Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.035048
Article

Hybrid Watermarking and Encryption Techniques for Securing Medical Images

Amel Ali Alhussan[1,*], Hanaa A. Abdallah[2], Sara Alsodairi[2] and Abdelhamied A. Ateya[3]

[1]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 84428, Saudi Arabia
[3]Department of Electronics and Communications Engineering, Zagazig University, Zagazig, Sharqia, 44519, Egypt
*Corresponding Author: Amel Ali Alhussan. Email: a_ashraf@zu.edu.eg
Received: 05 August 2022; Accepted: 30 September 2022

Abstract: Securing medical data while transmission on the network is required because it is sensitive and life-dependent data. Many methods are used for protection, such as Steganography, Digital Signature, Cryptography, and Watermarking. This paper introduces a novel robust algorithm that combines discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) digital image-watermarking algorithms. The host image is decomposed using a two-dimensional DWT (2D-DWT) to approximate low-frequency sub-bands in the embedding process. Then the sub-band low-high (LH) is decomposed using 2D-DWT to four new sub-bands. The resulting sub-band low-high (LH_1) is decomposed using 2D-DWT to four new sub-bands. Two frequency bands, high-high (HH_2) and high-low (HL_2), are transformed by DCT, and then the SVD is applied to the DCT coefficients. The strongest modified singular values (SVs) vary very little for most attacks, which is an important property of SVD watermarking. The two watermark images are encrypted using two layers of encryption, circular and chaotic encryption techniques, to increase security. The first encrypted watermark is embedded in the S component of the DCT components of the HL2 coefficients. The second encrypted watermark is embedded in the S component of the DCT components of the HH_2 coefficients. The suggested technique has been tested against various attacks and proven to provide excellent stability and imperceptibility results.

Keywords: Watermarking; discrete wavelet transform; discrete cosine transform; singular value decomposition; circular encryption; chaotic encryption

1 Introduction

Securing medical images is an important issue in healthcare. Patient information such as electronic health records (EHR) and medical images, e.g., X-rays, computerized tomography (CT), and Magnetic resonance imaging (MRI) scans, need to be shared on the network [1]. There are two ways to protect medical images: encryption, which provides confidentiality, and watermarking, which provides authentication [2]. Digital watermarking saves different information like texts, images, audio, or videos [3].

Transform domains are used in watermarking techniques [4,5]. Watermark embedding methods are commonly applied in the spatial domain [6,7] or the frequency domain [8,9]. The spatial domain is weak to the image threats such as (JPEG) compression; the frequency domain has better quality regarding image watermarking by altering their coefficients. The robustness requirements of digital watermarking algorithms operated in the frequency domain are better than spatial domain techniques [5].

A discrete cosine transform (DCT) converts images into low, mid, and high-frequency sub-bands. While high-frequency areas of the image can be removed when attacks (compression and noise) are applied, the image's major and important viewable regions are found in the low-frequency sub-bands [10]. In order to keep the watermark robust when compressed and prevent simultaneous changes to the desired or noticeable quality of the image, watermarks are inserted in middle-frequency sub-band coefficients [11,12].

In discrete wavelet transform (DWT), an image is split into four non-overlapping multi-resolution sub-bands [13], labeled LL (approximation sub-band), LH (horizontal sub-band), HL (vertical sub-band), and HH (diagonal sub-band). All of the signal's energy is occupied by sub-bands with low frequencies. High frequency encompasses the image's texture, edges, and outlines. Lower frequency sub-bands contain most of the image's energy; hence, when watermarks are inserted in low-frequency sub-bands, the image's quality may be diminished, but its robustness may be increased [14]. Typically, the human eye cannot detect changes in these sub-bands. The high-frequency range is used for watermark embedding since the human eye cannot detect it and has an adequate level of imperceptibility and robustness [15].

Using the singular value decomposition (SVD) transformation, a matrix can be split into three identically sized matrices. An image is a matrix of nonnegative scalar elements from the perspective of linear algebra [16].

Encryption is a series of mathematical operations applied to data to generate a different type of data called a cipher [17]. To distinguish between two forms of data, the plaintext is used for unencrypted data, and cipher text is used for encrypted data [18]. The capacity of a cipher to generate cipher text that cannot be easily reversed to the original plaintext is the security of encryption. There are two forms of encryption: there are two types (Symmetric key and Asymmetric key algorithm). There are many reasons to use encryption: Reliability refers to the fact that the cipher text can be recovered and that the recovered data is identical to the plaintext; the encryption mechanism will keep the information hidden, which is security [19,20]. The SHIFT function is used to shift the elements of a vector or array in a circular fashion. The size and data type of the output array are identical to those of the input array. Regardless of the number of dimensions in the input array, shifts are handled in the same way: Depending on the number of rows and columns supplied by the second and third parameters of the procedure, the contents of entire rows and/or columns are shifted to the rows above or below, or to the columns to the right or left. Positive values for the second and third parameters move rows up (or columns to the right), while negative values move rows down (or columns to the left) (or columns to the left) [21].

