

A hybrid DWT-DCT-SVD watermarking scheme using arnold transform

Van-Thanh Huynh¹, Thai-Son Nguyen², Thanh-C Vo¹

¹School of Engineering and Technology, Tra Vinh University, Trà Vinh, Vietnam

²Resource Development Institute, Tra Vinh University, Trà Vinh, Vietnam

Article Info

Article history:

Received Mar 23, 2025

Revised Oct 27, 2025

Accepted Nov 23, 2025

Keywords:

Arnold transform

Discrete cosine transform

Discrete wavelet transform

Medical image

Singular value decomposition

Watermarking

ABSTRACT

In telemedicine, medical images and electronic patient records (EPRs) are frequently transmitted and stored, making them vulnerable to tampering and theft. To ensure data security and copyright protection, this paper proposes a hybrid watermarking scheme based on discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). The method uses a two-level DWT to decompose the image, applies DCT to selected sub-bands, and embeds two watermarks. The first is a logo used for ownership verification, and the second is an EPR encrypted with the Arnold transform for privacy protection. SVD is then used to enhance robustness. Experimental results show that the proposed scheme achieves better image quality and stronger resistance to common attacks compared with existing watermarking methods.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Thai-Son Nguyen

Resource Development Institute, Tra Vinh University

85000 Vinh Long, Viet Nam

Email: thaision@tvu.edu.vn

1. INTRODUCTION

With the rapid development of image processing and digital transformation, digital data, i.e., texts, images, audio, and video, are increasingly transmitted and stored over public channels. In telemedicine, medical images, including MRI, ultrasound, X-ray, and CT scans, become more important for diagnostic procedures [1]. These images, obtained from hospitals, doctors, and insurance companies, are vulnerable to various malicious attacks. Any alteration to medical images or patient information can lead to misdiagnosis [2]. Therefore, preserving the integrity and confidentiality of medical data is essential [3]. Cryptography and watermarking techniques are two promising solutions to ensure data authenticity and security [4]. Cryptographic solutions, such as RSA, AES, and RC4, convert plaintext into ciphertext to secure data. However, encrypted data often attracts more attention from attackers. In contrast, watermarking conceals secret information into the cover data, making it imperceptible and difficult to detect. This approach ensures that the electronic patient records (EPRs) remain protected during transmission over open networks [2].

Image watermarking techniques are partitioned into two domains, namely the spatial domain and the frequency domain [5], [6]. Spatial domain techniques directly modify pixels to conceal watermarks. One of the simplest examples is the least significant bit replacement, which has been further improved in several works [7]-[10]. Spatial domain-based schemes offer lower complexity and easier implementation. However, these schemes exhibit lower image quality and weaker robustness. Consequently, research attention has shifted toward frequency domain watermarking. In frequency domain-based techniques, the cover image is first transformed into coefficients using well-known frequency transforms such as discrete cosine transform (DCT), discrete wavelet transform (DWT), redundant DWT, non-subsampled contourlet transform (NSCT),

stationary wavelet transform (SWT), principal component analysis (PCA), and singular value decomposition (SVD). These coefficients are then used to embed watermarks. To enhance security, hybrid watermarking schemes combining multiple transform algorithms have been proposed, such as SWT-DCT [11], [12], DWT-SVD [13]-[15], NSCT-RDWT-SVD [16], DWT-DCT-PCA [17], and RDWT-DCT-Schur decomposition [18].

Singh *et al.* [2] proposed a hybrid DCT-DWT-SVD watermarking scheme to achieve better imperceptibility and robustness against certain image processing and compression attacks. However, remained sensitive to geometric transformations like cropping, scaling, and rotation. To enhance robustness, a blind watermarking algorithm combining second-level DWT and SVD was proposed in [14], incorporating an encryption mechanism to resist intentional and unintentional attacks. Later, to improve authenticity [11], combined SWT and DCT for zero watermarking, using a chaotic map to scramble the watermark and protect it against geometric attacks. To maintain high security, Anand and Singh [15] proposed an improved dual watermarking technique using DWT-SVD, where Hamming coding minimized distortion. Their approach achieved higher robustness and imperceptibility but maintained image quality below 40 dB. To further enhance performance [16], combined NSCT, RDWT, and SVD in their watermarking scheme. Thakur *et al.* [16], singular values of two watermarks, i.e., the image watermark and the EPR watermark, are concealed into the singular matrix of the cover image. Their scheme improved image quality while maintaining robustness. Additionally, several studies have categorized the cover images into two regions, i.e., the region of non-interest (RONI) and the region of interest (ROI). Watermarking is performed only in the RONI region to preserve diagnostic quality [19], [20]. For instance, Swaraja [20] employed DWT and Schur transforms for watermarking in telemedicine applications, achieving stronger robustness while guaranteeing image quality. Besides efforts to enhance watermark robustness for copyright authentication, several studies focus on fragile watermarks for tamper detection, as proposed in [21]-[24].

