Implementation of an Efficient Secure Hybrid Reversible Tampering Detection Method in Medical Image

Souad Bekkouche, and Abdelaziz Tami

Original scientific article

***Abstract*—Medical image watermarking has gained significant attention in recent years as a critical tool for data security. Given that even minor distortions can compromise diagnostic accuracy and lead to misinterpretation, reversibility is paramount in medical imagery. This research introduces a sophisticated hybrid reversible watermarking architecture operating within the frequency domain. By leveraging the combined strengths of Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD), the system achieves an optimal balance between payload capacity, imperceptibility, and robustness. The proposed method generates the watermark directly from the host image's own features to enable self-embedding, ensuring highly accurate blind tamper detection and integrity verification without requiring the original image. To address security and authentication concerns, a dual-watermarking strategy is implemented. A reversible watermark (W_1), generated through the RLSB method, is embedded into the LL coefficients to preserve diagnostic integrity, while a secondary biometric logo (W_2) is integrated into the HH coefficients to facilitate authentication and confidentiality. Experimental results demonstrate high robustness against common signal processing attacks, while comparative analysis using AI-driven classification features confirms the superior performance of the proposed approach over existing methods.**

***Index Terms*—Combined watermark, *Multi-layered,* Frequency domain, Security medical data.**

I. Introduction

With today's development of digital networks and the rapid evolution of digital technology for the transmission and distribution of different types of data, such as texts, videos, audios, and images, the need for efficient techniques to protect the data against illegal recording and distribution becomes more and more important. Such kinds of data types can be subject to illegal distribution, duplication, and modification by intruders and non-authorized customers and require specific securing mechanisms in order to ensure legal uses and distribution processes. The watermarking concept [1] has emerged as one of the methods to protect copyright and ensure the security of multimedia based on embedding information (watermark) into the image, video, or audio. This watermark must be invisible and robust against any type of multimedia signal processing.

In the field of health, telemedicine takes a very important role in medical applications, where the problem is situated in the transmission of medical data and images via the Internet, where the appearance of the watermarking is very important in order to secure medical images shared via networks while maintaining their integrity and authentication [2]. The distortion generated after watermarking technology in medical imaging is undesirable, which can affect the diagnostic decision of the specialist; for this reason, the watermarking needs to satisfy the reversibility constraints. The idea of the reversible watermarking technique proposed by [3] is characterized by the ability to restore the original data from the watermarked one using a secret key. In contrast, the irreversible one cannot restore the original from the watermarked one [3, 4]. Several techniques have been proposed in the literature [5, 6], and in medical imaging there is some existing work of reversible watermarking applied on medical images [7, 8].

Watermarking can be classified into categories according to the embedding domain: spatial domain and transform domain. Insertion in the spatial domain is based on embedding the watermark directly in the cover image by modifying the pixel value [1, 9]. On the other hand, the embedding process in the transform domain is not directly in the cover image but in the coefficients transform [10] of this one, which is obtained. The aim of this paper is to present a new watermarking approach to ensure the three properties of security based on embedding the watermark W_3 generated by two watermarks (W_1 and W_2). W_1 is used to ensure authentication and integrity when watermark W_2 is used to verify the confidentiality properties.

The main contributions of this research work to solving the problems of the image processing field are as follows:

- Novel Hybrid Frequency-Domain Approach: The integration of DWT, DCT, and SVD transforms provides a multi-layered embedding scheme that significantly enhances both transparency and robustness compared to single-transform methods.
- Self-Generated Watermarking for Blind Tamper Detection: A key contribution is the generation of authentication data directly from the image content itself. This enables blind tamper detection, allowing for integrity verification without requiring the original host image.

Manuscript received March 16, 2026; revised May 22, 2026. Date of publication October 26, 2026. Date of current version October 26, 2026.

Authors are with the Université Dr Tahar Moulay de Saïda, Saïda Province, Algeria (e-mails: {sbekkouche2015, abaziz.tami}@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0282

- Data Security and Reversibility for Medical Applications: The method ensures a triple security layer (integrity, authentication, and confidentiality) while maintaining full reversibility. This is critical in medical imaging to prevent diagnostic errors caused by irreversible distortions.
- AI-Driven Performance Evaluation: The use of Artificial Intelligence (AI) for feature extraction and classification provides a more rigorous and objective framework for evaluating integrity and performance medical image watermarking.

The remainder of the paper is organized as follows: Section II discusses related works. Section III presents the proposed technique. In section IV, the experimental results are presented, the performances of the proposed method are evaluated and compared to those of existing ones using the PSNR, the NCC coefficient of correlation between the original watermark and the extracted watermark, and the elapsed time. We evaluate the robustness of the proposed watermarking according to salt & pepper noise, Gaussian noise, and speckle noise attacks.

II. Literature Review

The transform domain obtained after the DCT is similar to the one obtained using discrete Fourier transform (DFT) and allows an image to be divided into different frequency bands: high, middle, and low frequency. The techniques based on DCT have the great advantage of robust compression operations with a reduced computation time. [11] applied the DCT on the host image among the low frequencies and modify the n coefficients of the highest amplitude of the transform; the original image is required to extract the watermark.

In medical imaging, [12] studied three different watermarking techniques: DWT, SVD, and DWT-SVD applied to medical images. The experimental results show that the DWT and SVD are more suitable for medical applications. [13] Applied SVD on different sub bands of a Haar wavelet-transformed medical image. Experimentation is performed using MRI and CT scan medical images.

In recent study, [14] demonstrates that this specific combination provides unparalleled protection for biometric authenticity and patient privacy. Their research demonstrates that this specific combination leverages DWT for spatial-frequency localization, while DCT and SVD provide the structural stability necessary to protect biometric authenticity against sophisticated geometric attacks, all while maintaining the high peak signal-to-noise ratio (PSNR) .

Authors in [15] represent a significant advancement in medical image security through a triple self-embedding fragile watermarking scheme**.** This method is specifically designed for telemedicine to ensure image integrity and enable high-quality recovery without the original reference. The method in [15] generate the watermark from the image itself to avoid needing the original for verification based on the constructing authentication data directly from host image features allows for blind tamper detection. This approach is crucial for telemedicine, as it enables the system to identify unauthorized modifications (tampering) and even recover original pixels without requiring the original reference image. The integration of Artificial Intelligence (AI) with hybrid DWT-DCT-SVD frameworks has set a new benchmark for securing medical imagery. In accordance with recent developments in 2024 regarding deep feature extraction, our method integrates AI-driven analysis with hybrid DWT-SVD transformations. This synergy ensures that the authentication process remains robust against sophisticated manipulations [16].

III. Proposed Technique

This section proposes a reversible watermarking technique that involves embedding two types of watermarks. A reversible watermark W_1 is obtained by RLSB method [17] inserted into a fingerprint user to obtain a final watermark that is embedded into the original image to obtain the watermarked one as shown in Fig. 1.