Image pixels are randomly reconfigured in chaotic image encryption. The Cat map, the Line map, and the Baker map are all examples of chaotic maps that can be utilized for picture encryption [20,22]. The Cat map performs a geometric transformation. The line map extends all the pixels to make a straight line and then folds them according to a set of rules. After this operation, the plain image's pixels are randomly distributed in the encrypted image, and the adjacent pixels are no longer significant. On the other hand, the Baker map expands the image horizontally before folding it vertically. The positions of every pixel in the plain image are altered by repeating this method [23,24].

In this work, we develop a watermarking scheme to assess the effects of several medical image-processing techniques as attacks like Gaussian noise. A DWT-DCT-SVD transform method was performed to embed the watermark. The secret image is scrambled using circular and chaotic encryption. Simulation using Matlab was used to apply various image processing techniques to insert and extract watermarks to check whether watermarking is effective.

2 Related Works

This section summarizes the recently developed watermarking techniques introduced for medical imaging. In [25], Priya et al. proposed a medical image encryption method. In order to secure patient information, the electronic patient record is incorporated within the original medical photograph. The doctor's fingerprint is then added to the watermarked medical image, which is then encrypted into a visually significant encrypted image. The results reveal that the proposed approach achieves high peak signal to noise ratio values, resulting in high visibility. In addition, gives high data integrity by providing authentication using a fingerprint image.

In [26], Haddad et al. proposed a new biometric reinforcement security approach by combining two watermarking schemes on two levels. In the first level: the first watermark is generated using the fingerprint minutiae; this watermark is impeded into the face image using a wavelet packet decomposition. The previously watermarked face is used as the watermark on the second level. It is jammed into the original fingerprint image using the same watermarking procedure as in the first level. The resulting watermarked fingerprint can be used to verify one's identity. The proposed watermarking approach's visual quality, robustness, complexity, and verification accuracy are all examined. The results show that the proposed method is robust to several signal-processing attacks.

In [27], Thakkar et al. proposed a blind im-age-watermarking scheme. The logo and EPR are used as watermarks to verify and identify the original medical image. The ROI of the medical image is where the watermarks are placed, i.e., region of interest. The wavelet decomposition of the medical image's ROI is used in the DWT to produce various frequency sub-bands. They produce several singular matrices using block-SVD and the low-frequency sub-band LL of the ROI. At the receiving end, both watermark contents are blindly recovered. The experiment findings indicate that this strategy offers improved visibility of watermarked images and recovery of watermark content because of the DWT-SVD combination. The suggested approach is suitable for watermarking color photos and resistant to several signal-processing attacks.

A watermarking method with two modules, embedding, and extraction, was proposed by Aparna et al. in [28]. The fingerprint biometric is used for authentication, while the encryption and reversible watermarking ensure confidentiality and integrity, respectively. The fingerprint and the electronic health record watermarks are embedded in the medical image to verify the patient's identity (HER). The ROI region is separated from the input picture during the embedding phase using the RG algorithm. Then, compute the SHA-256 hash of the ROI. After that, elliptical cryptography should be used to protect the EHR. The next step is to extract the fingerprint's minutiae point and combine it with the previous ROI and Her. It is thus possible to compress hexadecimal numbers via arithmetic coded concatenation. Embed the compressed bit stream back into the original image after completing this step. At long last, they've got their hands on a copy of the watermarked image. The extraction method includes a reverse operation. According to experiments, this approach improves image quality and enhances embedding performance.

3 Proposed Technique

The proposed technique applies DWT of the original image to LL, LH, HL, and HH. Then the sub-band LH is decomposed using 2D-DWT to LL_1, LH_1, HL_1, and HH_1. Then the sub-band LH1 is decomposed using 2D-DWT to LL_2, LH_2, HL_2, and HH_2. Two frequency bands (HH_2) and (HL_2) are transformed by using 2D-DCT and then applying SVD to the DCT coefficients to get S values, and then the S values are added to the watermark at different depths. The two watermark images are encrypted using circular encryption and chaotic to increase security. The first encrypted watermark is embedded in the S component of the HL2 Coefficients' DCT components. In contrast, the second encrypted watermark is embedded in the S component of the HH2 Coefficients' DCT components.

