers, and obtains the host image through decompression. Ariatmanto and Ernawan [20] created a novel embedding technique with a good robustness and a desirable imperceptibility. At first, the host image was partitioned into non-overlapping blocks of the size 8×8 , and the variance of every block was calculated to determine the embedding regions. The binary watermark bits were embedded with various strengths, which depend on the set of self-designed rules [20]. Singh [21] put forward a robust watermarking technique for embedding medical images with the help of three transforms. Despite its high robustness, this technique demands a high computational cost.

Chan et al. [22] came up with a watermarking method that partitions the cover image and watermark image into blocks before embedding. To ensure robustness, an ordered Hadamard transform (OHT) was applied on the partitioned blocks. But this method is susceptible to some attacks. The watermarking technique proposed by Singh, D. and Singh, S. [23] divides the watermark in two parts: the first part is concerned with the four most significant bits, and the second part with remaining four bits of all pixels. Thereafter, the two parts are converted into the frequency domain. This technique achieves a good robustness at a high computational cost. Experimental results show that the technique is more robust and secure than the earlier approaches. Ghadi et al. [24] employed a Jacobian matrix to embed the watermark image in a spatial domain, with the mean of all the pixels in every 8×8 block as a key. This algorithm achieves a high imperceptibility and a high robustness, but requires lots of operations.

Bhatnagar et al. [25] applied fractional wavelet packet transforms to improve the robustness of watermarking against various attacks. In this method, it is only possible for the authorized to access data, for the prior knowledge of the host image is a must for data accesses. If the requestor is an unauthorized intruder, the watermark results will be eliminated through the degradation of the quality of the observed image. Abdelhakim et al. [26] designed a new fitness function based on artificial bee colony (ABC) algorithm to embed a watermark image. The blind watermarking technique, coupled with ABC fitness function, achieves a good robustness at the cost of computing time and robustness.

Moghaddam and Nemati [27] adopted an imperialist competitive algorithm (ICA) to locate the optimum pixels for embedding watermark image in the spatial domain. This watermarking method realizes a good robustness and a high imperceptibility, but takes numerous operations to embed watermark image. AL-Nabhani et al. [28] combined DWT and probabilistic neural network (PNN) into a robust watermarking technique, which trains the DWT coefficients to embed the watermark image. The watermarking method boasts high embedding capacity, imperceptibility, and embedding capacity. However, it cannot protect image quality

from being undermined by compression attacks. Dong et al. [29] proposed two watermarking methods for public and private watermarking applications. One of them relies on image normalization, and the other adopts mesh-based resynchronization. The two methods realize low bit error rates and perfect detection results, even under some attacks.

Arsalan et al. [30] developed an intelligent watermarking method coupling integer wavelet transform (IWT) and genetic programming (GP). The GP was adopted to select IWT coefficients, and then to embed watermark image. This method realizes good data payload and imperceptibility, but does not provide a good robustness. Han et al. [31] developed a robust and imperceptible watermarking method with a strong embedding capacity based on genetic algorithm. Arya et al. [32] proposed a non-blind watermarking method, which embeds two binary watermark bits in LL2 and HH2 sub-bands, and hence obtains a good robustness against attacks like JPEG compression, filtering, and geometric distortions. Soualmi et al. [33] created a blind watermarking technique for medical images: watermark data are embedded in four middle-band DCT coefficients, according to the orientation of these coefficients. In this way, the technique is robust against attacks like JPEG compression, noising, and median filtering. Nevertheless, the technique faces a low embedding capacity [33].

This paper designs an effective blind watermarking method for medical images. DCT, WDs, and Arnold chaotic map were synthesized to enhance the robustness against various attacks, such as JPEG compression, noising, and median filtering. The proposed method can realize a strong imperceptibility, and a good embedding capacity. The excellence in embedding capacity is attributed to embedding two watermark bits in a block of size 4×4 .

3. METHODOLOGY

The proposed watermarking technique includes two processes: watermark embedding, and watermark extraction.

3.1 Arnold scrambling

Digital image scrambling relocates image pixels randomly to increase confusion, turning the original image into a meaningless image. The security of image information is thereby improved. The scrambling mainly aims to transform a basic image into a disordered image, and to remove the high correlation among neighboring pixels. The most popular scrambling technique is the highly secure Arnold transform [34]. The Arnold scrambling method can be described as follows:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \bmod N; i', j', i \text{ and } j = \{0, \dots - 1\} \quad (1)$$

where, i and j are the coordinates of a pixel in the watermarking image; i' and j' are the coordinates of a pixel in the scrambled image. The original image can be restored through inverse Arnold scrambling as follows:

$$\begin{bmatrix} i \\ j \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} i' \\ j' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \right) \bmod N \quad (2)$$

3.2 WDs

The Weber's law illustrates that the ratio of the increment threshold to the background intensity is a constant [35]. Inspired by this law, Chen et al. [36] proposed a Weber's local descriptor (WLD), which contains a differential excitation (ξ) and an orientation (φ). The differential excitation $\xi(P)$ of a pixel P can be calculated by:

$$\xi(P) = \arctan \left[\sum_{n=0}^{m-1} \left(\frac{P_n - P}{P} \right) \right] \quad (3)$$

where, P_n is the intensity of m neighboring pixels. The orientation $\varphi(P)$ of a pixel P with m neighboring pixels can be calculated by:

$$\varphi(P) = \text{median}(\varphi(i)); i = \{0, \dots, m-1\} \quad (4)$$

where, $\varphi(i)$ can be expressed as:

$$\varphi(i) = \arctan \left(\frac{P_{R(i+4)} - P_i}{P_{R(i+6)} - P_{R(i+2)}} \right); i = \{0, \dots, m-1\} \quad (5)$$

where, $p_i (i = 0, \dots, m-1)$ are the neighbors of the current pixel P ; $R(y)$ is the modulus operation, i.e., $R(y) = \text{mod}(y, m)$. Formulas (4) and (5) indicate the insufficiency of computing only half of the angles, as there exists symmetry for $\varphi(i)$ s when I falls in $[0, m/2-1]$ or $[m/2, m-1]$. In this paper, the orientation φ is employed in the frequency domain for watermark embedding and extraction.