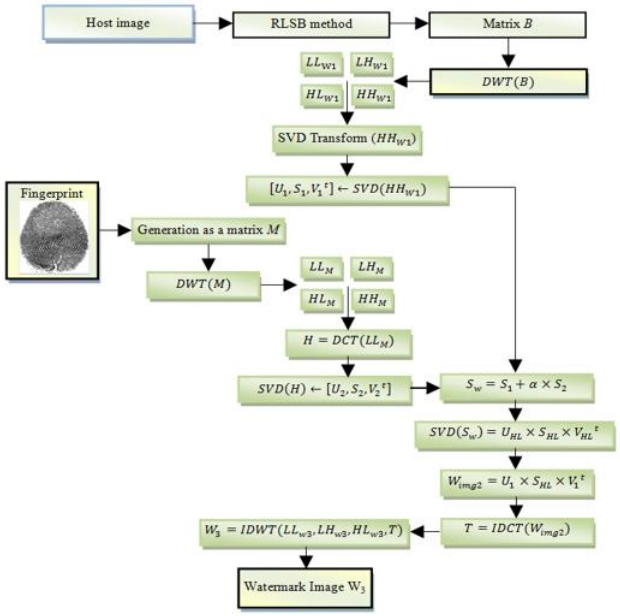


Fig.1. Generation of the watermark W_3.

A. Generation of the Watermarks W_1 and W_2

A reversible watermark W_1 is used to verify data authentication and integrity of the image generated by the RLSB method [17]. The result is a Matrix B. A second watermark W_2, used to check the confidentiality with a secret key and to verify the image's integrity. The watermark W_2 (fingerprint user) is a predefined as a matrix M. In order to generate the watermark W_3, the following algorithm is performed:

Algorithm 1

Inputs:

B: Matrix defining watermark (from RLSB method)

M: Matrix defining watermark W_2

α: Scaling factor.

Output: The final processed watermark to be inserted into the host image.

1. Apply DWT to matrix B:

$$LL_{W1}, LH_{W1}, HL_{W1}, HH_{W1} \leftarrow DWT(B)$$

2. Perform SVD on the high-frequency sub-band HH_{W1} to obtain its singular values:

$$[U_1, S_1, {V_1}^t] \leftarrow SVD(HH_{W1})$$

3. Apply DWT to matrix M defining W_2:

$$LL_M, LH_M, HL_M, HH_M \leftarrow DWT(M)$$

4. Apply the DCT transform on the sub-band LL_M to get:

$$H \leftarrow DCT(LL_M)$$

5. Perform SVD on the H to obtain its singular values:

$$[U_2, S_2, {V_2}^t] \leftarrow SVD(H)$$

6. Modify the singular values of W_1 by adding the scaled singular values of M:

$$S_W \leftarrow S_1 + (\alpha \times S_2)$$

7. Perform SVD on the matrix S_w:

$$[U_{HL}, S_{HL}, {V_{HL}}^t] \leftarrow SVD(S_W)$$

8. Construct the intermediate matrix:

$$Wimg2 \leftarrow U_1 \times S_{HL} \times {V_1}^t$$

9. Apply Inverse DCT (IDCT) to Wimg2 to obtain matrix T:

$$T \leftarrow IDCT(Wimg2)$$

10. Generate the final watermark W_3 by applying Inverse DWT (IDWT) using the original sub-bands and the modified matrix T:

$$W_3 \leftarrow IDWT(LL_{w3}, LH_{w3}, HL_{w3}, T)$$

B. Watermark Embedding Process

The watermark embedding process is performed detailed in the following algorithm. Fig. 3 gives a schematic representation of the enumerated steps. We present the process of embedding and extraction of the proposed approach with a complete diagram illustrated in Figs. 2 and 3.

Algorithm 2

Inputs:
- A: Matrix defining original image.
- W_3: watermark.
- α: Scaling factor.

Output: A_w.

1. Apply DWT to Host Image A:

$$(LL_A, HL_A, LH_A, HH_A) \leftarrow DWT(A)$$

2. Apply DCT to the high-frequency sub-band HH_A:

$$D \leftarrow DCT(HH_A)$$

3. Perform SVD on matrix to extract singular values:

$$[U_D, S_D, {V_D}^t] \leftarrow SVD(D)$$

4. Apply DWT to Watermark W3:

$$(LL_{W3}, HL_{W3}, LH_{W3}, HH_{W3}) \leftarrow DWT(W_3)$$

5. Apply DCT to the high-frequency sub-band HH_{W3}:

$$D1 \leftarrow DCT(HH_{W3})$$

6. Perform SVD on matrix D1:

$$[U_{D1}, S_{D1}, {V_{D1}}^t] \leftarrow SVD(D1)$$

7. Modify the singular values by adding the scaled host SVs to the watermark SVs:

$$IM \leftarrow S_{D1} + (\alpha \times S_D)$$

8. Perform SVD on the modified matrix IM:

$$[U_{IM}, S_{IM}, {V_{IM}}^t] \leftarrow SVD(IM)$$

9. Compute the watermarked transform matrix using the singular values from the previous step:

$$A_{W1} \leftarrow U_{D1} \times S_{IM} \times {V_{D1}}^t$$

10. Apply Inverse DCT (IDCT) to A_{W1}

$$IM_w \leftarrow IDCT(A_{W1})$$

11. Generate the final Watermarked Image by applying Inverse DWT to get A_w.

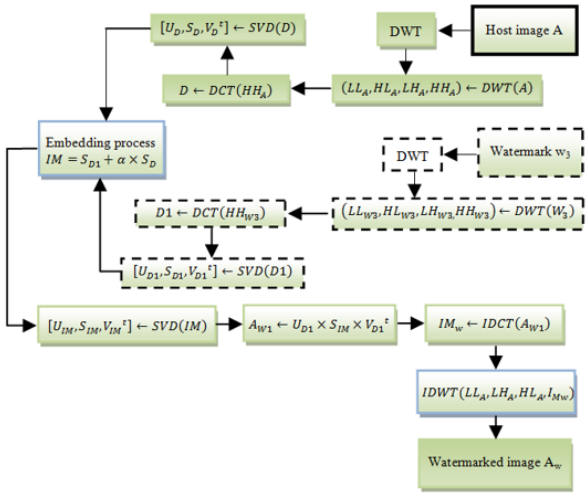


Fig. 2. Embedding process.