Since the hybrid schemes discussed in the previous section have not fully examined the selection coefficients for embedding, their ability to balance robustness and imperceptibility is limited. To further enhance both image quality and robustness, a novel hybrid watermarking scheme is proposed. In the proposed scheme, the original image is first transformed into four different sub-bands (LL_i , HH_i , LH_i , and HL_i) using DWT. Then, to achieve the balance between robustness and image quality, three sub-bands (HH_i , LH_i , and HL_i) are further decomposed using a second-level DWT. Next, the most suitable sub-bands are selected and processed using DCT. Then, DCT coefficients located in the mid-frequency ranges are chosen for embedding. Additionally, to increase security, the EPR watermark is encrypted using the Arnold transforms. Finally, both DCT coefficients and watermarks are processed using SVD for embedding. Experimental results show that the proposed scheme provides high image quality and strong robustness against various malicious attacks.

2. RELATED WORKS

2.1 Arnold transformation algorithm

The Arnold transformation, first introduced by Arnold and Avez [25], is known as Arnold's cat map. In this transformation, the pixels of the input image are mapped to new positions to generate chaotic images using (1). As a result, without the key, attackers find it difficult to reconstruct the original image.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \pmod{n} \quad (1)$$

Here, x_i and y_i is the pixel coordinates at the i^{th} iteration, while x_{i+1} and y_{i+1} are the updated coordinates at the $(i+1)^{th}$ iteration. The term $n \times n$ is the image size, and a and b are control parameters that regulate the mapping process.

2.2. Discrete wavelet transform

The DWT is one of the well-known transform techniques in processing signals and compressing images. In two-level DWT, an original image I is transformed twice, as shown in Figure 1. First, the image I is processed to create four sub-bands (LL , LH , HL , and HH). In this algorithm, the sub-band LL is used to present the coarse-scale DWT coefficients, and the remaining three sub-bands are used to present the fine-scale DWT coefficients. An example of the two-level DWT transform technique is shown in Figure 1.

2.3. Discrete cosine transform

The DCT, a mathematical algorithm, is utilized to convert an image into the frequency domain. For an original image of size $n \times n$, the corresponding DCT coefficients are computed using (2) and (3).

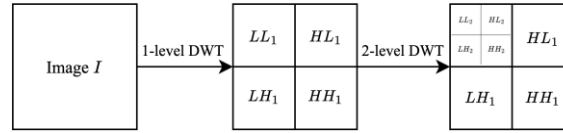


Figure 1. An example of a two-level DWT transform

$$G(p, q) = \frac{2}{n} K(p) K(q) \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} g(i, j) \cos\left(\frac{(2i+1)p\pi}{2n}\right) \cos\left(\frac{(2j+1)q\pi}{2n}\right) \quad (2)$$

$$\text{where, } K(t) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } t = 0 \\ 1, & \text{otherwise} \end{cases} \quad (3)$$

Here, the function $g(i, j)$ represents the pixel value at the spatial coordinate (i, j) in the input image, while $G(p, q)$ denotes the DCT coefficient at the frequency coordinate (p, q) in the DCT coefficient matrix.

2.4. Singular value decomposition

The SVD transform is widely employed in data science and image processing to decompose an image into three matrices. The decomposition is expressed in (4).

$$M = U \cdot S \cdot V^T \quad (4)$$

where M represents the input image, U and V are orthogonal matrices, S is the non-negative diagonal matrix, and V^T represents the transpose of V .

3. PROPOSED SCHEME

This section introduces a hybrid watermarking scheme to address two challenges of telemedicine security, i.e., authenticating the copyright of medical images and protecting the privacy of EPRs. The proposed scheme embeds two watermarks into a cover medical image. The first watermark (W_1), a binary logo image, is solely used to verify image copyright. Its primary goal is to recover the logo successfully rather than to conceal secret data. Consequently, for simplicity, the logo watermark is not encrypted. The second watermark, the *EPR*, is an image containing the patient's private information. It is used to protect patient privacy and is scrambled using the Arnold transform to enhance security. In the proposed scheme, the cover image is implemented using a combination of DWT, DCT, and SVD to select suitable coefficients for embedding both watermarks. The overall framework is partitioned into two main phases, namely the embedding phase and the extracting phase, which are illustrated in Figures 2 and 3, respectively. The detailed procedures of each phase are presented in the following subsections.