Then the method is applied by using another technique by embedding the watermark in the least significant bit of the singular values. Inverse SVD on changed S vector and original U, V vectors are used to create the watermarked image, which is then processed twice using inverse 2D-DCT and inverse 2D-DWT. This proposed addition technique improves the robustness of the host image without degrading it. Watermark embedding at the sender and watermark extraction at the receiver are the two aspects of the proposed technique, as introduced in algorithm 1. Fig. 1 shows the embedding process, Fig. 2 shows the 2-level DWT, and Fig. 3 presents the extraction process. The main steps of the extraction process are introduced in algorithm 2.

Algorithm 1: Proposed DWT, DCT, SVD-based watermarking technique

Sender:

Embedding process:

Step 1: Decompose the cover image into four sub-bands using 2D-DWT: LL, HL, LH, and HH.

Step 2: Choose the LH1 sub-band, and apply 2D-DWT on the sub-band to produce four smaller sub-bands: LL_2, HL_2, LH_2, and HH_2.

Step 3: Apply 2D-DCT to sub-bands (HL_2 and HH_2).

Step 4: Calculate the DCT coefficients' singular values for HL_2 and HH_2.

Step 5: Encrypt the two grey-scale watermark images (W_1, W_2) using circular and chaotic encryption techniques.

Step 6: Embed the first encrypted watermark in the (S values) of the coefficients of DCT of HH_2 and the second encrypted one in the singular values (S) of the DCT coefficients of HL_2 using two methods:

1-Least significant bits: put the bits of the encrypted watermark in the least significant bits of the s values of the DCT coefficients of the two sub-bands HH2 and HL2.

2-The additive technique: by the following equations:

- Singular values (Watermarked sub-band (HH2)) = Singular values (dct2 (HH2)) + k1 (factor) * encrypted watermark1.
- Singular values (Watermarked sub-band (HL2)) = Singular values (dct2 (HL2)) + k1 (factor) * encrypted watermark2.

Step 7: Use inverse SVD on the changed S vector and the original U and V vectors.

Step 8: Apply inverse DCT (IDCT) to each sub-band.

Step 9: Apply the inverse DWT (IDWT) to the DWT transformed image, including the updated sub-band, to get the watermarked image.