C. Watermark Extraction Process

The watermark extraction process is performed according to the algorithms detailed in the following, based on two extraction phases: extraction of W_3 and extraction of W_1. Fig.4 gives a schematic representation of the enumerated parts:

Part 1: Extraction of Watermark W_3*

Algorithm 3

Inputs:
- ${A_w}^*$: Watermarked image (possibly attacked)
- α_1: Scaling factors used during embedding
- U_{D1},V_{D1},S_D: Original SVD matrices from the embedding phase

U_1, $V1^t$, S_1: Original SVD matrices from the W_1.
LL_{w3}, HL_{w3}, H_{w3}: Original DWT coefficients of W_3.
Output:
W_3^*: Extracted primary watermark
W_1^*: Extracted secondary watermark

1. Apply DWT to the watermarked image A_W^*:

$$(LL_{AW}^*, HL_{AW}^*, LH_{AW}^*, HH_{AW}^*) \leftarrow DWT(\mathrm{A_W}^*)$$

2. Apply DCT to the high-frequency sub-band:

$$E \leftarrow DCT(HH_{AW}^*)$$

3. Perform SVD on matrix E:

$$[U_E^*, S_E^*, V_E^*] \leftarrow SVD(E)$$

4. Calculate matrix $F3$ using original $U_{D1}$and $V_{D1}{}^t$:

$$F_3 \leftarrow \left(U_{D1} \times S_E^* \times V_{D1}{}^t\right)$$

5. Isolate the corrupted singular values (S_r):

$$S_r \leftarrow (F_3 - S_D)/\alpha$$

6. Inverse DCT: Apply IDCT to the extracted singular values:

$$W_c \leftarrow IDCT(S_r)$$

7. Apply IDWT using original coefficients and Wc:

$$W_3^* \leftarrow IDWT(LL_{w3}, HL_{w3}, LH_{w3}, W_c)$$

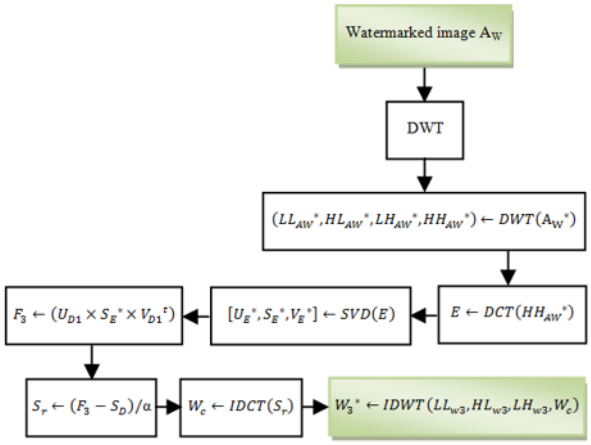


Fig. 3. Extraction process of W_3.

Part 2: Extraction of Watermark W_1*

Algorithm 4

Inputs:
W_3^*: Possibly attacked watermark image.
U_1, S_1, V_1: Original SVD components (pre-stored)
$LL_{W1}LH_{W1}HL_{W1}$: Original DWT approximation coefficients
α: Scaling factor
$LL_{W3}{}^*, HL_{W3}{}^*, LH_{W3}{}^*, HH_{W3}{}^*$: DWT sub-bands.
$U_{W3}{}^*, S_{W3}{}^*, V_{W3}{}^*$: SVD matrices of HH*$w3$
S_{r1}, F_2: Intermediate matrices.

Outputs: $W_1{}^*$: Extracted watermark

1. Decompose $W_3{}^*$ using Discrete Wavelet Transform (DWT):

$$LL_{W3}{}^*, HL_{W3}{}^*, LH_{W3}{}^*, HL_{W3}{}^* \leftarrow DWT(W_3{}^*)$$

2. Apply Singular Value Decomposition (SVD) on the $HH_{W3}{}^*$ sub-band.

$$U_{W3}{}^*, S_{W3}{}^*, V_{W3}{}^* \leftarrow SVD(HH_{W3}{}^*)$$

3. Compute the corrupted singular matrix $Sr1$:

$$S_{r1} \leftarrow (S_1 - S_{W3}{}^*)/\alpha$$

4. Reconstruct the matrix F_2 using original U_1, $V_1{}^t$ and extracted S_{r1}:

$$F_2 \leftarrow U_1 \times S_{r1} \times V_1{}^t$$

5. Obtain the extracted watermark W_1* by applying Inverse DWT (IDWT):

$$W_1{}^* \leftarrow IDWT(LL_{W1}, HL_{W1}, LH_{W1}, F_2).$$

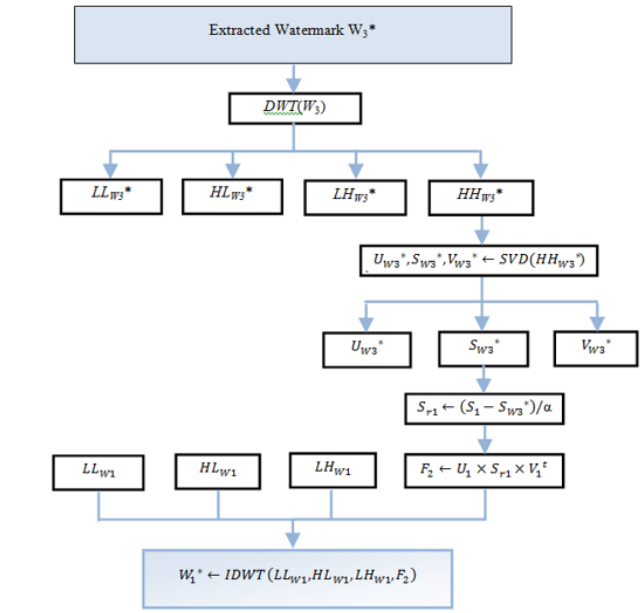
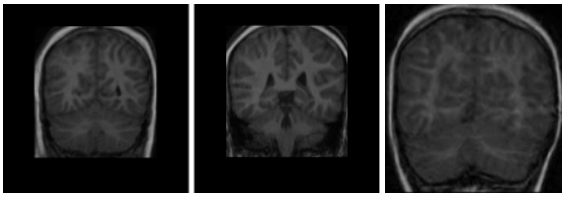


Fig. 4. Watermark W_1 extraction process.

IV. Results and Discussions

To evaluate the proposed method, we use three medical images, IRM_31, IRM_32, and IRM_33 of 256×256 grayscale (as shown in Fig .5). The original watermark image W_1 is sized 1×206, and the original watermark image W_2 is sized 106×143, the original fingerprint and the extracted one are shown in Fig. 6.a and Fig. 6.b.



(a) (b) (c)

Fig. 5. Original test image: IRM_1, (b) IRM_2, (c) IRM_3.



(a) (b)

Fig. 6. Original watermark: (a) original biometric watermark W, (b) obtained biometric watermark.

TABLE I
COMPARISON BETWEEN PROPOSED METHOD AND THE APPROACH [20]

Methods	Proposed method	Approach [20]
Type of applied transform of cover image	DWT, SVD, DCT, hash function	DWT, SVD
Type of applied transform of watermark	DWT, SVD	Chaotic map, SVD
Type of watermark	Use of two types of watermarks Reversible watermark W_1 and Watermark W_2 (user fingerprint) to obtain W_3	Watermark W_2 (fingerprint)
Size of watermark	Size of W_1=1×206 Size of W_2=124x137	124 ×137
Sub-bands Embedding	(LLC+HHW$_1$) & (HHC+HH W_1)	HHC+DCT (Watermark)
Security properties	Integrity, confidentiality and authentication	Integrity, confidentiality

TABLE II
COMPARISON BETWEEN PROPOSED METHOD AND THE APPROACH [20] FOR IRM_31, IRM_32 AND IRM_33 IN TERM OF PSNR, SSIM AND ELAPSED TIME.