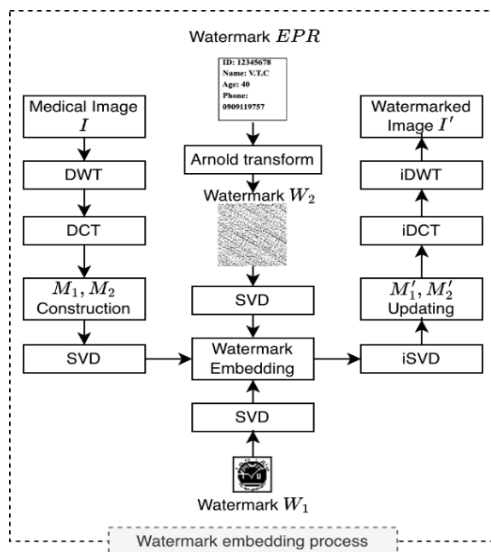


Figure 2. Flowchart of the embedding process

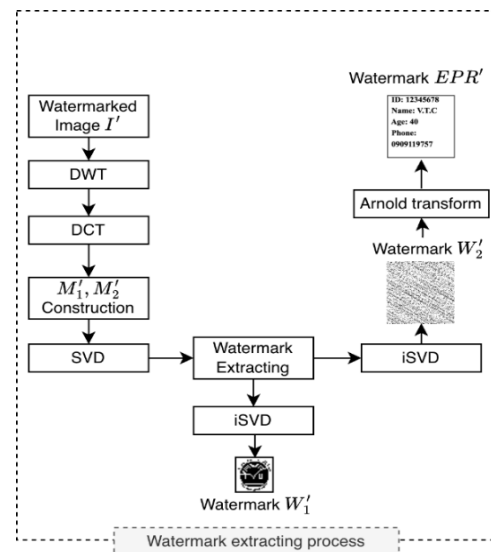


Figure 3. Flowchart of the extraction process

3.1. The procedure in the embedding phase

The watermarks embedding process begin by applying a two-level DWT to the cover image to decompose it into multiple frequency sub-bands. Specific sub-bands are then divided into blocks and further transformed using the DCT transformation. Key DCT coefficients are selected to construct two matrices M_1 and M_2 . The matrix M_1 is used to conceal the first watermark W_1 , a copyright logo of size 32×32 pixels, while the matrix M_2 is used to conceal the second watermark EPR , which is an image containing patients' identification information of size 128×128 pixels. To enhance security for patients, the watermark EPR is scrambled using the Arnold transform to generate W_2 . Then, SVD is applied to both the matrices and the watermarks. The singular values of the watermarks are embedded into the corresponding singular values of the matrices, scaled by a strength factor α . Finally, inverse SVD, DCT, and DWT are performed to reconstruct the watermarked image. The pseudocode for the watermark embedding process is summarized in Algorithm 1.

Algorithm 1. Watermark embedding

Input: Cover image I , watermark W_1 , watermark EPR

Output: Watermarked image I^*

Initialize matrices:

