Joint watermarking encryption compression algorithm for securing an e-healthcare application

Daham Abderrahmane[1], Ouslim Mohamed[2]
[1]Department of Mathematics and Computer Science, Faculty of Science and Technology, University of Tahri Mohamed Bechar, Bechar, Algeria
[2]LMSE Lab, Department of Electronic, Faculty of Electrical Engineering, University of Sciences and Technology Mohamed Boudiaf Oran, Bir El Djir, Algeria

Article Info

Article history:

Received Jul 3, 2023
Revised Aug 4, 2023
Accepted Aug 15, 2023

Keywords:

Chao-encryption
Discrete wavelet transform-singular value decomposition
Joint-compression
Medical imagee
Modulo-one transformations
Telemedecine
Watermarking

ABSTRACT

Radiological imaging generates large data volumes for diagnosing. These data volumes still constitute an immense challenge for individual radiology practices, either when complying with the archive, hacker manipulation or swiftly distributing images among specialists as part of the diagnostic process. Analyzing images through illegal distortions may lead to inaccurate medical decisions. Watermarking techniques can be used to authenticate images, detect, and recover illegal changes made to teleradiology images as well. In this paper, a new blind medical image watermarking joint crypto-compression system is proposed to simultaneously achieve watermarking and compression. A discrete wavelet transform is applied to the medical image to locate different frequency sub-bands. The watermark is scrambled using one-dimensional chaotic map generator with uniform distribution modulo-one transformations for generating highly independent and uniformly distributed random chaotic sequences. A particle crypto-compression algorithm is applied for the insertion step: the scrambled watermark is inserted into the highest singular value derived from the compressed low-frequency sub-band, ensuring a delicate balance between imperceptibility and robustness. From the conducted tests and comparison of the obtained results with other techniques, we concluded that the robustness of the algorithm under various attacks was improved by the excellent value of the NC parameter, especially in the case of compression and geometric attacks.

Corresponding Author:

Daham Abderrahmane
Department of Mathematics and Computer Science, Faculty of Science and Technology
University of Tahri Mohamed Bechar
Bechar, Algeria
Email: daham_abderrahmane@yahoo.fr

1. INTRODUCTION

Telemedicine applications are experiencing growing usage owing to the swift advancements in digital imaging, information technology, and communication technologies. Medical data, encompassing medical images and patient information, is extracted and transmitted across unsecured networks linking different hospital locations, for many reasons, such as telephone diagnosis, treatment, teleconferencing between clinicians, medical consultation, distance learning, and training. Medical images might be either intentionally or unintentionally manipulated by unauthorized users [1]. The recent COVID-19 pandemic has underscored the consistent creation and online dissemination of medical images, emphasizing the urgent need for protection against unauthorized access. Medical data protection is necessary because of its vital role for patients health.

Its deterioration can be a direct or an indirect cause of serious damage to patients' health. Embedding a hidden stream of bits in a file or an image is called digital watermarking. In one hand, the medical image watermarking, confidentiality, authentication, and diagnosis are the intended purposes for inserting watermark information, including the hospital's logo, patient details, and the doctor's signature, into the medical image. The digital watermarking offers additional advantages: access control, avoidance of detachment, confidentiality, non-repudiation, indexing, saving memory and bandwidth [2]. Watermarking could be versatile in providing location sabotage, self-recovery, and verification of ownership. Even though it has its advantages, watermarking has some weaknesses; for instance, it does not hide information, neither from the image itself nor from the brand.

In the other hand, cryptography approaches protect data during transmission. The person who has the secret key and the algorithm can decrypt the data into a useful format. But after decryption, the data is no longer protected, and it is very difficult to verify its integrity and origin. This type of protection is called the "a priori" method of protection. Therefore; watermarking approaches have come as an additional protective technique to prove integrity, authenticity, and origin. After the decryption of the data, we always have the possibility to either identify if the data has been tampered with or if it is in its original form. This type of protection is called the posterior protection method [3]. The aforementioned limitations of cryptography and watermarking show that each of these approaches taken individually is not sufficient to provide a high level of security. Different approaches have been proposed to take advantage of the complementary between encryption and watermarking techniques. Watermarking and encryption methods for digital image data in this field must be entirely reversible. The original plain image data involved in cryptographic and watermarking processes should be fully recoverable, given the sensitivity of the conveyed data in medical images [4]. The exchange of databases between hospitals requires an effective transmission channel to reduce the cost of health care. Medical images are typically identified through an attached file that contains essential information. This method of identification poses a potential risk associated with intentional or unintentional data modification [5]. Depending on the link established between the message and its host, different watermarking applications have been invented as a means of securing medical images in health: i) integrity control and tamper detection: there is thus a need to prove that the images on which the diagnoses and any insurance claims are based have preserved their integrity via the insertion of signatures of the image making it possible to detect, locate and identify the nature of the modification with sometimes the possibility of reconstructing the original image [6], [7]; ii) authenticity: a critical requirement in patient records is to authenticate the different parts of the electronic patient record, in particular the images. More often an image is identied by an attached or a header which carries all the needed information (digital imaging and communications in medicine (DICOM) solution to the radiology images is well known), check its authenticity by watermarking, the unique DICOM identifier of the image or those of the patient or the acquisition modality [6]–[8]; iii) reliability and traceability of a medical image are key issues for medical data sharing, compared to the multimedia domain where copyright issues are of major concern (reliability based on the outcomes of integrity and authenticity) [2]; and iv) control of use with the concealment of access rights and patient consent, the insertion of secure links between documents. By watermarking the image with the account ID associated report, and the report with that of the image, we know which documents are linked and it becomes more difficult to falsify data [9].