3.3 Watermark embedding

Figure 1 illustrates the complete process of watermark embedding. Firstly, the region of interest (ROI) is selected in the medical image (host image). Then, the watermark image is embedded in the ROI to provide additional protection of the watermark image. After that, the ROI is divided into non-overlapping blocks of the size 4×4 . Each block is subjected to the DCT, and the middle-band coefficients of DCT are used for embedding the watermark image.

Soualmi's method [33] only embedded one bit in each 4×4 block, whereas our method embeds two bits in each 4×4 block to enhance the embedding capacity. To embed an $N \times N$ binary watermark image, Soualmi's method [33] required that the host image must be no smaller than $4N \times 4N$. By contrast, a host image of $2N \times 4N$ or $4N \times 2N$ is sufficient in our method. In other words, in Soualmi's approach [33], a host image of $4N \times 4N$ can embed only one $N \times N$ binary watermark image. Meanwhile, in

our method, a host image of $4N \times 4N$ can embed two $N \times N$ binary watermark images or a single $2N \times N$ or $N \times 2N$ binary watermark image. Before embedding, the binary watermark image is scrambled by Arnold chaotic map to enhance the security of the binary watermark image.

To improve the robustness of Arnold transform, this paper proposes a two-level image scrambling process. Firstly, pseudo random number sequences R_0 and R_1 of the size N are generated, and the size of the binary watermarking image is denoted as $N \times N$. Then, the rows of the binary watermarking image are permuted with pseudo random number sequence R_0 , and the columns of the image are permuted with pseudo random number sequence R_1 . After the rows and columns are scrambled into an image, all the pixels of this image are scrambled by Arnold transform.

As shown in Figure 2, the watermark image is mainly embedded through the following steps:

- Step 1 Scramble the two $N \times N$ binary watermarking images through two-level image scrambling process (the concatenation of these two images is denoted by W).
- Step 2 Select the ROI of the medical image (host image).
- Step 3 Divide the selected ROI into 4×4 non-overlapping blocks $B_i, i = 1, \dots, N^2$.
- Step 4 Set $i = 1$
- Step 5 Apply DCT on a block B_i and select 2 middle-band coefficients (C_1 and C_2).
- Step 6 Calculate the orientation (φ) of B_i :

$$\varphi(B_i) = \arctan \left(\frac{C_1}{C_2} \right)$$

- Step 7 Adjust the boundaries: If $\varphi(B_i) = 0^\circ$ or 45° or -45° or 90° or -90° , modify $\varphi(B_i)$ by a small angle through modification of either of C_1 and C_2 of B_i .
- Step 8 Embed the scrambled binary watermarking image bits W_{2i-1} and W_{2i} on the two middle-band coefficients C_1 and C_2 of B_i according to the following cases:

- Case 1 If $0^\circ < \varphi(B_i) < 45^\circ$, modify the values of $C_1, C_2, C_3,$ and C_4 as follows:
 - If $W_{2i-1}W_{2i} = 01$, then $C_1 = -C_1$.
 - If $W_{2i-1}W_{2i} = 10$, then permute (C_1, C_2).
 - If $W_{2i-1}W_{2i} = 11$, then permute (C_1, C_2) and $C_1 = -C_1$.
 - $C_1 = C_1 + K$.
- Case 2 If $45^\circ < \varphi(B_i) < 90^\circ$, modify the values of $C_1, C_2, C_3,$ and C_4 as follows:
 - If $W_{2i-1}W_{2i} = 11$, then $C_1 = -C_1$.
 - If $W_{2i-1}W_{2i} = 00$, then permute (C_1, C_2).
 - If $W_{2i-1}W_{2i} = 01$, then permute (C_1, C_2) and $C_1 = -C_1$.
 - $C_1 = C_1 + K$.
- Case 3 If $-45^\circ < \varphi(B_i) < 0^\circ$, modify the values of $C_1, C_2, C_3,$ and C_4 as follows:
 - If $W_{2i-1}W_{2i} = 00$, then $C_1 = -C_1$.