IRM_31			
	PSNR	Elapsed time	SSIM
Proposed technique	55.69618403	13.4316861	0.9991437404
Approach [20]	22.50434730	12.0432772	0.2524972891
IRM_32			
Proposed technique	54.955426	13.2444849	0.9990466806
Approach [20]	23.0274	11.700075	0.2736581681
IRM_33			
Proposed technique	55.220450	14.8980955	0.9991113209
Approach [20]	22.0799	12.1212777	0.3960760597

To estimate the similarity between the original watermark and the extracted watermark using NC ('Normalized cross correlation') which is the quality of the extracted watermark between the watermark image and the extracted watermark image and also was used to measure the similarity between the original watermarks W and the extracted watermarks W', the bigger the values of the correlation coefficient [18], indicate the robustness of the watermark that is defined as below:

$$NCC = \frac{\sum_i \sum_j W(i,j), W^*(i,j)}{\sum_i \sum_j W(i,j)^2} \quad (1)$$

The watermark imperceptibility and the performance of methods are simulated via the Peak Signal to Noise Ratio (PSNR) and MSE [19] between the original image and the watermarked image, which are defined as below:

$$PSNR = 10.\log_{10} \frac{X \max^2}{MSE} = \frac{255^2}{MSE} \quad (2)$$

$$MSE = \frac{1}{MN} \sum_i \sum_j (I(i,j) - I_w(i,j))^2 \quad (3)$$

where I (i, j) is the pixel values at the position (i, j) of the original image and I_w (i, j) is the pixel values at the position (i, j) of the watermarked or image, where M and N are the height and width of the image. I_w is the Original Image and I_w is the Watermarked Image and X is the peak signal value of the original image. Images having high PSNR value are preferable. For a good image the SNR value must be high. Table I shows the comparison between proposed technique and Method [20] in term of security type.

To evaluate the performance of our method in terms of imperceptibility and robustness, the experimental results are separated into two parts: the first is allowed to test the imperceptibility property, while the second is allowed to analyze the robustness against some types of standard and interesting attacks.

A. Imperceptibility Property

To evaluate the quality of our method, we estimate the PSNR between host images and watermarked ones. The PSNR difference between the original and watermarked images is displayed in Table II and Table III, along with a comparison to the approach [20]. Second, SSIM compares brightness, contrast, and structure to determine how similar two images are based on the visual properties of the human eye. The values range from 0 to 1, with 1 denoting that the two photos are identical. Equation (4) is used to express SSIM [21].

$$SSIM = \frac{(2\mu_A\mu_{AW}+C_1)(2\sigma_{AAW}+C_2)}{(\mu^2{}_A+\mu_{AW}{}^2+C_1)+(\sigma^2{}_A+\sigma^2{}_{AW}+C_2)} \quad (4)$$

For each of the test grayscale medical images IRM_31, IRM_32, and IRM_33, Table II and Table III display the PSNR that was achieved between the cover image and the watermarked image. The findings show that, in terms of PSNR, the watermarked image is imperceptible. The obtained watermarked image, which is identical to the cover image, is displayed in Fig. 7, and Fig. 8. It is evident that it is challenging to discern between the original and watermarked images. Thus, the imperceptibility or invisibility is confirmed.

In security and biometrics, FAR and FRR are the two key

metrics used to measure the accuracy and performance of an authentication system. Equations (5) and (6) are used to express FAR and FRR [24].

$$FAR = \frac{number\ of\ falseAcceptance}{Total\ number\ of\ impostors} \quad (5)$$

$$FRR = \frac{Number\ of\ False\ rejections}{Total\ number\ ogf\ Genuine\ Atempts} \quad (6)$$

TABLE III
COMPARISON RESULTS OF PROPOSED METHOD FOR DIFFERENT VALUE OF α

α	α= 0.02	α= 0.002	α= 0.0002
PSNR	51.247089933110	55.2204506584014	55.29603557250

Table III shows the PSNR obtained between the cover image and the watermarked image for all test grayscale images: medical images IRM_31, IRM_32, and IRM_33, respectively. Figs. 9 and 10 show the results which indicate that the imperceptibility of the watermarked image is good in terms of PSNR and SSIM. Figs. 7 and 8 show the obtained watermarked image, which is indistinguishable from the cover image, and we can see that it is difficult to differentiate between the original images and their watermarked images. So the invisibility or imperceptibility is verified.

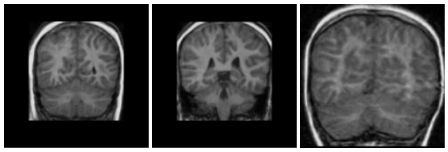


Fig. 7. Watermarked medical images that are shown in Fig. 5. of proposed technique.

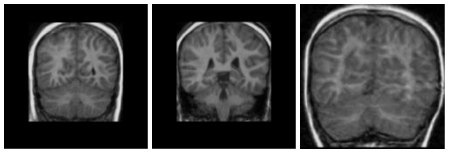


Fig. 8. Watermarked medical images that are shown in Fig. 5. of the approach [20].

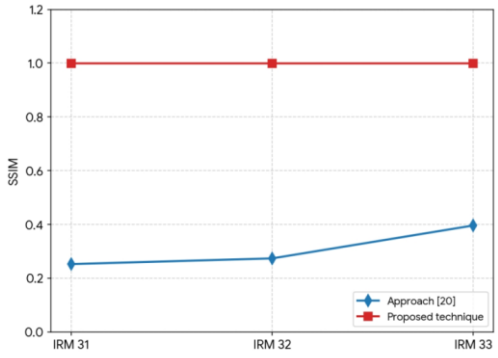


Fig. 9. Comparison between proposed method and the approach [20] for IRM_31, IRM_32 and IRM_33 in term SSIM.

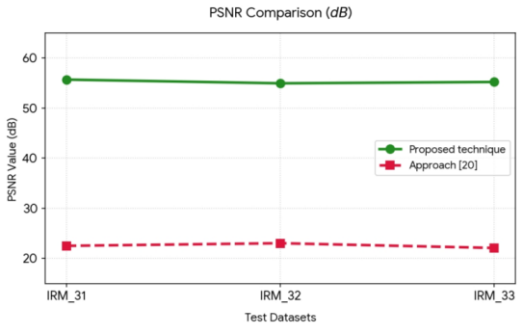


Fig. 10. Comparison between proposed method and the approach [20] for IRM_31, IRM_32 and IRM_33 in term PSNR.