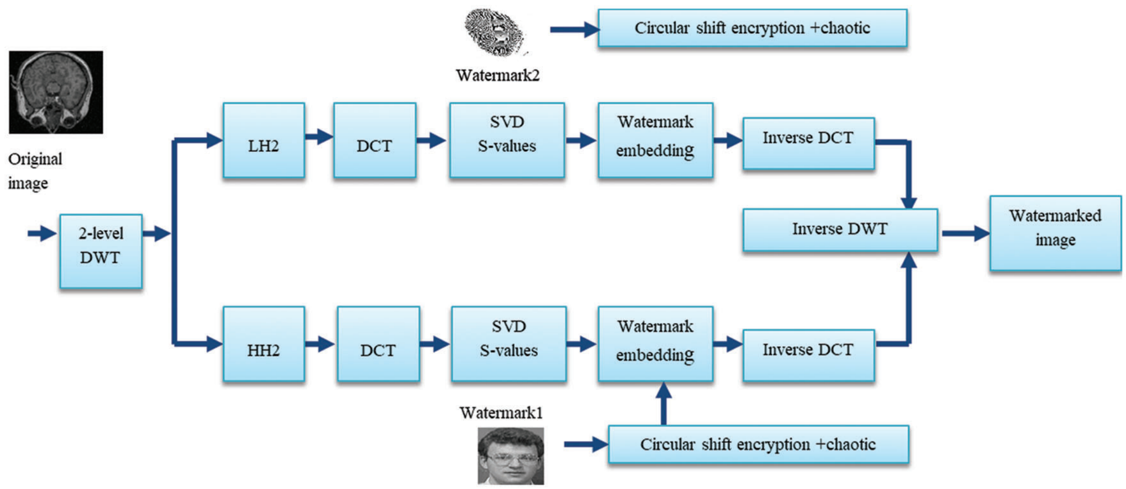


Figure 1: Main steps of the embedding process

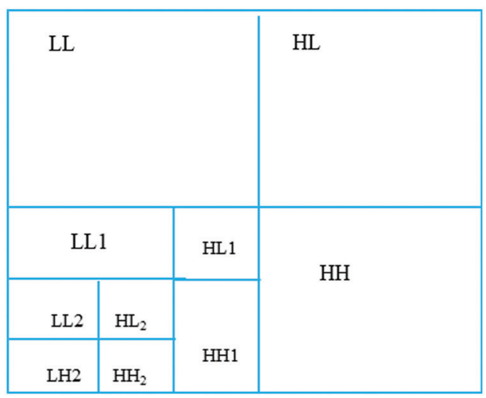


Figure 2: 2-level DWT

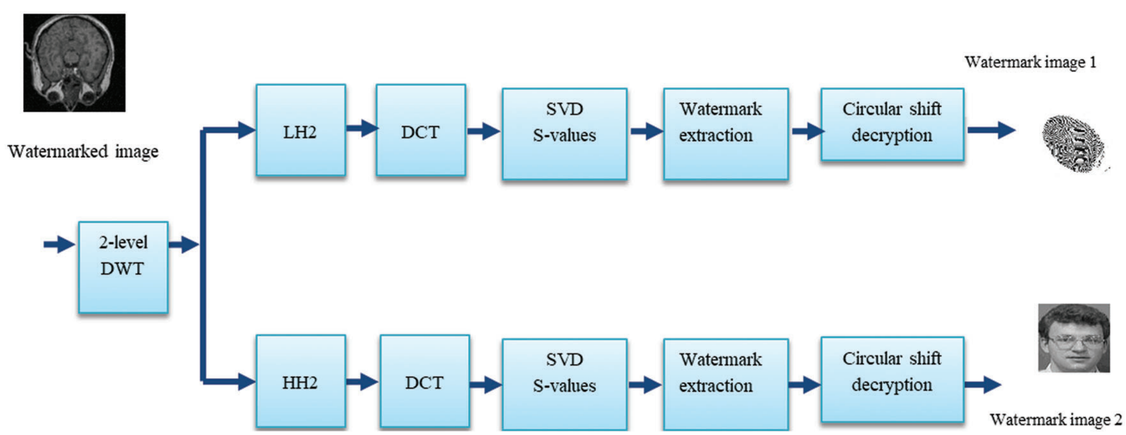


Figure 3: Main steps of the extraction process

Algorithm 2: Extraction algorithm

Extraction process:

Step 1: Decompose the watermarked image into four sub-bands using 2D-DWT: LL, HL, LH, and HH.

Step 2: - Apply 2D-DWT to LH to get four sub-bands, then select the LH1 sub-band.
- Apply 2D-DWT to the LH1 sub-band to get four sub-bands, then select the HH_2 and HL_2 sub-bands.

Step 3: Apply 2D-DCT to the sub-bands (HL2 and HH2), and extract coefficients of DCT.

Step 4: Calculate the singular values of DCT coefficients for HL_2 and HH_2.

Step 5: Reconstruct the watermark:

1- Take the singular values' LSB (least significant bits).

2- Use the equations:

- Encrypted watermark1 = S (watermarked sub-band (HH_2) − S (original sub-band (HH_2))/k1;
- Encrypted watermark2 = S (watermarked sub-band (HL_2) − S (original sub-band (HL_2))/k1.

Step 6: Decrypt the watermarks using circular decryption + chaotic decryption.

4 Performance Evaluation

4.1 Performance Measures

Two independent parameters can be used to assess the quality of digital watermarking: imperceptibility and resilience. The PSNR of the host picture and the embedded image in dB are used to determine imperceptibility. Higher PSNR is preferred since it effectively hides the designated picture. The original and restored watermark images are compared to determine robustness. When the peak signal-to-noise ratio (PSNR) is high, the watermarked image resembles the original image more closely, implying that the watermark is undetectable. Watermarked images with a PSNR greater than 35 are generally acceptable. The following performance evaluation measures are used in most watermarking projects.

For invisible watermarking methods, the watermark should be imperceptible, and the human eye should not be able to distinguish between the watermarked and the original images. This measure is subjective and thus is not always reliable for evaluating a watermarking algorithm.

The peak signal-to-noise ratio (PSNR) measure is used between the watermarked and the unwatermarked images. It is related to imperceptibility, where a higher PSNR means a higher imperceptibility [29].

$$PSNR(dB) = 10\log_{10}\left(\frac{255^2}{\frac{1}{N^2}\sum_{x,y}\left(A_w(x,\ y) - A(x,\ y)\right)^2}\right) \tag{1}$$

A correlation coefficient measure is used between the extracted and the original watermarks, where a higher correlation coefficient means that the extracted watermark is the one of interest. This measure is calculated as follows [29].

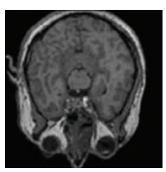
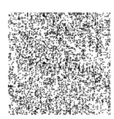
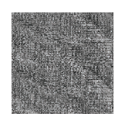
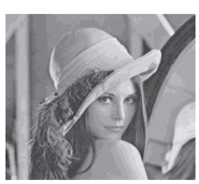
$$c_r\left(W,\ \hat{W}\right) = \frac{\sum_y W(y)\hat{W}(y)}{\sqrt{\sum_y W^2(y)\sum_y \hat{W}^2(y)}} \tag{2}$$

where, W and W^ are the original and extracted watermarks, respectively.