M_1 is matrix of size 32×32

M_2 is matrix of size 128×128

```

1. Begin
2.   $[[LL]_1, [HL]_1, [LH]_1, [HH]_1] \leftarrow \text{dwt2}(I, \text{'Haar'})$ 
3.   $[[LL]_{2HL1}, [HL]_{2HL1}, [LH]_{2HL1}, [HH]_{2HL1}] \leftarrow \text{dwt2}([HL]_1, \text{'Haar'})$ 
4.   $[[LL]_{2LH1}, [HL]_{2LH1}, [LH]_{2LH1}, [HH]_{2LH1}] \leftarrow \text{dwt2}([LH]_1, \text{'Haar'})$ 
5.   $[[LL]_{2HH1}, [HL]_{2HH1}, [LH]_{2HH1}, [HH]_{2HH1}] \leftarrow \text{dwt2}([HH]_1, \text{'Haar'})$ 
6.   $\{512 \text{ blocks } A \text{ of size } 8 \times 8\} \leftarrow ([\text{form}] \text{ } [HH]_{2HL1}, [HH]_{2LH1})$ 
7.  for  $i \leftarrow 1$  to 512 do
8.     $A_i \leftarrow \text{dct2}(A_i)$ 
9.     $M_1 \leftarrow ([\text{form}] \text{ } A_{(i(2,5))})^* A_{(i(3,4))}^*$ 
10.  end
11.  $\{2048 \text{ blocks } B \text{ of size } 4 \times 4\} \leftarrow ([\text{form}] \text{ } [HL]_{2HH1}, [LH]_{2HH1})$ 
12.  for  $i \leftarrow 1$  to 2048 do
13.     $B_i \leftarrow \text{dct2}(B_i)$ 
14.     $M_2 \leftarrow ([\text{form}] \text{ } [B]_{(i(1,2))})^* B_{(i(2,1))}^* B_{(i(3,1))}^* B_{(i(2,2))}^* B_{(i(1,3))}^* B_{(i(1,4))}^* B_{(i(2,3))}^* B_{(i(3,2))}^*$ 
15.  end
16.  $W_2 \leftarrow \text{Arnold}(EPR)$ 
17.  $[[U]_1, S_1, V_1] \leftarrow \text{svd}(M_1)$ 
18.  $[[U]_{W1}, S_{W1}, V_{W1}] \leftarrow \text{svd}(W_1)$ 
19.  $[[U]_2, S_2, V_2] \leftarrow \text{svd}(M_2)$ 
20.  $[[U]_{W2}, S_{W2}, V_{W2}] \leftarrow \text{svd}(W_2)$ 
21.  $S_1 \leftarrow S_1 + \alpha \cdot S_{W1}$ 
22.  $S_2 \leftarrow S_2 + \alpha \cdot S_{W2}$ 
23.  $M_1 \leftarrow U_1 \cdot S_1 \cdot V_1^T$ 
24.  $M_2 \leftarrow U_2 \cdot S_2 \cdot V_2^T$ 
25. for  $i \leftarrow 1$  to 512 do
26.   $[[A]_{(i(2,5))}, A_{(i(3,4))}] \leftarrow \text{update } M_1^*$ 
27.   $A_i \leftarrow \text{idct2}(A_i)$ 
28. end
29. for  $i \leftarrow 1$  to 2048 do
30.   $[B]$ 
31.   $_{(i(1,2))}, B_{(i(2,1))}, B_{(i(3,1))}, B_{(i(2,2))}, B_{(i(1,3))}, B_{(i(1,4))}, B_{(i(2,3))}, B_{(i(3,2))}] \leftarrow \text{update } M_2^*$ 
32.   $B_i \leftarrow \text{idct2}(B_i)$ 
33. end
33.  $[HH']_{2HL1}, [HH']_{2LH1} \leftarrow [A]_i^*$ 
34.  $[HL']_{2HH1}, [LH']_{2HH1} \leftarrow [B]_i^*$ 
35.  $[[HL]_1 \leftarrow \text{idwt2}([LL]_{2HL1}, [HL]_{2HL1}, [LH]_{2HL1}, [HH]_{2HL1}^*, \text{'Haar'})$ 
36.  $[[LH]_1 \leftarrow \text{idwt2}([LL]_{2LH1}, [HL]_{2LH1}, [LH]_{2LH1}, [HH]_{2LH1}^*, \text{'Haar'})$ 
37.  $[[HH]_1 \leftarrow \text{idwt2}([LL]_{2HH1}, [HL]_{2HH1}^*, [LH]_{2HH1}^*, [HH]_{2HH1}, \text{'Haar'})$ 
38.  $I^* \leftarrow \text{idwt2}([LL]_1, [HL]_1^*, [LH]_1^*, [HH]_1^*, \text{'Haar'})$ 
39. return  $I^*$ 
40. End

```


where $m \times n$ represents the size of the image. $I_{i,j}$ and $I'_{i,j}$ denote pixel values before and after embedding the watermarks, respectively.

In addition, the normalized cross correlation (NCC) value is utilized to evaluate the similarity of the extracted watermark and the embedded watermark. By using NCC value, defined by (7), the robustness of the watermarking schemes is estimated under various malicious attacks.

$$NCC = \frac{\sum_{i=1}^m \sum_{j=1}^n W_{i,j} \cdot W'_{i,j}}{\sum_{i=1}^m \sum_{j=1}^n W_{i,j} \cdot W_{i,j}} \quad (7)$$

where W and W' denote the embedded and the extracted watermarks, respectively. The pair (i, j) represents the coordinate of pixel located at the i^{th} row and j^{th} column of the embedded or extracted watermark.

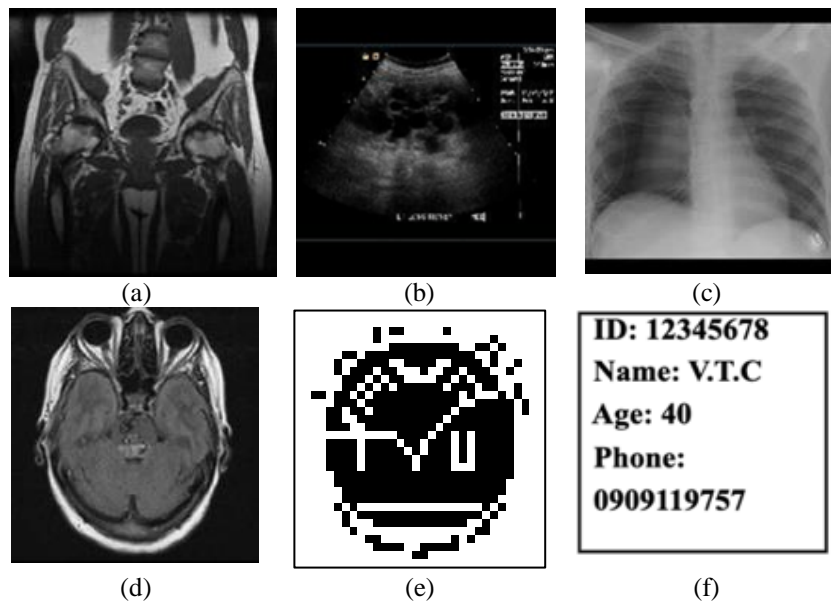


Figure 2. Samples of cover images: (a) MRIs, (b) ultrasounds, (c) X-rays, (d) CT scans, (e) watermark W_1 , and (f) watermark EPR