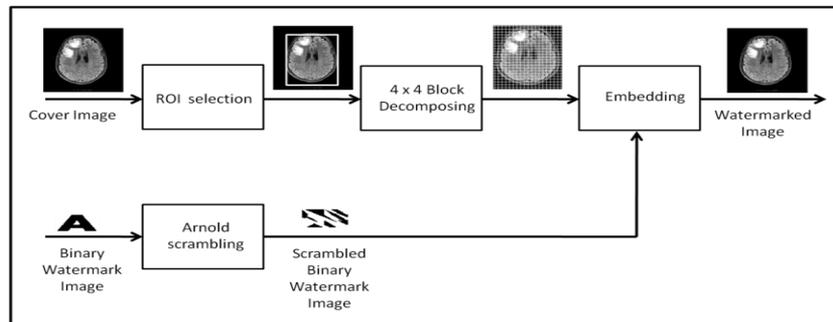


Figure 1. Watermark embedding process

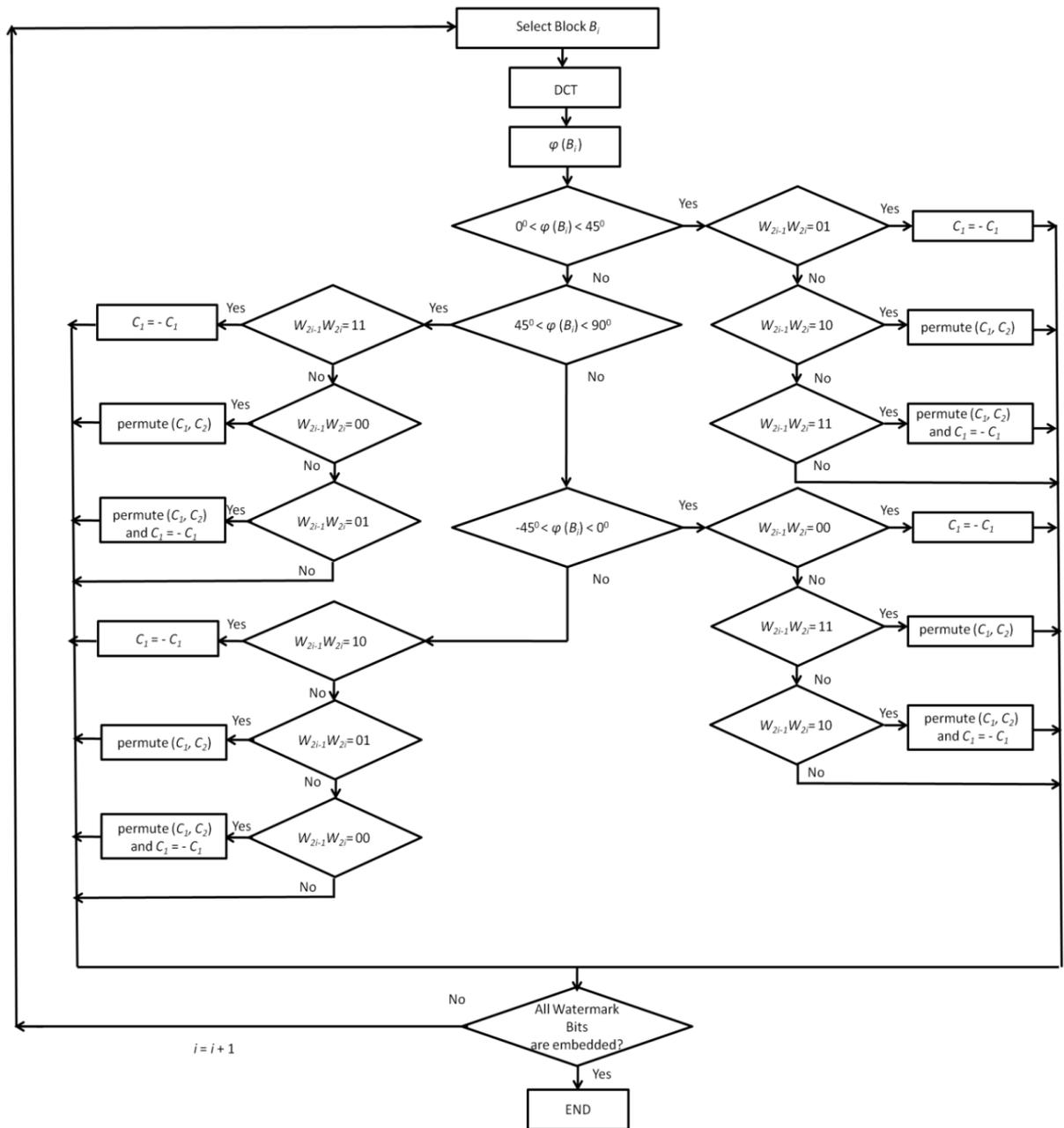


Figure 2. Flow of watermark bits embedding in our algorithm

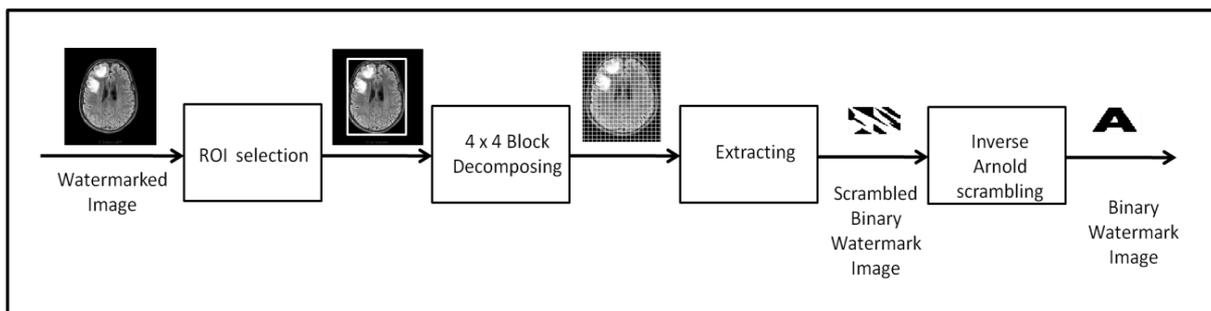


Figure 3. Watermark extracting process

- If $W_{2i-1}W_{2i} = 11$, then permute (C_1, C_2) .
 - If $W_{2i-1}W_{2i} = 10$, then permute (C_1, C_3) and $C_1 = -C_1$.
 - $C_1 = C_1 + K$.
 - If $W_{2i-1}W_{2i} = 10$, then permute $C_1 = -C_1$.
 - If $W_{2i-1}W_{2i} = 01$, then permute (C_1, C_2) .
 - If $W_{2i-1}W_{2i} = 00$, then permute (C_1, C_2) and $C_1 = -C_1$.
 - $C_1 = C_1 + K$.
- Case 4 If $-90^\circ < \varphi(B_i) < -45^\circ$, modify the values of C_1, C_2, C_3 , and C_4 as follows:
- where, K is an embedding strength to reinforce the presence of

the watermark.