In this paper a blind x-ray image watermarking scheme joint crypto-compression system is presented, the watermark is inserted in the most appropriate discrete wavlet transform (DWT) blocks which again helped the scheme in achieving high robustness by preserving the image quality. The security of watermarking is greatly improved when 1D logistic map modulation is carefully applied. Our work's primary contributions can be outlined as:

- Security: the information of watermark should be safe and difficult to tamper or forge. Tamper-detection in the watermarking system can be used to check authenticity. A crypto system with a broad chaos range is introduced for the watermark image encryption. The proposed scheme is capable of guaranteeing the security of the watermarks in the host image and preserves the integrity of the medical image. Therefore, by testing integrity, the system determines whether the watermark data has been tampered or not. Even if the embed algorithm is cracked, the attacker would never be able to restore the encrypted watermark images validly from the host image without the correct secret keys, so our scheme will be able to restore the bit which is formed due to the tampering of the watermarked compressed image under diverse types of attacks.
- Robustness: the proposed scheme combining the DWT with singular value decomposition (SVD) has high robustness, which can effectively restore all the embedded watermarks with high NC values when confronting with the threats of several typical strong attacks.
- Capacity and compression: a new algorithm joint compression-insertion is introduced into our scheme to compress the low low (LL) sub band with the good signal-to-noise ratio (PSNR) quality and the structural similarity index measure (SSIM) for pursuing high capacity and can hide a large amount of metadata secretly into the medical image. The algorithm has the capability to embed a chaotic watermark sequence

that perfectly allows retaining the most energy of the original LL subband and has a low effect on the x-ray image, so the compressed insertion technique does not affect the original image. However, the proposed chaotic maps are able to produce high-quality random numbers.

The remainder of the paper is organized as follows: section 2 introduces the basic theory method which aims to build our crypto-watermarking systems. Section 3 explains the proposed research method. The effectiveness of the proposed method is highlighted in section 4. Finally, section 5 summarizes the paper by giving concluding remarks and future works.

2. BASIC CONCEPTS

2.1. Discrete wavelet transform

A wavelet transform is a time-frequency domain analysis method that can achieve either time domain or frequency domain localization, and as the characteristics of multi-resolution analysis [10]. Using wavelet transform makes the watermarking more robust and difficult to manipulate [11]. Figure 1 is a schematic diagram of the first-level wavelet decomposition using low-pass and high-pass filters (LPF, HPF).

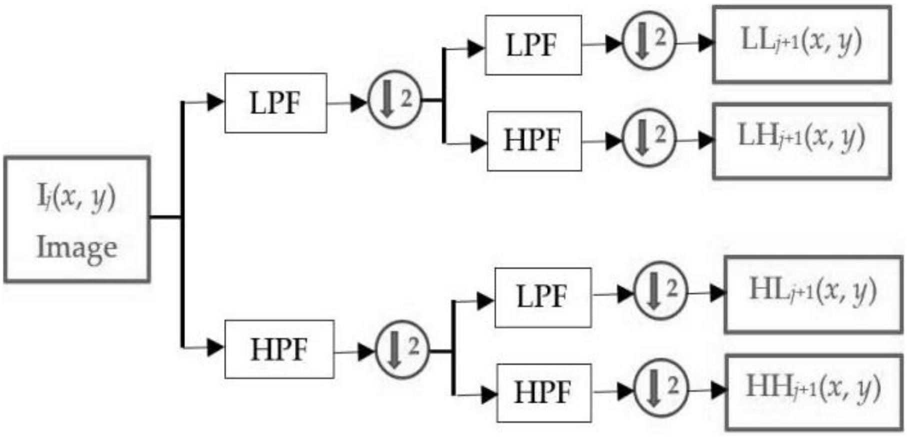


Figure 1. Three-level wavelet decomposition tree [12]

2.2. Singular value decomposition

SVD serves as a powerful numerical analysis tool for matrix analysis [13]. During the SVD transformation, a matrix can be decomposed into three matrices of the same size as the original matrix. Consider an image, denoted as I, with dimensions $M \times N$. The SVD of I is defined by (1).

$$I = USV^T \tag{1}$$

Here, S represents the singular matrix, V represents the right singular matrix, U represents the left singular matrix, and T denotes the transposition operation.