4.2 Results

Experiments have been done on both medical and standard images. The test shows the imperceptibility of the original image, which has been watermarked. The robustness of the watermark is approved by applying different types of attacks: image cropping, noise, i.e., salt and pepper-Gaussian, image rotation, and median filter. Experiments were done on different images; a 1024 × 1024-host image and 128 × 128 of two watermark images were used. Table 1 shows the host image, two watermark images, and the encrypted watermarks. Row (A) for medical image with fingerprint and the image of patient as watermarks in order to protect the MRI of the patient. In addition, row (B) shows the original image of "Lena" and the watermarked images.

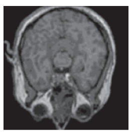
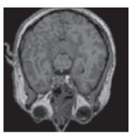
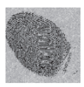
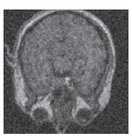
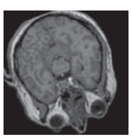
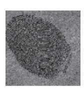
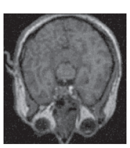
Table 1: The original image, the two original watermarks, and the encrypted watermarks

	Original image	Original watermark1	Original watermark2
(A)			
		Encrypted watermark1	Encrypted watermark2
			
	Original image	Original watermark1	Original watermark2
(B)			
		Encrypted watermark1	Encrypted watermark2
			

The extracted watermarks with and without attacks such as median filter, Rotation, Cropping, Gaussian, and Salt and Pepper are shown in Tables 2 and 3, respectively, for medical and Standard images. The (A) part uses the DWT-DCT-SVD-additive technique with watermark depth = 0.09, while the (B) part uses DWT-DCT-SVD-LSB.

Table 2: Results of the proposed techniques with different types of attacks (A) using the DWT-DCT-SVD-additive technique with watermark depth = 0.09, (B) using DWT-DCT-SVD-LSB

(A) Results of watermarking using the DWT-DCT-SVD-additive technique with watermark depth =0.09

Attack type	Watermarked image	Recovered watermark1	Recovered watermark2
Without attack			
Median filter [33]			
Gaussian noise variance=0.1			
Rotation 80			
cropping			
salt and pepper noise variance=0.02			

(B) Results of Watermarking using DWT-DCT-SVD-LSB

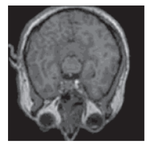
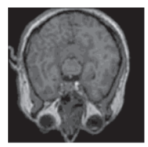
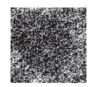
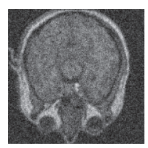
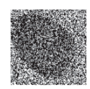
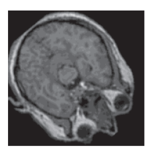
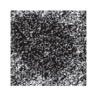
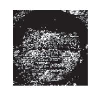
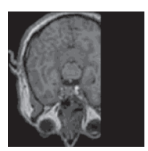
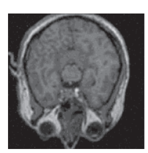
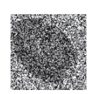
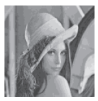
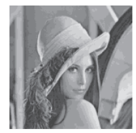
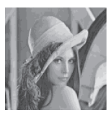
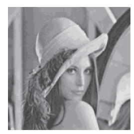
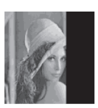
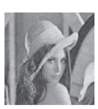
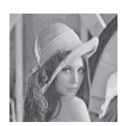
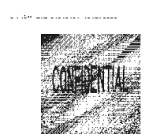
Watermarked image	Recovered watermark1	Recovered watermark2	Attack type
			Without attack
			**Median filter [33]**
			**Gaussian noise variance=0.1**
			**Rotation 80**
			**cropping**
			**salt and pepper noise variance=0.02**

Table 3: Result of proposed techniques in the standard image with different types of attacks (A) using the DWT-DCT-SVD-additive technique with watermark depth = 0.09, (B) using DWT-DCT-SVD-LSB

(A) Results of Watermarking using the DWT-DCT-SVD-additive technique with watermark depth =0.09				(B) Results of Watermarking using DWT-DCT-SVD-LSB			
Attack type	**Watermarked image**	**Recovered watermark1**	**Recovered watermark2**	**Watermarked image**	**Recovered watermark 1**	**Recovered watermark2**	**Attack type**
Without attack							Without attack
Median filter [33]							**Median filter [3 3]**
Gaussian noise variance=0.1							**Gaussian noise variance=0.1**
Rotation 80							**Rotation 80**
cropping							**cropping**
salt and pepper noise variance=0.02							**salt and pepper noise variance=0.02**

A PSNR representation with values higher than 35 dB is within an acceptable level of degradation, which means that it is almost not seen by the Human visual system (HVS). The extracted watermarks after various attacks with Correlation values as a measure for robustness are shown in Tables 4 and 5, respectively, for the medical and standard image; (A) Using DWT-DCT-SVD-additive technique with watermark depth = 0.09, and (B) using DWT-DCT-SVD-LSB.