Step 9 Apply the inverse DCT on a block B_i .

Step 10 If not all the watermark bits are embedded, return to Step 5 with $i = i + 1$.

During the embedding process, the WLD, i.e., orientation (φ) of B_i , is calculated with only two middle-band coefficients instead of four in formula (5). Taking two coefficients instead of four can improve the imperceptibility, and effectively solve the above four possible cases. In addition, the presence of four cases makes it possible to embed two watermark bits in one block, thereby increasing the embedding capacity.

3.4 Watermark extracting

Figure 3 explains the flow of watermark image extraction. Because our watermarking technique is a blind approach, the embedding secret is sufficient for the extracting a watermark image. Similar to the embedding process, the extraction process firstly selects the ROI of the host image, and then extracts a watermark image from that ROI.

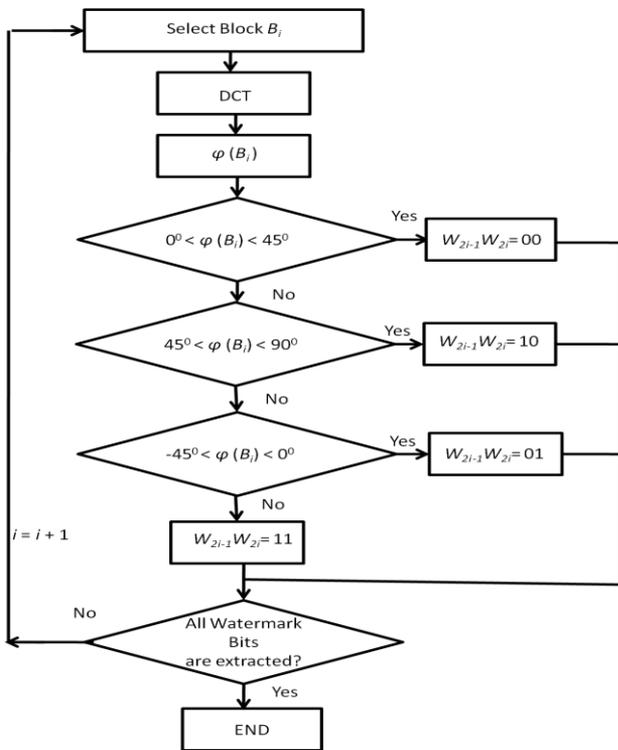


Figure 4. Flow of watermark bits extraction in our algorithm

As shown in Figure 4, the watermark image can be extracted in the following steps:

- Step 1 Select the ROI of the medical image (host image).
- Step 2 Divide the selected ROI of host image into 4×4 non-overlapping blocks B_i , $i = 1, \dots, N^2$.
- Step 3 Set $i = 1$
- Step 4 Apply DCT on a block B_i , and select 2 middle-band coefficients (C_1 and C_2).
- Step 5 Calculate the orientation (φ) of B_i by:
- Step 6 Extract the scrambled binary watermarking image bits W_{2i-1} and W_{2i} according to the following cases:
 - Case 1 If $0^\circ < \varphi(B_i) < 45^\circ$, $W_{2i-1}W_{2i} = 00$
 - Case 2 If $45^\circ < \varphi(B_i) < 90^\circ$, $W_{2i-1}W_{2i} = 10$
 - Case 3 If $-45^\circ < \varphi(B_i) < 0^\circ$, $W_{2i-1}W_{2i} = 01$
 - Case 4 If $-90^\circ < \varphi(B_i) < -45^\circ$, $W_{2i-1}W_{2i} = 11$

Step 7 Apply the inverse DCT on a block B_i .

Step 8 If not all the watermark bits are extracted, return to Step 4 with $i = i + 1$.

Step 9 Inverse scramble the extracted watermark image to get the original watermark image.

4. EXPERIMENTAL RESULTS

Several experiments were carried out on grayscale medical images (host images) of 256×256 and a binary watermark image of 32×64 . The embedding strength K in these tests was set to 30. The proposed watermarking method was tested against various attacks, such as JPEG compression, filtering, noising, and geometric distortions.

Figure 5 shows the host images and the binary watermark image used in the experiments. The experimental results were evaluated by famous metrics like peak signal-to-noise ratio (PSNR), structural similarity (SSIM), and normalized cross-correlation (NC). The PSNR and SSIM were calculated between the watermark image and the host image. The PSNR can be calculated by the mean squared error (MSE):

$$MSE = \frac{1}{m \times n} \sum_{u=0}^{m-1} \sum_{v=0}^{n-1} [X(u, v) - Y(u, v)]^2 \quad (6)$$

$$PSNR = 10 \log \left(\frac{255^2}{MSE} \right) \text{ dB} \quad (7)$$

where, X and Y are the host and watermark images of the size $m \times n$. The SSIM between the host and watermark images can be defined as:

$$SSIM = \frac{(2\mu_1\mu_2 + c_1)(2\sigma_j + c_2)}{(\mu_1^2 + \mu_2^2 + c_1)(\sigma_1^2 + \sigma_2^2 + c_2)} \quad (8)$$

where, μ_1 and μ_2 are the mean values of the host and watermark images, respectively; σ_1 and σ_2 are the variances of the host and watermark images, respectively; σ_j is the covariance of the watermark images; c_1 and c_2 are the two constants used to avoid the zero dominators. The NC between the original watermark W and the extracted watermark W' can be calculated by:

$$NC = \frac{1}{wm \times wn} \sum_{u=0}^{wm-1} \sum_{v=0}^{wn-1} [W(u, v) \oplus W'(u, v)] \quad (9)$$

where, \oplus is the exclusive-or (XOR) operation; $w_m \times w_n$ is the size of the watermark image. The quality of watermark image was evaluated with $PSNR$ and $SSIM$, while the quality of extracted watermark image was evaluated with NC . Figure 6(a)-(j) display the watermark images of the host images in Figures 5(a)-(j), respectively. The binary watermark image extracted from these watermark images is shown in Figure 6 (k).