Based on the evaluation of the gain factor (α), $\alpha = 0.4$ was selected for the experiments, as it provides an optimal balance between quality image and robustness. Table 1 presents the performance metrics (PSNR and NCC) for different types of medical images without any attacks. Notably, for all image types, the proposed scheme achieves high PSNR values, consistently exceeding 68.3 dB. This indicates that the watermarked images exhibit minimal distortion compared to their original counterparts. One of the main reasons is that the proposed scheme selects DCT coefficient candidates from the mid-frequency region. Moreover, during the embedding process, only minimal changes are made to these coefficients to preserve image quality. Furthermore, the NCC values obtained for all medical image types remain at 1.00, demonstrating a strong similarity between the embedded and extracted watermarks.

Table 1. The proposed scheme's performance with $\alpha = 0.4$

Medical image	PSNR (dB)	NCC	
		W_1	EPR
CT scans	68.35	1.00	1.00
MRIs	68.35	1.00	1.00
Ultrasounds	68.35	1.00	1.00
X-Rays	68.35	1.00	1.00

To illustrate the distortion reduction achieved by the proposed scheme, Figure 5 presents a visual comparison between the original and watermarked medical images. Specifically, Figures 5(a)-(d) show the original MRI, ultrasound, X-ray, and CT scan images, respectively. Figures 5(e)-(h) display the

corresponding watermarked versions produced by the proposed scheme. As observed, no noticeable visual differences can be detected between each pair of original and watermarked images, demonstrating the imperceptibility and robustness of the embedding process.

To prove the performance, the proposed scheme is also compared with four existing schemes, including Anjum *et al.* [1], Anand and Singh [15], Thakur *et al.* [16], and Swaraja [20]. Table 2 shows that the PSNR and the NCC values obtained by the proposed scheme surpass those of the four existing schemes. For a fair comparison, the optimal results of each scheme were selected while the gain factor α is set to 0.4 in the proposed scheme. It is obvious that in Table 2, the proposed scheme is superior to the other four schemes in terms of the PSNR and the NCC values.

To assess the effectiveness of authenticating medical image copyright and protecting electronic patient information, the robustness of the proposed scheme is evaluated under various attack scenarios using MRI images. Tables 3 and 4 indicate that the NCC values of the proposed scheme are close to 1.00 for most attacks, indicating strong similarity between the extracted and original watermark. Although the NCC is acceptable under most of the evaluated attacks, the proposed scheme offers a low NCC value in the cropping attacks. However, all NCC values remain above 0.83, demonstrating good robustness.

Table 5 provides a comparative assessment between the proposed scheme Anand and Singh [15]. Various attacks were conducted in the experiment. It is noticeable that the proposed scheme achieves greater robustness compared to [15]. in most of the test attacks. Using the combination of the DWT, DCT, and SVD mechanisms, the proposed scheme carefully selected the suitable sub-bands in each transform domain for watermark embedding. As a result, the proposed scheme achieves stronger robustness against most of the various attacks. Moreover, by determining the optimal gain factor α for embedding data, it ensures a high balance between robustness and imperceptibility in the proposed scheme.

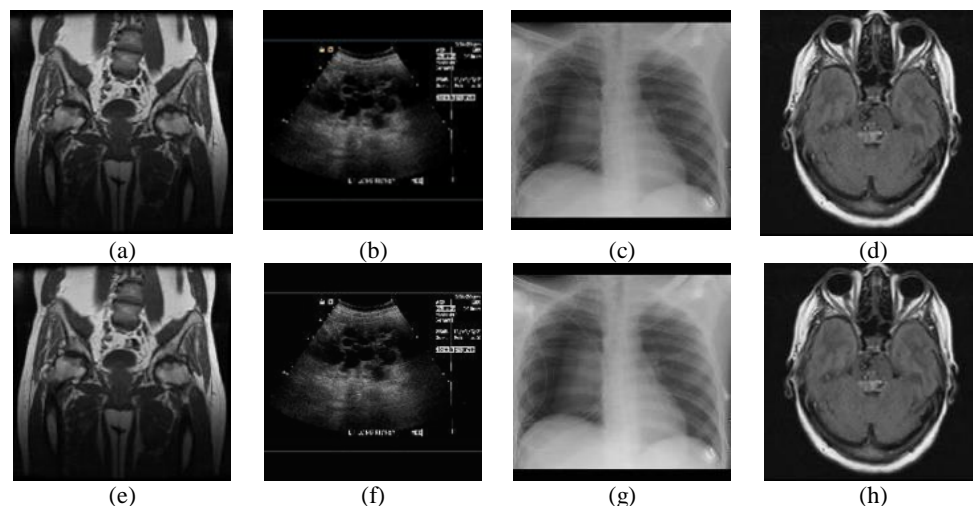


Figure 5. Visual comparison between the original and watermarked images: (a)-(d) the original images and (e)-(h) the corresponding watermarked images