Table 4: PSNR of watermarked medical image and correlation of recovered watermarks in (A) using the DWT-DCT-SVD-additive technique with watermark depth = 0.09 and (B) using DWT-DCT-SVD-LSB

(A) Results of watermarking using DWT-DCT-SVD-additive technique with watermark depth = 0.09				(B) Results of watermarking using DWT-DCT-SVD-LSB			
Attack type	PNSR dB	Correlation of watermarked 1	Correlation of watermarked 2	PNSR dB	Correlation of watermarked 1	Correlation of watermarked 2	Attack type
Without attack	38.86	0.99	0.99	64.97	0.99	0.84	Without attack
Median filter [3 3]	42.32	0.97	0.95	59.66	0.34	0.83	Median filter [3 3]
Gaussian noise variance = 0.1	12	0.99	0.84	12.01	0.42	0.47	Gaussian noise variance = 0.1
Rotation 80	15	0.85	0.86	14.42	0.30	0.35	Rotation 80
Cropping	17.43	0.98	0.98	17.45	0.88	0.89	cropping
Salt and pepper noise variance = 0.02	19.54	0.99	0.88	24.43	0.42	0.47	salt and pepper noise variance = 0.02

Table 5: PSNR of watermarked standard image and correlation of recovered watermarks in (A) using the DWT-DCT-SVD-additive technique with watermark depth = 0.09 and (B) using DWT-DCT-SVD-LSB

(A) Results of watermarking using the DWT-DCT-SVD-additive technique with watermark depth = 0.09				(B) Results of watermarking using DWT-DCT-SVD-LSB			
Attack type	PNSR dB	Correlation of watermarked 1	Correlation of watermarked 2	PNSR dB	Correlation of watermarked 1	Correlation of watermarked 2	Attack type
Without attack	37.34	0.97	0.97	69.6	0.95	0.91	Without attack
Median filter [3 3]	39.83	0.73	0.87	45.41	0.92	0.56	Median filter [3 3]
Gaussian noise variance = 0.1	11.36	0.95	0.91	11.38	0.42	0.25	Gaussian noise variance = 0.1
Rotation 80	11.27	0.59	0.41	10.68	0.59	0.63	Rotation 80
Cropping	10.32	0. 95	0.95	10.33	0.88	0.89	cropping
Salt and pepper noise variance = 0.02	20.58	0. 97	0.95	32.50	0.51	0.34	salt and pepper noise variance = 0.02

Table 6 applies the DWT-DCT-SVD-additive technique with watermark depth = 0.09 to different medical images. Results show that the robustness of watermarks is high even after applying different types of attacks; the watermarks can be recovered with acceptable quality. In Image 1, the average correlation for recovered watermark1 (W_1) equals .92 and .89 for watermark2 (W_2). In Image 2, the average correlation for recovered W_1 equals .91 and .88 for W_2. In Image 3, the average correlation for recovered W_1 equals .92 and .89 for W_2. In Image 4, the average correlation for recovered W_1 equals .93 and .88 for W_2. Table 7 compares proposed techniques with and without encryption to watermarks. The results show the high quality of the extracted watermark image in the additive technique using encrypted watermarks even in the presence of attacks. Figs. 4 and 5 show the comparison among the applied techniques using the effective additive watermarks with and without encryption to watermarks and the LSB watermarking with and without encryption to watermarks; it is shown that the watermarking using the additive technique using encrypted watermarks gives high performance even in the presence of attacks.

Table 6: Results of different medical images Watermarking using the DWT-DCT-SVD-additive technique with watermark depth = 0.09

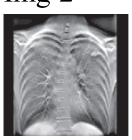
Image	Attack type	PNSR	Correlation of watermarked 1	Correlation of watermarked 2
Img 1	Without attack	39.06	0.99	0.97
	Median filter [3 3]	42.48	0.90	0.93
	Gaussian noise variance = 0.1	12.06	0.99	0.84
	Rotation 20	14.18	0.67	0.82
	Cropping	17.19	0.98	0.94
	Salt and pepper noise variance = 0.03	19.42	0.99	0.88
Img 2	Without attack	39.16	0.99	0.96
	Median filter [3 3]	42.32	0.88	0.91
	Gaussian noise variance = 0.1	11.67	0.99	0.84
	Rotation 20	11.89	0.64	0.79
	Cropping	12.16	0.97	0.94
	Salt and pepper noise variance = 0.03	19.99	0.99	0.89
Img 3	Without attack	39.16	0.99	0.96
	Median filter [3 3]	42.46	0.92	0.92
	Gaussian noise variance = 0.1	12.22	0.99	0.85
	Rotation 20	14.32	0.66	0.79
	Cropping	17.11	0.97	0.94
	Salt and pepper noise variance = 0.03	19.12	0.99	0.88
Img 4	Without attack	39.06	0.99	0.97
	Median filter [3 3]	42.25	0.91	0.91
	Gaussian noise variance = 0.1	12.03	0.99	0.84
	Rotation 20	14.61	0.71	0.83
	Cropping	19.48	0.99	0.88
	Salt and pepper noise variance = 0.03	17.34	0.97	0.89