Table 1 lists the performance results, e.g., $PSNR$, $SSIM$, NC , embedding time, and extraction time, of the proposed method for various host images and a binary watermark image in Figure 5. The results of the proposed algorithm were evaluated in terms of imperceptibility, robustness, and computational complexity.

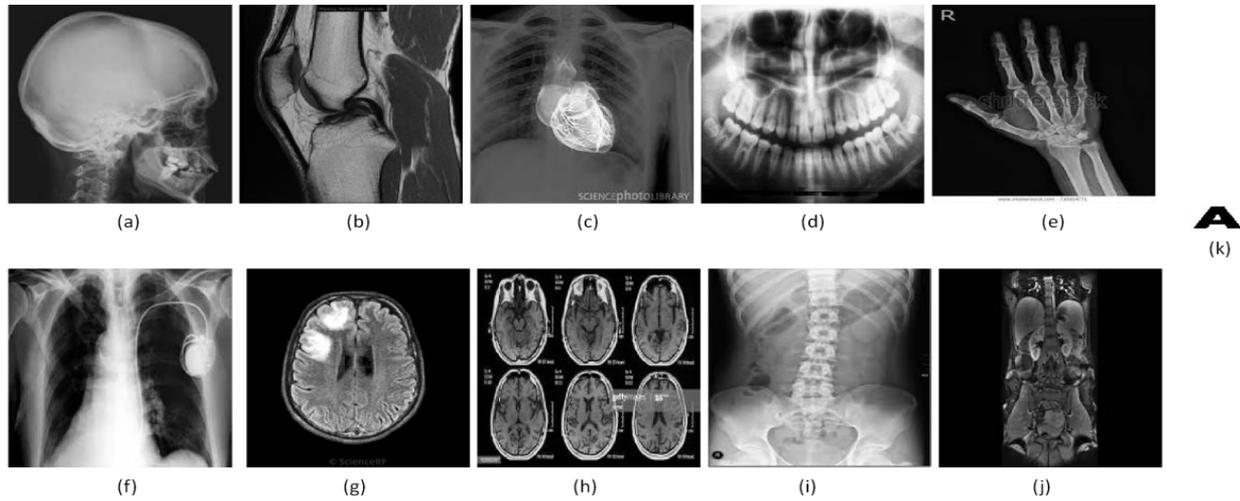


Figure 5. (a)-(j) the host images, and (k) the binary watermark image

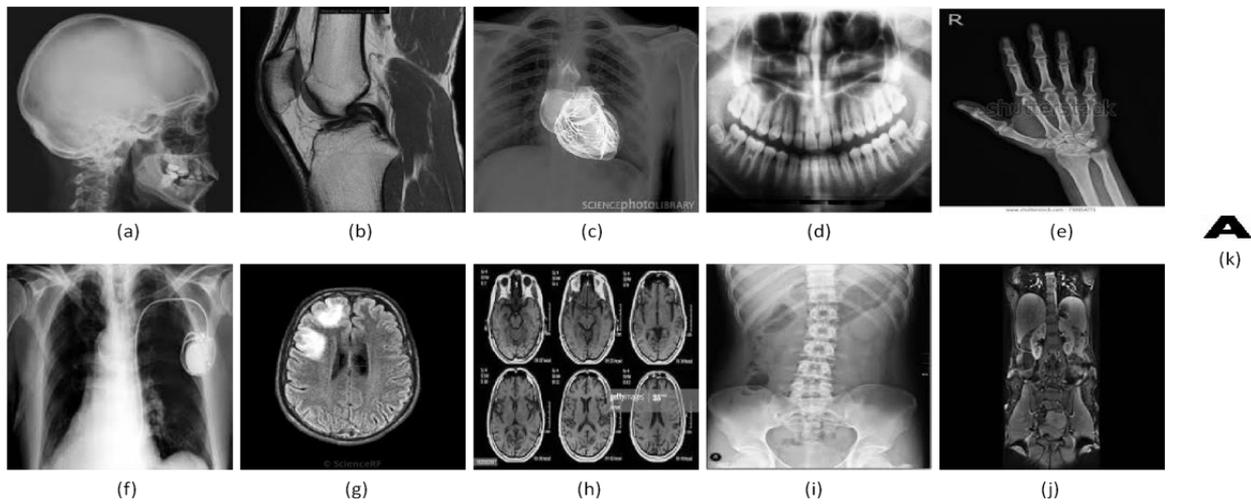


Figure 6. (a)-(j) the watermark images of the host images in Figures 5 (a) – (j), respectively, and (k) the binary watermark image extracted from these watermark images

4.1 Imperceptibility measurement

The watermark imperceptibility refers the degree to which the watermark image is similar to the host image. Hence, the imperceptibility of the proposed watermarking technique can be measured by *PSNR* and *SSIM*. If the *MSE* is small or the *PSNR* is high, then the watermark has a strong imperceptibility, i.e., the watermark image is not severely distorted. The closer the *SSIM* is to 1, the more similar the watermark image is to the host image.