TABLE IV
COMPARISON RESULTS OF PROPOSED METHOD FOR IRM_31, IRM_32 AND IRM_33 IN TERM OF NC

Proposed method			
Watermarked image	Type of attack	Nc_1(reversible watermark)	$N_{C3}(W_3)$
IRM_31	Salt & Pepper noise	0.9998620811498	0.978735265384
	Gaussian	0.9996536586258	0.904637978206
	Speckle	0.9998620811498	0.966912142372
	Rotation(90°)	0.9999512213177	0.989741971703
	Rotation (120°)	0.9998620811498	0.959126795555
	Rotation(180°)	0.9999512213177	0.989741971703
IRM_32	Salt & Pepper noise	0.9999116156035	0.980804916398
	Gaussian	0.9996578101726	0.904398628631
	Speckle	0.9998637519698	0.975795972465
	Rotation(90°)	0.9999518120192	0.991186935021
	Rotation (120°)	0.9999116156035	0.977550122975
	Rotation(180°)	0.9999518120192	0.99118693502
IRM_33	Salt & Pepper noise	0.9999520379545	0.982453942242
	Gaussian	0.9996593984446	0.905762249255
	Speckle	0.9998643913408	0.974750342230
	Rotation(90°)	0.9999520379545	0.993012779880
	Rotation (120°)	0.9999520379545	0.981910521088
	Rotation(180°)	0.9999520379545	0.993012779880

TABLE V
PERFORMANCE COMPARISON METRICS (STANDARD DEVIATION, MEAN AND PSNR) FOR DIFFERENT TEST IMAGES BETWEEN THE PROPOSED METHOD AND APPROACH [20]

Proposed method			
Test Image	PSNR	Standard Deviation (σ)	Mean (μ)
Image_31	56.75	0.3708	0.0029
Image_32	55.9349	0.4072	0.0003
Image_33	55.91	0.4081	0.0043
Lena image	37.38	3.4496	0.0035
Approach [20]			
Image_31	24.67	14.8842	0.5952
Image_32	25.57	13.4195	0.6614
Image_33	23.31	17.3831	1.1040
Lena image	17.6177	33.4930	1.9097

TABLE VI
EVALUATION METRICS (BER, ELAPSED TIME AND PSNR FOR DIFFERENT TEST IMAGES BETWEEN THE PROPOSED METHOD AND APPROACH [20]

Proposed method			
Test image	BER	Elapsed_time	PSNR
Image_31	0.0279	11.8093	56.7469
Image_32	0.0279	10.9825	55.9146
Image_33	0.0338	11.1853	55.9349
Lena image	0.2178	12.9325	37.3755
Approach [20]			
Image_31	0.1304	17.6749	24.6694
Image_32	0.1293	18.9385	25.5656
Image_33	0.2473	17.3785	23.3109
Lena image	0.3225	17.8777	17.6177

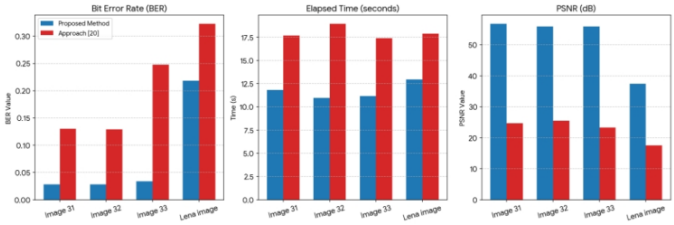


Fig. 11. Graphical analysis of BER, Elapsed_time, and PSNR for different test images between proposed method and Approach [20].

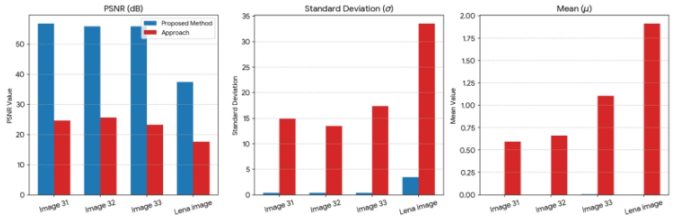


Fig.12. Comparison between proposed method and the approach [20] for IRM_31, IRM_32 and IRM_33 in term PSNR, Standard Deviation and Mean.

The Proposed Method demonstrates exceptionally high PSNR values across the first three images, ranging from 55.91 dB to 56.75 dB, and 37.38 dB for the Lena image, the approach [20] exhibits significantly lower PSNR values, ranging between 17.61 dB and 25.57 dB. The approach [20] shows much lower PSNR values (ranging from 17.61 dB to 25.57 dB, indicating lower quality and more noise. On conclude that the proposed method significantly outperforms Approach [20] in terms of imperceptibility, preserving the original quality of the medical images much better. In term of standard Deviation (σ) indicate that the Lower standard deviation values indicate more uniform error distribution and stability.

The proposed method maintains very low variation and tight statistical control compared to approach [20], proving its consistency and stability. Keeps the standard deviation very low, ranging from 0.3708 to 0.4081 for the medical images, and 3.4496 for the Lena image the approach [20] shows much higher distortion variability, with values stretching from 13.4195 up to 33.493.

A mean value closer to zero indicates that the watermarked image is nearly identical to the original. The Proposed Method achieves near-zero mean values across all tests, with the lowest being 0.0003 (Image_32) and the highest being only 0.0043 (Image_33).The Method [20] has substantially higher mean error rates, ranging from 0.5952 to 1.9097.This confirms that the proposed method introduces negligible average pixel distortion compared to Method. The proposed method introduces almost no average distortion compared to the existing approach.

The table VI presents the evaluation Metrics (BER, Elapsed Time, and PSNR) this table evaluates error rates, execution speed, and reconstruction quality. The table VI evaluates the performance of a proposed method against an existing approach from the literature approach [20].The comparison is based on three standard evaluation metrics: Bit Error Rate (BER), Elapsed time (in seconds), and PSNR.

The results obtained after performing the test across four distinct test images: image_31, image_32, image_33 and Lena. The proposed method consistently achieves a significantly lower BER across all images compared to Approach. For instance, on image_31 the proposed method reduces the BER to 0.0279 compared to 0.1304 for the existing approach. In term of Elapsed_time, the lower elapsed_time signifies faster processing executes much faster. For instance, it processes Image_1 in 11.80 seconds compared to 17.67 seconds for Method [20].The proposed method is significantly faster, processing each image is Approximately 10.9 to 18.9 seconds. On average, the proposed method reduces computational time by roughly 30% to 40%.

B. Robustness Property and Security Analysis & Active Attack Models

Active attacks: Direct system manipulation to alter data, disrupt operations, or gain unauthorized control. Unlike passive attacks that only eavesdrop, active attacks compromise the integrity or availability of a system and often result in immediate, observable damage [22, 23]. Unlike passive attacks that only try to read or detect a watermark, active attacks directly alter the media file (image, video, audio, or text) to defeat the ownership tracking mechanism.