Table 2. The PSNR (in dB) and NCC of five schemes without attacks on the MRI image

Method	Anjum <i>et al.</i> [1]	Anand and Singh [15]	Thakur <i>et al.</i> [16]	Swaraja [20]	Proposed
PSNR	55.49	46.98	54.49	56.23	68.35
NCC	0.98	1.00	1.00	1.00	1.00

Table 3. Robustness of the proposed scheme under different attacks

Attacks	NCC		Attacks	NCC	
	W_1	EPR		W_1	EPR
Salt and pepper noise (density = 0.001)	0.9922	0.9941	Image rotation (100)	0.8701	0.9971
Salt and pepper noise (density = 0.005)	0.9951	1.0000	Center cropping (50%)	0.8896	0.9440
JPEG compression (quality factor = 100)	0.9990	1.0000	Center cropping (75%)	0.9902	0.8716
Gaussian noise (variance = 0.05)	0.9951	1.0000	Average filtering (3×3)	1.0000	0.9396
Gaussian noise (variance = 0.10)	0.9961	1.0000	Average filtering (5×5)	1.0000	0.9396
Gaussian noise (variance = 0.20)	0.9912	1.0000	Brightness adjustment (+50)	1.0000	1.0000
Image rotation (5°)	0.9063	0.9513	Contrast enhancement (factor = 1.20)	0.9443	1.0000

Table 4. NCC performance of the extracted watermark for hybrid attacks

Attacks	NCC	
	W_1	EPR
Gaussian filtering (3×3 , 0.01) + Median filtering (3×3)	0.9736	1.0000
Gaussian filtering (3×3 , 0.01) + Average filtering (3×3)	1.0000	0.9368
Salt and pepper noise (density = 0.01) + Average filtering (3×3)	1.0000	0.9377
Scaling (factor = 0.5 + JPEG compression (quality factor = 50)	1.0000	0.8275

Table 5. Robustness comparison between our scheme Anand and Singh's scheme [15]

Attacks	Anand and Singh [15]	Proposed scheme
Salt and pepper noise (density = 0.0001)	1.0000	0.9922
Salt and pepper noise (density = 0.0005)	0.9491	0.9932
Salt and pepper noise (density = 0.001)	0.8831	0.9707
Gaussian noise (variance = 0.0001)	0.9732	0.9473
Gaussian noise (variance = 0.0005)	0.8459	0.9775
Image rotation (1°)	0.5587	0.8701
JPEG compression (quality factor = 10)	0.4051	0.9883
JPEG compression (quality factor = 50)	0.8503	0.9385
JPEG compression (quality factor = 90)	0.9999	0.9629
Speckle noise (variance = 0.001)	0.9823	0.9951
Speckle noise (variance = 0.005)	0.8797	0.9980
Cropping [20 20 400 480]	0.5159	0.7919
Median filtering [1 1]	1.0000	0.9932
Histogram equalization	0.9873	0.9443

In the frequency domain, the low frequency sub-band LL contains global image information, enabling watermark recovery even after cropping. However, modifying LL significantly distorts the marked image. In contrast, middle and high frequency sub-bands HL , LH , and HH capture localized details like edges and textures, making them more sensitive to regional changes, such as cropping. To maintain image quality, the proposed scheme uses middle and high frequency sub-bands HL_1 , LH_1 , and HH_1 from the first level DWT. For embedding the first watermark (W_1), further DWT is applied to HL_1 and LH_1 to select the second-level high frequency sub-band HH_{2HL_1} and HH_{2LH_1} , respectively. Similarly, DWT is applied to HH_1 to identify second-level middle frequency sub-bands HL_{2HH_1} and LH_{2HH_1} for embedding the second watermark (EPR).

Cropping attacks physically remove parts of the image, including high-frequency details in the affected regions. When the watermark is hidden in these regions, the corresponding portion of the watermark will be permanently lost, leading to incomplete watermark recovery. Cropping is among the most challenging attacks for watermarking algorithms, and the proposed method is no exception. However, by using optimal coefficients in middle and high frequency sub-bands, the proposed scheme balances image quality and robustness.