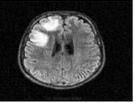
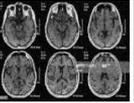
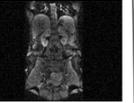
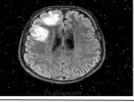
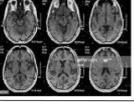
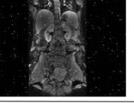
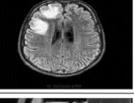
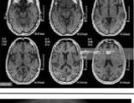
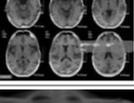
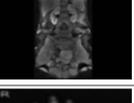
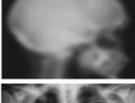
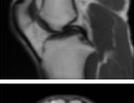
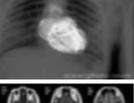
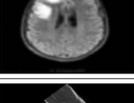
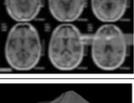
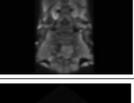
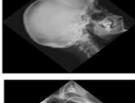
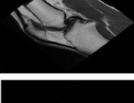
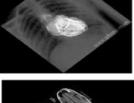
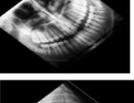
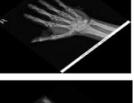
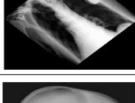
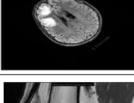
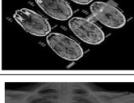
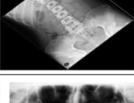
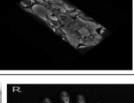
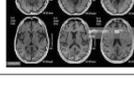
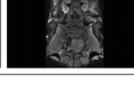
Table 1 shows the watermark imperceptibility of the proposed watermarking technique in terms of *PSNR* and *SSIM* between the watermark image and the host image. It is very clear that the proposed watermarking method achieved very encouraging results: the *PSNR* values for all images exceeded 42dB, and the *SSIM* values for all watermark images surpassed 0.99. It is also apparent that no visual degradation was found in the watermark images, through comparison with the original host images. Hence, the proposed watermarking technique maintains the quality of the watermark image, as compared to

the host images. This is because only two middle-band coefficients of the blocks are slightly adjusted during the embedment of binary watermark data. Furthermore, the *NC* for all images was equal to 1, suggesting that each extracted watermark image is similar to the original watermark image.

Table 1. Performance results of the proposed method

Cover Image in Figure 5	Performance results				
	PSNR (dB)	SSIM	NC	Embedding Time (s)	Extraction Time (s)
(a)	58.59	0.9994	1	0.0916	0.0419
(b)	47.71	0.9948	1	0.0888	0.0410
(c)	52.21	0.9962	1	0.0908	0.0411
(d)	53.40	0.9979	1	0.0863	0.0407
(e)	49.58	0.9979	1	0.0905	0.0411
(f)	54.69	0.9987	1	0.0936	0.0418
(g)	48.05	0.9977	1	0.0943	0.0421
(h)	43.64	0.9949	1	0.0938	0.0423
(i)	55.25	0.9985	1	0.0927	0.0413
(j)	49.55	0.9981	1	0.0978	0.0426

Table 2. Robustness measurement of the proposed method

	Attacked watermarked images					Extracted watermark images	Average NC value
White-noise $V = 0.005$							0.9075
							
Salt and pepper noise $V = 0.01$							0.9824
							
Speckle noise $V = 0.01$							0.9702
							
Median Filtering [3,3]							0.8939
							
Average filtering [3,3]							0.8895
							
Rotation by 45°							0.7457
							
JPEG compression (50)							0.8926
							

4.2 Robustness measurement

The robustness refers to the ability of a watermark to withstand the attacks that try to modify the original image. Here, the robustness is measured by *NC*. The closer the *NC* value is to 1, the more similar the extracted watermark image is to the original watermark. The robustness of our method was tested under various attacks, namely, JPEG compression,

filtering, noising, and geometric distortions. The *NC* values were calculated under each attack.

Table 2 presents the mean *NC* results. It can be observed that the proposed algorithm achieved a good robustness, as the *NC* values were high except for geometric distortions like rotation and scaling. The good robustness comes from the slight change of the orientation, when the coefficients are modified during attacks. Even if the watermark image is under

attack, our method can extract a binary watermark image with minimal distortion.

4.3 Computational complexity measurement

The computational complexity refers to the time consumed in the embedding and extraction processes of the watermarking method. Table 1 shows the time required for embedding and extracting the watermark images in various medical images. It is evident that our method took a very short execution time: less than 94ms was consumed for embedding, and 43ms for extraction. The time efficiency mainly arises from the swiftness of our method in embedding/extracting the binary watermark image in/from medical images.

5. PERFORMANCE COMPARISON

To demonstrate its efficiency, our method was compared with Soualmi’s method [33] in terms of imperceptibility, robustness, and computational complexity. For Soualmi’s method [33] and our method, 32×32 and 32×64 binary watermark images were embedded on the grayscale medical images (host images) of 256×256, respectively. The embedding strength K of both watermarking methods was set to 30. Table 3 compares the imperceptibility levels of the two methods. Table 4 compares the robustness levels of the two methods in terms of mean NC . Table 5 compares the computational complexities of the two methods.

It is clear from the Table 3 that, on average, the $PSNR$ values of the proposed method were approximately 1.55dB higher than those of Soualmi’s method [33] on various host images. This table also shows that our method achieved an approximately 0.003 higher mean $SSIM$ than Soualmi’s method [33]. Table 4 displays that the proposed watermarking method realized better average NC values than Soualmi’s method [33]. Table 5 shows that our watermarking method consumed a short time in embedding and extracting watermark bits.

Overall, the proposed watermarking method provides better imperceptibility, robustness, and computational complexity than Soualmi’s method [33], while doubling the embedding capacity. In Soualmi’s method [33], one watermark bit is embedded in a 4×4 block. Our method doubles the embedding capacity by embedding two watermark bits instead of one in a 4×4 block. The imperceptibility is improved by taking two coefficients instead of four coefficients.