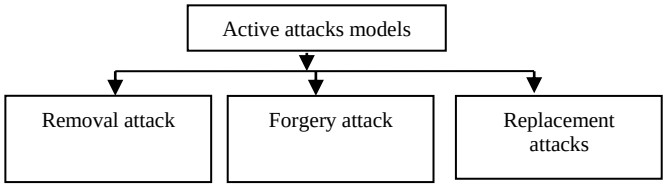
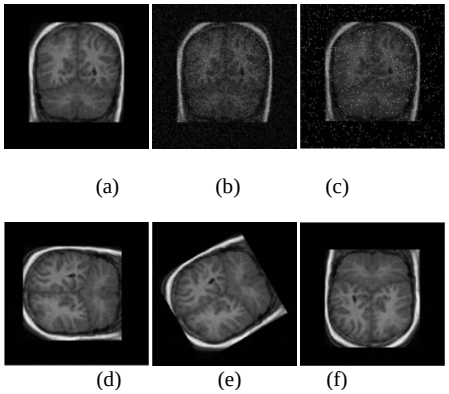


Fig. 13. Active security attacks types.

The noise image means the pixel image whose intensity is very different from those of neighboring pixels. The addition of an additive or multiplicative noise has largely been addressed in the communications and signal processing theory. With the addition of salt and pepper, Gaussian, and speckle noise, the performance of the watermarking scheme is analyzed. Table IV shows the normalized correlation values NC_1 between the original reversible watermark w_1 and the extracted watermark W_1* from the watermark W and N_{C2} between the original W_3 and the extracted W_3* after applying different attacks on the medical watermarked images and presents their comparison results with NC_2 between the original W_2 and the extracted W_{2*} using the approach [20]. The extracted watermark after different attacks is shown in the

following Fig. 15. From Table IV, we can conclude that our method is robust against some kinds of attacks that are applied to the medical watermarked images IRM_31, IRM_32, and IRM_33.

A very important property is that it must ensure a watermarking algorithm is robust against attacks. So to evaluate the robustness of our watermarking method, several types of attacks were implanted. The attack methodology on the watermarked image is based on the idea that an attacker does not have any access to the original image or the watermarked image. The attacks are, therefore, done on the watermarked image using only the watermarked image as input. The effect of these attacks on the watermarked images is shown in the following Fig. 14.



(a) (b) (c)

(d) (e) (f)

Fig. 14. The watermarked image introduced to various attacks: (a) salt & Pepper (with quality factor 60%) of the watermarked image, (b) Watermarked image attacked by after Gaussian noise, (c) Watermarked image attacked by Speckle noise, (d) Watermarked image attacked by Rotation attack (90°), (e) Watermarked image attacked by Rotation (120°), f) Watermarked image attacked by Rotation (180°).

TABLE VII
ROBUSTNESS EVALUATION OF THE PROPOSED METHOD AND APPROACH [20] AGAINST VARIOUS SECURITY ATTACKS FOR MEDICAL IMAGE

Proposed method			
IRM image	SSIM	NCC	PSNR (attacked image)
Man-in-the-Middle (MitM) attack	0.9402	0.9740	30.96
Forgery attack	0.9500	0.7081	15.98
Replacement attack	0.9504	0.7059	15.96
Speckle attack	0.9393	0.9945	37.5809
Imresize attack	0.9881	0.9881	39.1573
Salt and pepper	0.9913	0.88040.9913	39.2583
Gaussian attack	0.1517	0.8174	21.64451
Compression jpeg attack	0.9153	0.9897	34.8312
Cropping attack	0.9953	0.9985	42.9726
Approach [20]			
IRM image	SSIM	NCC	PSNR (attacked image)
Man-in-the-Middle (MitM) attack	0.8804	0.9373	26.56
Forgery attack	0.8303	0.6949	15.44
Replacement attack	0.808	0.6928	15.42
Speckle attack	0.8250	0.9093	36.9781
Imresize attack	0.9768	0.9906	24.8554
Salt and pepper	0.8540	0.9098	39.1075
Gaussian attack			21.6521
Compression jpeg attack	0.8497	0.9092	30.1111
Cropping attack	0.9354	0.9728	28.2484

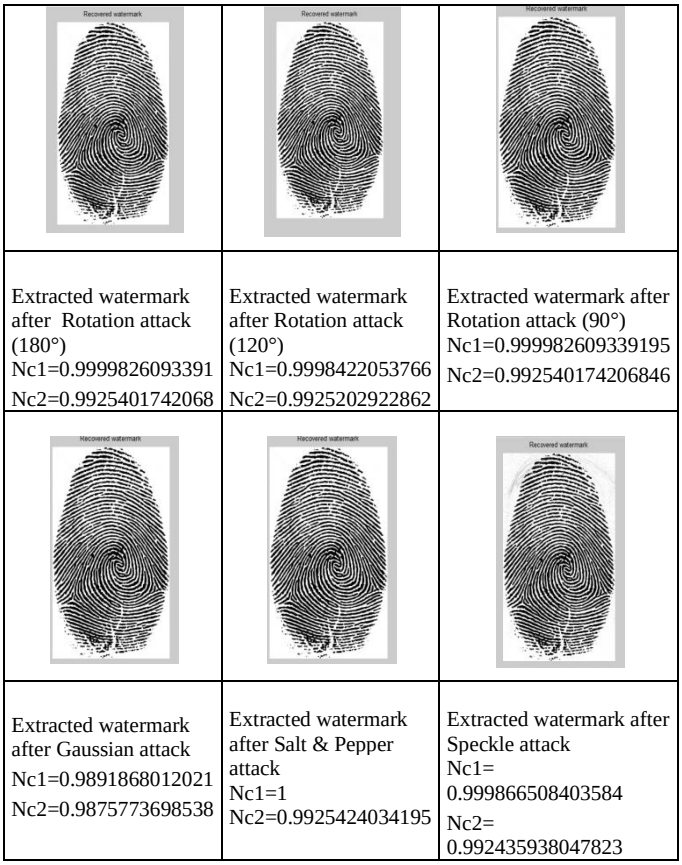


Fig. 15. Extracted watermark after different attacks from watermarked image.

TABLE VII
ROBUSTNESS EVALUATION OF THE PROPOSED METHOD AND APPROACH [20] AGAINST VARIOUS SECURITY ATTACKS FOR MEDICAL IMAGE

Proposed method			
IRM image	SSIM	NCC	PSNR (attacked image)
Man-in-the-Middle (MitM) attack	0.9402	0.9740	30.96
Forgery attack	0.9500	0.7081	15.98
Replacement attack	0.9504	0.7059	15.96
Speckle attack	0.9393	0.9945	37.5809
Imresize attack	0.9881	0.9881	39.1573
Salt and pepper	0.9913	0.88040.9913	39.2583
Gaussian attack	0.1517	0.8174	21.64451
Compression jpeg attack	0.9153	0.9897	34.8312
Cropping attack	0.9953	0.9985	42.9726
Approach [20]			
IRM image	SSIM	NCC	PSNR (attacked image)
Man-in-the-Middle (MitM) attack	0.8804	0.9373	26.56
Forgery attack	0.8303	0.6949	15.44
Replacement attack	0.808	0.6928	15.42
Speckle attack	0.8250	0.9093	36.9781
Imresize attack	0.9768	0.9906	24.8554
Salt and pepper	0.8540	0.9098	39.1075
Gaussian attack			21.6521
Compression jpeg attack	0.8497	0.9092	30.1111
Cropping attack	0.9354	0.9728	28.2484