Although the proposed scheme is less robust against cropping attacks compared to other types of attacks, it outperforms the previous method [15], achieving an NCC of 0.7919 compared to 0.5159, as shown in Table 5. Additionally, the proposed scheme demonstrates superior image quality as illustrated in Table 2, achieving 68.35 dB compared to 55.49 dB, 46.98 dB, 54.49 dB, and 56.23 dB achieved by the methods of [1], [15], [16], [20], respectively. To enhance robustness against cropping attacks, watermarking schemes may need to sacrifice image quality by embedding in LL or using redundant embedding across multiple sub-bands.

5. CONCLUSION

In this paper, a novel hybrid scheme based on DWT-DCT-SVD combined with the Arnold transform is proposed for embedding two distinct watermarks. The first watermark is a logo image, while the second contains the private EPR information. To enhance robustness, the proposed scheme selects optimal coefficients from the DWT, DCT, and SVD domains for watermark embedding. Furthermore, to increase the security, the Arnold transform is applied to encode the EPR watermark before embedding. To ensure the balance between robustness and imperceptibility, DCT coefficients located in the mid-frequency region are carefully selected, and the optimal gain factor is determined during the embedding phase. Experimental results demonstrate that the proposed method achieves high-quality watermarked images and strong robustness against several malicious attacks. In future work, we aim to extend the approach to color images and explore the integration of advanced algorithms, such as deep learning, to further enhance watermarking security.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Van-Thanh Huynh	✓	✓	✓	✓	✓			✓	✓		✓			✓
Thai-Son Nguyen	✓	✓		✓		✓	✓			✓		✓	✓	
Thanh-C Vo		✓	✓	✓		✓			✓		✓			

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

Data availability does not apply to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] R. Anjum, P. Verma, and S. Verma, "Multiple image watermarking for efficient storage and transmission of medical images," in *Advances in Computing and Data Sciences*, pp. 92–102, 2019, doi: 10.1007/978-981-13-9942-8_9.
- [2] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, Eds., *Medical Image Watermarking*. Cham: Springer International Publishing, 2017, doi: 10.1007/978-3-319-57699-2.
- [3] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an ehealth arrangement," *IEEE Access*, vol. 7, pp. 69758–69775, 2019, doi: 10.1109/ACCESS.2019.2919381.
- [4] K. Annadurai and S. Rani, "Two level security for medical images using watermarking/encryption algorithms," *International Journal of Imaging Systems and Technology*, vol. 24, Mar. 2014, doi: 10.1002/ima.22086.
- [5] F. Y. Shih and X. Zhong, "High-capacity multiple regions of interest watermarking for medical images," *Information Sciences*, vol. 367–368, pp. 648–659, Nov. 2016, doi: 10.1016/j.ins.2016.07.015.
- [6] D. Awasthi, A. Tiwari, P. Khare, and V. K. Srivastava, "A comprehensive review on optimization-based image watermarking techniques for copyright protection," *Expert Systems with Applications*, vol. 242, p. 122830, May 2024, doi: 10.1016/j.eswa.2023.122830.
- [7] A. Bamatraf, R. Ibrahim, and Mohd. N. B. M. Salleh, "Digital watermarking algorithm using LSB," in *2010 International Conference on Computer Applications and Industrial Electronics*, Dec. 2010, pp. 155–159, doi: 10.1109/ICCAIE.2010.5735066.
- [8] S. D. Muyco and A. A. Hernandez, "Least significant bit hash algorithm for digital image watermarking authentication," in *Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence*, in ICCAI '19. New York, NY, USA: Association for Computing Machinery, Apr. 2019, pp. 150–154, doi: 10.1145/3330482.3330523.
- [9] A. Boonyapalanant, M. Ketcham, and M. Piyaneeanart, "Hiding patient injury information in medical images with QR code," in *Recent Advances in Information and Communication Technology 2019*, P. Boonyopakorn, P. Meesad, S. Sodsee, and H. Unger, Eds., in *Advances in Intelligent Systems and Computing*. Cham: Springer International Publishing, 2020, pp. 258–267, doi: 10.1007/978-3-030-19861-9_25.
- [10] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the smart healthcare system using steganography and chaotic functions based on DNA," *Security and Privacy*, vol. 7, no. 3, p. e363, May 2024, doi: 10.1002/spy2.363.
- [11] Q. Dai, J. Li, U. A. Bhatti, Y.-W. Chen, and J. Liu, "SWT-DCT-based robust watermarking for medical image," in *Innovation in Medicine and Healthcare Systems, and Multimedia*, Y.-W. Chen, A. Zimmermann, R. J. Howlett, and L. C. Jain, Eds., Singapore: Springer, 2019, pp. 93–103, doi: 10.1007/978-981-13-8566-7_9.
- [12] S. Kumar, A. Rajpal, N. K. Sharma, S. Rajpal, A. Nayyar, and N. Kumar, "ROSEmark: Robust semi-blind ECG watermarking scheme using SWT-DCT framework," *Digital Signal Processing*, vol. 129, p. 103648, Sept. 2022, doi: 10.1016/j.dsp.2022.103648.
- [13] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669–3697, Feb. 2017, doi: 10.1007/s11042-016-3928-7.
- [14] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Generation Computer Systems*, vol. 101, pp. 1223–1246, Dec. 2019, doi: 10.1016/j.future.2019.07.064.