Table 3. Imperceptibility comparison of the proposed method with Soualmi’s method [33]

Cover image in Figure 5	Our method		Soualmi’s method [33]	
	PSNR (dB)	SSIM	PSNR (dB)	PSNR (dB)
(a)	58.59	0.9994	54.05	0.9982
(b)	47.71	0.9948	46.06	0.9887
(c)	52.21	0.9962	50.09	0.9929
(d)	53.40	0.9979	50.25	0.9958
(e)	49.58	0.9979	49.39	0.9962
(f)	54.69	0.9974	49.28	0.9952
(g)	48.05	0.9977	47.18	0.9950
(h)	43.64	0.9949	42.97	0.9856
(i)	55.25	0.9985	50.58	0.9958
(j)	49.55	0.9981	48.40	0.9947

Table 4. Robustness comparison in terms of mean NC

Attack	Our method	Soualmi’s method [33]
White-Noise ($V=0.005$)	0.9075	0.8188
Salt & Pepper Noise ($V=0.01$)	0.9824	0.9539
Speckle Noise ($V=0.01$)	0.9702	0.8262
Median Filtering [3, 3]	0.8939	0.8079
Average Filtering [3, 3]	0.8895	0.8651
Rotation-45°	0.7457	0.6739
JPEG-Compression (50)	0.8926	0.8146

Table 5. Computational complexity comparison in terms of embedding and extracting time

Cover image in Figure 5	Our method		Soualmi’s method [33]	
	Embedding time (s)	Extraction time (s)	Embedding time (s)	Extraction time (s)
(a)	0.0916	0.0419	0.0951	0.0418
(b)	0.0888	0.0410	0.0923	0.0411
(c)	0.0908	0.0411	0.0907	0.0418
(d)	0.0863	0.0407	0.0843	0.0392
(e)	0.0905	0.0411	0.0934	0.0410
(f)	0.0936	0.0418	0.0920	0.0424
(g)	0.0943	0.0421	0.1037	0.0441
(h)	0.0938	0.0423	0.0956	0.0421
(i)	0.0927	0.0413	0.0922	0.0420
(j)	0.0978	0.0426	0.1077	0.0489

6. CONCLUSIONS

This paper presents an efficient blind watermarking method, which employs the DCT, WDs, and Arnold chaotic map to embed a binary watermark image in medical images. By computing the WDs, e.g., orientation, with only two middle-band DCT coefficients, our method realizes better imperceptibility and robustness, with considerably more embedding capacity. Besides, the method demonstrates a notable robustness performance against various attacks, such as noising, JPEG compression, and median filtering. The imperceptibility results of our method are interesting and encouraging. In addition, the proposed embedding and extraction algorithms take a short time for embedding and extracting the binary watermark image.

REFERENCES

- [1] Bhowmik, D., Oakes, M., Abhayaratne, C. (2016). Visual attention-based image watermarking. IEEE Access, 4: 8002-8018. <https://doi.org/10.1109/ACCESS.2016.2627241>
- [2] Shi, Y.Q., Li, X., Zhang, X., Wu, H.T., Ma, B. (2016). Reversible data hiding: Advances in the past two decades. IEEE Access, 4: 3210-3237. <https://doi.org/10.1109/ACCESS.2016.2573308>
- [3] Najafi, E., Loukhaoukha, K. (2019). Hybrid secure and robust image watermarking scheme based on SVD and