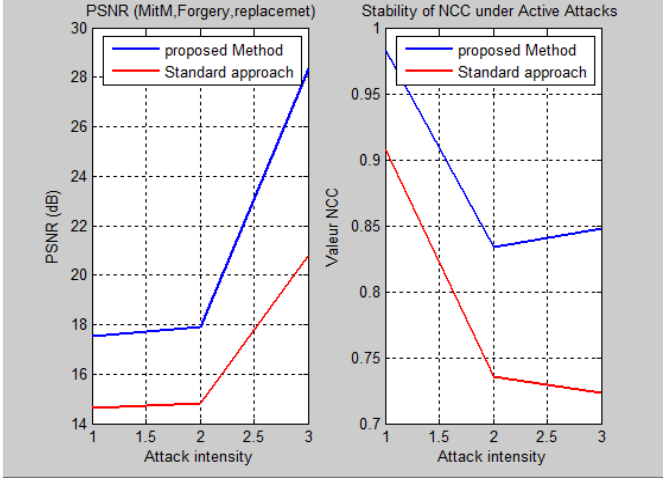


Fig. 16. Performance and stability analysis of PSNR et NCC under varying attack intensities for Image IRM.

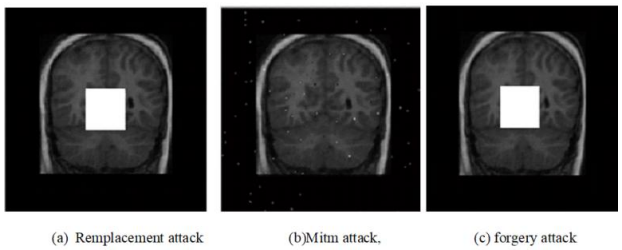


Fig. 17. Impact of replacement, MitM, and Forgery attacks on the medical image.

TABLE VIII
ROBUSTNESS EVALUATION OF THE PROPOSED METHOD AND APPROACH [20] AGAINST VARIOUS SECURITY ATTACKS (FORGERY, REPLACEMENT AND MITM) FOR MEDICAL IMAGE AND LENA IMAGE

Proposed method			
Test Image	PSNR _Forgery	PSNR_replacement	PSNR_ Man-in-the-Middle (MitM) attack
Image_31	15.98	15.9608	31.0147
Image_32	15.94	15.9091	30.8317
Image_33	15.9622	15.9355	31.0106
Lena image	17.55	17.89	28.32
Method [20]			
Image_31	15.4414	15.4196	25.9853
Image_32	15.51	15.4735	26.9879
Image_33	15.2328	15.2102	15.4735
Lena image	14.64	14.8066	20.8022

The table VII evaluates the performance and robustness compares the performance of two images processing watermarking schemes under various types of attacks using different images (IRM image). It uses the three benchmark metrics: SSIM, NCC, and PSNR (attacked image) to compare the proposed method against approach [20].

The proposed method demonstrates excellent resistance to most structural alterations maintaining SSIM et NCC values very close to 1.0 (mostly above 0.94). To evaluate the impact of the embedding factor α, we analyze the trade-off between host image quality, Normalized Cross-Correlation (NCC) under attacks, and resistance limits.

The table VIII presents a robustness evaluation comparing the proposed method against approach [20] under three types of security attacks: Forgery, Replacement, and Man–in-the-Middle (MitM). The evaluation is conducted across four test images (image_31, image_32, image_33 and Lena image), using PSNR as the evaluation metric to measure how the image quality is preserved after an attack.

TABLE IX
COMPARISON OF NCC AND PSNR METRICS FOR THE PROPOSED METHOD WITH FACTORS $\alpha 1$ AND $\alpha 2$

Factor α	$\alpha 1 = 0.5$ $\alpha 2$=0.002	$\alpha 1 = 0.5$ $\alpha 2$=0.008
PSNR	56.7469	55.8389
NCC (compression Jpeg)	0.9153	0.9152
Spekle	0.9402	0.9394
Gaussian	0.1511	0.1522
Imresize	0.988	0.9881
Cropping	0.9952	0.9952
Salt& Pepper	0.9874	0.9895
Forgery	0.9500	0.9497
Replacement	0.9504	0.9501
MitM	0.9537	0.9377

For IRM medical images, the proposed method shows comprehensive superiority. Medical images demand strict data integrity to avoid diagnostic errors. The proposed method successfully ensures that even under severe geometric modification, heavy noise, or malicious security interception, the essential structural components (SSIM) and image fidelity (PSNR) remain highly preserved compared to the existing Method.

Table IX presents performance metrics and robustness evaluation results for a proposed method under different configurations of a factor (α), keeping $\alpha 1 = 0.5$ while varying $\alpha 2$ between 0.002 and 0.008. It evaluates the method using PSNR and various attacks.

TABLE X
ERROR RATES (FAR AND FRR) OF THE PROPOSED METHOD AND APPROACH [20]

Proposed method		
Thresholds μ	FAR (Fausse acceptations)	FRR (Faux rejects)
0.100	0%	100%
0.20	25%	0%
0.30	0%	0%
0.40	0%	0%
0.50	0%	0%
0.60	0%	0%
0.70	0%	0%
0.80	0%	0%
Approach [20]		
0.10	100%	0%
0.20	25%	0%
0.30	0%	0%
0.40	0%	0%
0.50	0%	0%
0.60	0%	25%
0.70	0%	25%
0.80	0%	50%

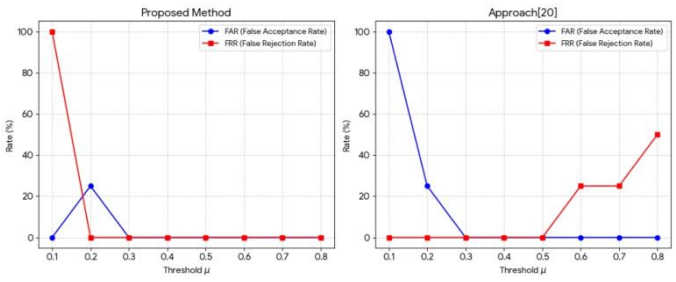


Fig. 18. Graphical comparison of False Acceptance Rate (FAR) and False Rejection Rate (FRR) performance.

Table X presents performance comparison results based on specific thresholds.

The proposed method significantly outperforms approach [20] by offering a much wider and more stable operational window. Between the thresholds of 0.30 and 0.80, the proposed method achieves an ideal performance state with **0%** FAR and 0% FRR simultaneously, whereas approach [20] suffers from high false rejection rates in the upper threshold range.

V. Conclusion

In this paper we present a new reversible and robust watermarking method to verify and ensure the security properties of authentication, confidentiality, and integrity, based on embedding the watermark W_3 obtained after combining two types of watermarks: the reversible watermark (to verify authentication and integrity) and watermark W_2 (logo or fingerprint user) to verify the confidentiality aspect. This new watermarking image is based on embedding the watermark in the transform domain DWT, DCT, and SVD.