Table 7: Comparison among proposed techniques with and without encryption to watermarks

Attacks	Proposed technique + encryption-additive. "correlation"		Proposed technique without encryption-additive. "correlation"		Proposed technique + encryption-LSB "correlation"		Proposed technique without encryption-LSB "correlation"	
Without attack	0.97	0.97	0.97	0.96	0.95	0.91	0.95	0.91
Median filter [3 3]	0.74	0.86	0.65	0.76	0.92	0.56	0.89	0.44
Gaussian noise variance = 0.1	0.95	0.84	0.79	0.49	0.42	0.25	0.38	0.24
Image rotation	0.61	0.60	0.50	0.34	0.59	0.63	0.70	0.61
Cropping	0.95	0.95	0.96	0.96	0.88	0.89	0.90	0.89
Salt and pepper noise variance = 0.02	0.97	0.95	0.31	0.20	0.51	0.34	0.41	0.32

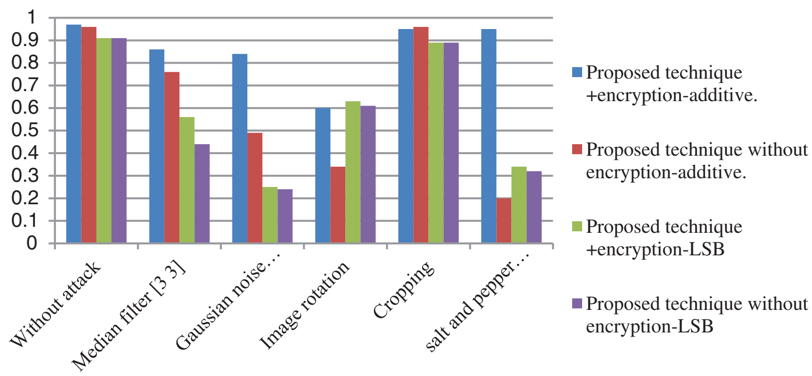


Figure 4: Comparison among proposed techniques with and without encryption for watermark 1

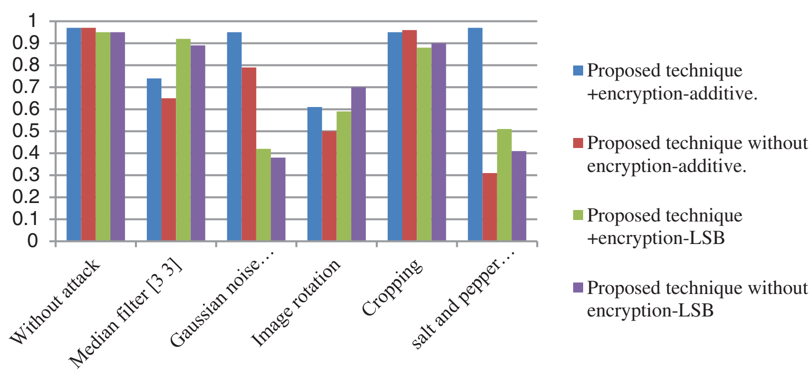


Figure 5: Comparison among proposed techniques with and without encryption for watermark 2

5 Conclusions

The experimental results show that the modified watermarking technique-using additive in DWT domain with encrypted watermarks using circular and chaotic encryption to watermarks technique enhances the imperceptibility measurements PSNR as well as the robustness of the system against attacks such as data filtering. The modified technique improves robustness against all attacks than watermarking without encryption. In addition, the technique-using additive is better than using LSB.

Acknowledgement: The authors extend their appreciation to Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R308), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R308), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Asgari Taghanaki, K. Abhishek, J. P. Cohen, J. Cohen-Adad and G. Hamarneh, "Deep semantic segmentation of natural and medical images: A review," *Artificial Intelligence Review*, vol. 54, no. 1, pp. 137–178, 2021.

[2] R. Thabit, "Review of medical image authentication techniques and their recent trends," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13439–13473, 2021.

[3] N. Sangeetha, X. Anita and R. Vijayarajan, "Medical image watermarking: A review on wavelet-based methods," in *Signal and Image Processing Techniques for the Development of Intelligent Healthcare Systems*. Singapore: Springer, pp. 203–221, 2021.