- [15] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, Feb. 2020, doi: 10.1016/j.comcom.2020.01.038.
- [16] S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools and Applications*, vol. 79, no. 7, pp. 4263–4276, Feb. 2020, doi: 10.1007/s11042-018-6691-0.
- [17] S. A. Hosseini and P. Farahmand, "An attack resistant hybrid blind image watermarking scheme based on combination of DWT, DCT and PCA," *Multimedia Tools and Applications*, vol. 83, no. 7, pp. 18829–18852, Feb. 2024, doi: 10.1007/s11042-023-16202-2.
- [18] A. Tiwari, D. Awasthi, and V. K. Srivastava, "Image security enhancement to medical images by RDWT-DCT-Schur decomposition-based watermarking and its authentication using BRISK features," *Multimedia Tools and Applications*, vol. 83, no. 22, pp. 61883–61912, July 2024, doi: 10.1007/s11042-023-15878-w.
- [19] D. S. Chauhan, A. K. Singh, B. Kumar, and J. P. Saini, "Quantization based multiple medical information watermarking for secure e-health," *Multimed. Tools Appl.*, vol. 78, no. 4, pp. 3911–3923, Feb. 2019, doi: 10.1007/s11042-017-4886-4.
- [20] K. Swaraja, "Medical image region based watermarking for secured telemedicine," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28249–28280, Nov. 2018, doi: 10.1007/s11042-018-6020-7.
- [21] G. Azizoglu and A. N. Toprak, "A novel reversible fragile watermarking method in DWT domain for tamper localization and digital image authentication," *Biomedical Signal Processing and Control*, vol. 84, p. 105015, July 2023, doi: 10.1016/j.bspc.2023.105015.
- [22] S. Sharma, J. J. Zou, G. Fang, P. Shukla, and W. Cai, "A review of image watermarking for identity protection and verification," *Multimed Tools Appl.*, Sept. 2023, doi: 10.1007/s11042-023-16843-3.
- [23] S. Sharma, S. Shivani, and N. Saxena, "An efficient fragile watermarking scheme for tamper localization in satellite images," *Computers and Electrical Engineering*, vol. 109, p. 108783, Aug. 2023, doi: 10.1016/j.compeleceng.2023.108783.
- [24] P. Aberna and L. Agilandeswari, "Optimal semi-fragile watermarking based on maximum entropy random walk and swin transformer for tamper localization," *IEEE Access*, vol. 12, pp. 37757–37781, 2024, doi: 10.1109/ACCESS.2024.3370411.
- [25] V. I. Arnol'd and A. Avez, *Ergodic Problems of Classical Mechanics*. Addison-Wesley, 1989.

BIOGRAPHIES OF AUTHORS






Van-Thanh Huynh    received a bachelor's degree in information technology from Can Tho University, Can Tho City, Vietnam, in 2005. From December 2005, he has been a lecturer at Tra Vinh University, Tra Vinh, Vietnam. In 2017, he received the M.S. degree in information technology from the Department of Information Science and Engineering, Information Technology University, Ho Chi Minh City, Vietnam. He is currently working toward a Ph.D. degree in information technology at Tra Vinh University, Vietnam. His current research interests include watermarking, steganography, image processing, information security, and computer networking. He can be contacted at email: hvthanh@tvu.edu.vn.



Thai-Son Nguyen    received the M.S. and Ph.D. degrees from Feng Chia University, Taichung, Taiwan, in 2011 and 2015, respectively, all in computer science. He has served as a lecturer at Tra Vinh University, Vietnam, since 2006. From 2019, he was Dean of the School of Engineering and Technology, Tra Vinh University. He is currently an Associate professor. His research interests include image processing, information hiding, image recognition, information security, IoT, and artificial intelligence applications. Dr. Son has served as a member of the Editorial Board for the Scientific Journal of Tra Vinh University and the Journal of Science, Engineering and Technology. He can be contacted at email: thaison@tvu.edu.vn.



Thanh-C Vo    was received the bachelor's degree in information technology from the University of Science, Ho Chi Minh City, Vietnam, in 2003 and the M.S. degree in Information Systems from Can Tho University, Can Tho City, Vietnam, in 2016. He is currently a PhD student. He has worked as a lecturer in the School of Engineering and Technology, Tra Vinh University since 2008. His areas of interest include data hiding, information security, and image and signal processing. He can be contacted at email: vothanhc@tvu.edu.vn.