The analysis of the experimental results shows that this method maintains a high quality of watermarked images and robustness against various types of attacks, such as rotation attacks with different angles, salt & pepper noise, Gaussian noise, and speckle noise, and proves that the application of our proposed method is valid for medical images (IRM_31, IRM_32, IRM_33).

Our method gives good results compared to the method [20]; the reason refers to the type of used transform. In the future, we will try to compare our method with other methods that have been applied to grayscale images using only medical images and especially color medical images based on embedding the color watermark with the other transform and testing the robustness property against other attacks.

References

[1] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001, doi: 10.1109/79.939835.

[2] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egypt. Inform. J.*, vol. 14, no. 1, pp. 1–13, Mar. 2013, doi: 10.1016/j.eij.2012.11.002.

[3] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U.S. Patent 5,646,997, Jul. 8, 1997.

[4] O. M. Al-Qershi and K. B. Ee, "Authentications and data hiding using a reversible ROI-based watermarking scheme for DICOM images," in *World Academy of Science, Engineering and Technology Proceedings*, vol. 50, 2009, doi: 10.5281/zenodo.1057398.

[5] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003, doi: 10.1109/TCSVT.2003.815962.

[6] G. Feng, Z. Qian, and N. Dai, "Reversible watermarking via extreme learning machine prediction," *Neurocomputing*, vol. 82, pp. 176–184, Apr. 2012, doi: 10.1016/j.neucom.2011.11.004.

[7] B. Lei, I. Y. Soon, and Z. Li, "Reversible watermarking scheme for medical image based on differential evolution," *Expert Syst. Appl.*, vol. 41, no. 12, pp. 5652–5665, Sep. 2014, doi: 10.1016/j.eswa.2014.03.018.

[8] M. E. Farfoura, S.-J. Horng, J.-L. Lai, R.-S. Run, R.-J. Chen, and M. K. Khan, "A blind reversible method for watermarking relational databases based on a time stamping protocol," *Expert Syst. Appl.*, vol. 39, no. 3, pp. 3185–3196, Feb. 2012, doi: 10.1016/j.eswa.2011.09.005.

[9] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. Burlington, MA, USA: Morgan Kaufmann, 2007, ISBN: 978-0123725851, doi: 10.5555/1564551.

[10] J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, "Digital watermarking," *J. Electron. Imaging*, vol. 11, no. 3, pp. 414–415, Jul. 2002, doi: 10.1117/1.1494073.

[11] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997, doi: 10.1109/83.650120.

[12] M. Sachin, N. Rajarathnam, and V. M. Ranjeet, "Comparative performance evaluation of DWT, SVD, and hybrid DWT-SVD watermarking for medical data integrity," *Medical Image Security Review*, vol. 14, no. 1, pp. 45–62, Jan. 2025, doi: 10.1016/j.medimg.2025.01.012.00

[13] E. Praveen Kumar, R. E. Philip, P. Sunil Kumar, and M. G. Sumithra, "DWT-SVD based reversible watermarking algorithm for embedding the secret data in medical images," in *Proc. 2013 4th Int. Conf. Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, India, 2013, pp. 1–5, doi: 10.1109/ICCCNT.2013.6726484.

[14] V. Sundhararaj, B. Meenakshipriya, P. Nirmala Devi, and K. Ezhil Vignesh, "DWT-DCT-SVD: A hybrid image watermarking algorithm with biometric authenticity and FPP resistant enhancement," *Circuits Syst. Signal Process.*, vol. 44, no. 1, pp. 6650–6675, Jan. 2025, doi: 10.1007/s00034-025-03097-7.

[15] H. Ozkaya and V. Aslantaş, "A novel self-embedded dual watermarking method for image tampering detection and recovery," *Arab. J. Sci. Eng.*, vol. 50, no. 2, pp. 1145–1162, Feb. 2025, doi: 10.1007/s13369-025-10047-7.

[16] T. A. Razak, M. A. Ali, and Z. Zheng, "Robust medical image watermarking based on DWT-SVD and deep feature extraction," *Med. Biol. Eng. Comput.*, vol. 62, no. 4, pp. 1125–1142, Apr. 2024, doi: 10.1007/s11517-023-03001-w.

[17] S. Boucherkha and M. Benmohamed, "A lossless watermarking based authentication system for medical image," *Int. J. Signal Process.*, vol. 1, no. 4, pp. 240–244, 2004.

[18] M.-S. Hsieh, "Wavelet-based image watermarking and compression," Ph.D. dissertation, Institute of Computer Science and Information Engineering, National Central University, Taiwan, Dec. 2001. [Online]. Available: National Central University Library.

[19] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[20] Y. Dong and G. Wang, "Image robust watermarking method based on DWT-SVD transform and chaotic map," *Complexity*, vol. 2024, pp. 1–13, May 2024, doi: 10.1155/2024/6618382.

[21] K. Sehra, S. Raut, A. Mishra, P. Kasturi, S. Wadhera, G. J. Saxena, and M. Saxena, "Robust and secure digital image watermarking technique using Arnold transform and memristive chaotic oscillators," *IEEE Access*, vol. 9, pp. 72465–72483, 2021, doi: 10.1109/ACCESS.2021.3079310.

[22] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Upper Saddle River, NJ, USA: Pearson, 2020.

[23] A. R. Smith and M. Jones, "An analysis of active and passive cyber attacks on distributed systems," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 2, pp. 1024–1035, Jun. 2023, doi: 10.1109/TNSM.2023.1234567.

[24] R. Cappelli, D. Maio, and D. Maltoni, "Evaluation techniques for biometrics-based authentication systems," in *Proc. 15th Int. Conf. Pattern Recognition (ICPR)*, Sep. 2000, vol. 2, pp. 561–564, doi: 10.1109/ICPR.2000.906204.



Souad Bekkouche is an Associate Professor at University of SAIDA-Dr. Moulay Tahar, SAIDA, Algeria. She received the M.S. degrees in Computer Science from from Djillali Liabes University of Sidi Bel Abbes, Algeria, in 2012, and her Doctorate degree in Computer Science in 2016 from Djillali Liabes University of Sidi Bel Abbes, Algeria. Her current research interests are networking, network security, images processing, cryptography and IoT.



Abdelaziz Tami is an Associate Professor at University of SAIDA-Dr. Moulay Tahar, SAIDA, Algeria. He received the M.S. degrees in Computer Science from the National Superior School of Computing of Algiers, Algeria, in 2012, his Doctorate degree in Computer Science in 2021 from Djillali Liabes University of Sidi Bel Abbes, Algeria, and his Habilitation to Supervise Research (HDR) degree in 2025 from University of SAIDA-Dr. Moulay Tahar, SAIDA, Algeria. His current research interests are networking, wireless ad-hoc, vehicular networks, network security, images processing, cryptography and IoT.