[4] P. Kadian, S. M. Arora and N. Arora, "Robust digital watermarking techniques for copyright protection of digital data: A survey," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3225–3249, 2021.

[5] M. R. Keyvanpour, N. Khanbani and M. Boreiry, "A secure method in digital video watermarking with transform domain algorithms," *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 20449–20476, 2021.

[6] X. Zhang and Q. Su, "A spatial domain-based color image blind watermarking scheme integrating multilevel discrete Hartley transform," *International Journal of Intelligent Systems*, vol. 36, no. 8, pp. 4321–4345, 2021.

[7] J. Ooi, H. L. Khor, S. C. Liew and S. I. Hisham, "Performance comparison of spatial domain-based watermarking techniques," in *Proc. 2021 Int. Conf. on Software Engineering & Computer Systems and 4th Int. Conf. on Computational Science and Information Management (ICSECS-ICOCSIM)*, Pekan, Malaysia, IEEE, pp. 64–69, 2021.

[8] A. Stallin, K. P. Kumar and B. Prabha, "Hidden image watermarking based on frequency domain technique," in *Proc. 2022 Second Int. Conf. on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, IEEE, pp. 1–6, 2022.

[9] A. Sahin and I. Guler, "A survey of digital image watermarking techniques based on discrete cosine transform," *International Journal of Information Security Science*, vol. 10, no. 3, pp. 99–110, 2021.

[10] S. Kumar, B. Panna and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019.

[11] N. K. Murthy, S. Sharma, M. J. P. Priyadarsini, R. Ranjan, S. Sarkar *et al.,* "Image steganography using discrete cosine transform algorithm for medical images," in *Proc. Advances in Automation, Signal Processing, Instrumentation, and Control*, Singapore, Springer, pp. 2349–2358, 2021.

[12] R. Wang, N. Fang, Y. He, Y. Li, W. Cao *et al.,* "Multi-modal medical image fusion based on geometric algebra discrete cosine transform," *Advances in Applied Clifford Algebras*, vol. 32, no. 2, pp. 1–23, 2022.

[13] M. Diwakar, A. Tripathi, K. Joshi, A. Sharma, P. Singh *et al.,* "A comparative review: Medical image fusion using SWT and DWT," *Materials Today: Proceedings*, vol. 37, pp. 3411–3416, 2021.

[14] S. P. Yadav and S. Yadav, "Fusion of medical images using a wavelet methodology: A survey," *IEIE Transactions on Smart Processing & Computing*, vol. 8, no. 4, pp. 265–271, 2019.

[15] V. Anusuya and V. S. Raghavan, "A review on medical image compression using wavelet transform in medical images," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 6, pp. 2925–2933, 2021.

[16] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, pp. 426–437, 2019.

[17] V. Pavithra and C. Jeyamala, "A survey on the techniques of medical image encryption," in *Proc. 2018 IEEE Int. Conf. on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, IEEE, pp. 1–8, 2018.

[18] K. N. Singh and A. K. Singh, "Towards integrating image encryption with compression: A survey," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 18, no. 3, pp. 1–21, 2022.

[19] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, 2020.

[20] B. Zolfaghari and T. Koshiba, "Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap," *Applied System Innovation*, vol. 5, no. 3, pp. 57, 2022.

[21] A. K. Singh, A. Anand, Z. Lv, H. Ko and A. Mohan, "A survey on healthcare data: A security perspective," *ACM Transactions on Multimidia Computing Communications and Applications*, vol. 17, no. 2s, pp. 1–26, 2021.

[22] G. Grassi, "Chaos in the real world: Recent applications to communications, computing, distributed sensing, robotic motion, bio-impedance modelling and encryption systems," *Symmetry*, vol. 13, no. 11, pp. 2151, 2021.

[23] G. Ghosh, D. Anand, S. Verma, N. Z. Jhanjhi and M. N. Talib, "A review on chaotic scheme-based image encryption techniques," *Intelligent Computing and Innovation on Data Science*, vol. 248, pp. 473–481, 2021.

[24] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair *et al.,* "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, pp. 1–19, 2022.

[25] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Networks and Applications*, vol. 26, pp. 1–8, 2019.

[26] L. R. Haddada, B. Dorizzi and N. E. B. Amara, "A combined watermarking approach for securing biometric data," *Signal Processing: Image Communication*, vol. 55, pp. 23–31, 2017.

[27] 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, 2017.

[28] P. Aparna and P. V. V. Kishore, "Biometric-based efficient medical image watermarking in E-healthcare application," *IET Image Processing*, vol. 13, no. 3, pp. 421–428, 2019.

[29] K. N. Hussin, A. K. Nahar and H. K. Khleaf, "A visual enhancement quality of digital medical image based on bat optimization," *Engineering and Technology Journal*, vol. 39, no. 10, pp. 1550–1570, 2021.