- sharp frequency localized contourlet transform. *Journal of Information Security and Applications*, 44: 144156. <https://doi.org/10.1016/j.jisa.2018.12.002>
- [4] Qin, C., Ji, P., Zhang, X., Dong, J., Wang, J. (2017). Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. *Signal Processing*, 138: 280-293. <https://doi.org/10.1016/j.sigpro.2017.03.033>
- [5] Singh, D., Singh, S.K. (2017). DCT based efficient fragile watermarking scheme for image authentication and restoration. *Multimedia Tools and Applications*, 76(1): 953-977. <https://doi.org/10.1007/s11042-015-3010-x>
- [6] Abd El-Latif, A., Abd-El-Atty, B., Hossain, M.S., Rahman, M.A., Alamri, A., Gupta, B.B. (2018). Efficient quantum information hiding for remote medical image sharing. *IEEE Access*, 6: 21075-21083. <https://doi.org/10.1109/ACCESS.2018.2820603>
- [7] Naseri, M., Heidari, S., Baghfalaki, M., Fatahi, N., Gheibi, R., Batle, J., Farouk, A., Habibi, A. (2017). A new secure quantum watermarking scheme. *Optik*, 139: 77-86. <https://doi.org/10.1016/j.ijleo.2017.03.091>
- [8] Soliman, M.M., Hassanien, A.E., Onsi, H.M. (2016). An adaptive watermarking approach based on weighted quantum particle swarm optimization. *Neural Computing and Applications*, 27: 469-481. <https://doi.org/10.1007/s00521-015-1868-1>
- [9] El-Latif, A.A.A., Abd-El-Atty, B., Hossain, M.S., Elmougy, S., Ghoneim, A. (2018). Secure quantum steganography protocol for fog cloud Internet of Things. *IEEE Access*, 6: 10332-10340. <https://doi.org/10.1109/ACCESS.2018.2799879>
- [10] Cooley, J., Lewis, P., Welch, P. (1959). The finite Fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 17(2): 77-85. <https://doi.org/10.1109/TAU.1969.1162036>
- [11] Roy, S., Pal, A.K. (2017). A blind DCT based color watermarking algorithm for embedding multiple watermarks. *AEU - International Journal of Electronics and Communications*, 72: 149-161. <https://doi.org/10.1016/j.aeue.2016.12.003>
- [12] Keivani, M., Sazdar, A.M., Mazloum, J., Rahmani, A.E. (2020). Application of empirical wavelet transform in digital image watermarking. *Traitement du Signal*, 37(5): 839-845. <https://doi.org/10.18280/ts.370517>
- [13] Nouioua, N., Seddiki, A., Ghaz, A. (2020). Blind digital watermarking framework based on DTCWT and NSCT for telemedicine application. *Traitement du Signal*, 37(6): 955-964. <https://doi.org/10.18280/ts.370608>
- [14] Lee, Y., Seo, Y., Kim, D. (2019). Digital blind watermarking based on depth variation prediction map and DWT for DIBR free-viewpoint image. *Signal Processing: Image Communication*, 70: 104-113. <https://doi.org/10.1016/j.image.2018.09.004>
- [15] Alshoura, W.H., Zainol, Z., Teh, J.S., Alawida, M., Alabdulatif, A. (2021). Hybrid SVD-based image watermarking schemes: A review. *IEEE Access*, 9: 32931-32968. <https://doi.org/10.1109/ACCESS.2021.3060861>
- [16] Zhang, Z., Zhang, M., Wang, L. (2020). Reversible image watermarking algorithm based on quadratic difference expansion. *Mathematical Problems in Engineering*, 2020: 1-8. <https://doi.org/10.1155/2020/1806024>
- [17] Taha, T.B., Ngadiran, R., Ehkan, P. (2018). Adaptive image watermarking algorithm based on an efficient perceptual mapping model. *IEEE Access*, 6: 66254-66267. <https://doi.org/10.1109/ACCESS.2018.2878456>
- [18] Ernawan, F., Kabir, M.N. (2018). A robust image watermarking technique with an optimal DCT-psychovisual threshold. *IEEE Access*, 6: 20464-20480. <https://doi.org/10.1109/ACCESS.2018.2819424>
- [19] Sun, L., Xu, J., Liu, S., Zhang, S., Li, Y., Shen, C. (2018). A robust image watermarking scheme using Arnold transform and BP neural network. *Neural Computing and Applications*, 30(8): 2425-2440. <https://doi.org/10.1007/s00521-016-2788-4>
- [20] Ariatmanto, D., Ernawan, F. (2020). An improved robust image watermarking by using different embedding strengths. *Multimedia Tools and Applications*, 79: 12041-12067. <https://doi.org/10.1007/s11042-019-08338-x>
- [21] Singh, A.K. (2017). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications*, 76: 8881-8900. <https://doi.org/10.1007/s11042-016-3514-z>
- [22] Chan, H., Hwang, W., Cheng, C. (2015). Digital hologram authentication using a Hadamard-based reversible fragile watermarking algorithm. *Journal of Display Technology*, 11(2): 193-203. <https://doi.org/10.1109/JDT.2014.2367528>
- [23] Singh, D., Singh, S. (2016). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, 76: 13001-13024. <https://doi.org/10.1007/s11042-016-3706-6>
- [24] Ghadi, M., Laouamer, L., Nana, L., Pascu, A. (2016). A novel zero watermarking approach of medical images based on Jacobian matrix model. *Security and Communication Networks*, 9: 50203-5218. <https://doi.org/10.1002/sec.1690>
- [25] Bhatnagar, G., Raman, B., Wu, Q.M.J. (2012). Robust watermarking using fractional wavelet packet transform. *IET Image Processing*, 6(4): 386-397. <https://doi.org/10.1049/iet-ipr.2010.0400>
- [26] Abdelhakim, A.M., Saleh, H.I., Nassar, A.M. (2017). A quality guaranteed robust image watermarking optimization with artificial bee colony. *Expert Systems with Applications*, 72: 317-326. <https://doi.org/10.1016/j.eswa.2016.10.056>
- [27] Moghaddam, M.E., Nemati, N. (2013). A robust color image watermarking technique using modified imperialist competitive algorithm. *Forensic Science International*, 233(1-3): 193-200. <https://doi.org/10.1016/j.forsciint.2013.09.005>
- [28] AL-Nabhani, Y., Jalab, H.A., Wahid, A., Noor, R.M. (2015). Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. *Journal of King Saud University - Computer and Information Sciences*, 27(4): 393-401. <https://doi.org/10.1016/j.jksuci.2015.02.002>
- [29] Dong, P., Brankov, J.G., Galatsanos, N.P., Yang, Y., Davoine, F. (2005). Digital watermarking robust to geometric distortions. *IEEE Trans. Image Process.*, 14(12): 2140-2150. <https://doi.org/10.1109/tip.2005.857263>
- [30] Arsalan, M., Qureshi, A.S., Khan, A., Rajarajan, M. (2017). Protection of medical images and patient related

- information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, 51: 168-179. <https://doi.org/10.1016/j.asoc.2016.11.044>
- [31] Han, J., Zhao, X., Qiu, C. (2016). A digital image watermarking method based on host image analysis and genetic algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 7: 37-45. <https://doi.org/10.1007/s12652-015-0298-3>
- [32] Arya, R.K., Singh, S., Saharan, R. (2015). A secure non-blind block based digital image watermarking technique using DWT and DCT. *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2042-2048. <https://doi.org/10.1109/ICACCI.2015.7275917>
- [33] Soualmi, A., Alti, A., Laouamer, L. (2018). A new blind medical image watermarking based on weber descriptors and Arnold chaotic map. *Arabian Journal for Science and Engineering*, 43: 7893-7905. <https://doi.org/10.1007/s13369-018-3246-7>
- [34] Wu, J., Liu, Z., Wang, J., Hu, L., Liu, S. (2021). A compact image encryption system based on Arnold transformation. *Multimedia Tools and Applications*, 80: 2647-2661. <https://doi.org/10.1007/s11042-020-09828-z>
- [35] Jain, A.K. (1989). *Fundamentals of Digital Image Processing*. vol. 3. Prentice-Hall, Englewood Cliffs.
- [36] Chen, J., Shan, S., He, C., Zhao, G., Pietikainen, M., Chen, X., Gao, W. (2010). WLD: A robust local image descriptor. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(9): 1705-1720. <https://doi.org/10.1109/TPAMI.2009.155>