The diagonal elements of matrix S, denoted as diag ($s1$, $s2$, ... sn), adhere to the order specified by (2). Minor alterations to S result in minimal impact on the resulting image pixels [14]. Consequently, watermark information can be embedded without perceptibly affecting the visual representation of the host image.

$$s1 \geq s2 \geq \cdots \geq sn \tag{2}$$

SVD is usually used to extract the eigenvalues of images to achieve dimensionality reduction and image compression. SVD-based image watermarking schemes exhibit certain drawbacks, some of these drawbacks include: the false positive problem (FPP), and an undesirable trade-off among crucial properties, such as imperceptibility, embedding capacity, and robustness [15], [16].

2.3. Chaotic systems

Numerous image encryption algorithms have been proposed, leveraging various chaotic systems, owing to their distinct characteristics, including sensitivity to initial conditions, unpredictability, randomness, and high complexity [17]. Chaotic encryption finds application in securing medical images, safeguarding sensitive patient data, and enhancing the security of digital information in general. The pseudorandom nature which governs the concept of chaotic encryption is utilized for achieving better security when used together with watermarking techniques [18]. In our work, we use an encryption technique based specifically on a 1D logistic function. The logistic function is given by (3).

$$x_{n+1} = rx_n(1 - x_n) \tag{3}$$

Where $x_n \in (0,1)$, $r \in [0,4]$, $n = 0, 1, 2, \ldots$, both r and x_0 are initial values of the logistic function and x_n is the logistic function value with n elements of the whole number [19].

3. THE PROPOSED METHOD

The watermark encryption algorithm is made of two parts that is confusion and diffusion. The confusion is implemented by shuffling of the 1D-logistic map. After n iterations, we get n values of $x1, x2, \ldots xn$, which represent a chaotic sequence, which is a one-dimensional, called sequence A. A modulo one transformation is then applied to confine A to a unit interval. This can be a form of enhancing the security of the watermarking process by making it more resistant to unauthorized extraction or tampering.

3.1. Uniform distribution modulo-one transformation

The values generated by the chaos logistic function (sequence A) will be transformed using the threshold function $f(x)$ as depicted in (4).

$$f(X_{n+1}) = mod(X_n \times 10^3, 256) \tag{4}$$

Where n is the iteration number, the ‘mod’ operation is to ensure that its output data will be within the range of [0,255].

When we terminate the confusion step, the diffusion mechanism is undertaken by applying exclusive-or (XOR) operation to encrypt the watermark with an initial random value, as it is given by (5).

$$FEW(i) = OW(i) \oplus PSW(i) \tag{5}$$

Where $\oplus$ the XOR operation, $FEW(i)$ is the final encrypted watermark image. After this encryption process, $FEW(i)$ cannot be found through a random search. At the end, we combine all 1D matrices back into a 2D watermark matrix (w) with size of $M \times N$ using (6).

$$W(i,j) = FEW(j+1), j <= N \tag{6}$$

3.2. Joint encryption watermark compression algorithm

Mathematically, the forward model for k-space measurement involves the following steps.

- Step 1: the singular values represent the image energy [20]. Indeed, the full energy of the image I is represented in (7).

$$||I|| = trace[I^T \times I] = \sum_{i=1}^{m} \sum_{j=1}^{n} I^2\,(i,j) = \sum_{i=1}^{n} \sigma_i^2 \tag{7}$$

- Step 2: image coding, therefore, is intuitively achieved by setting the weakest singular values to zero. Choosing only the initial k values ($k \le n$) we can approximate I by (8).

$$I_k = U \times S_K \times V^T = \sum_{i=1}^{K} \sigma_i^2 \times u_i \times v_i^T \tag{8}$$

I_k represents the encoded matrix of k singular values. The product $U \times I_k$ represents the principal component of the image [21]. The corresponding energy is given by (9).

$$||I_k|| = trace\left[{I_k}^T \times I_k\right] = \sum_{i=1}^{k} \sigma_i^2 \tag{9}$$

In our watermarking system, K represents the scrambled watermark which will be inserted in the medical image, the output image represents LL sub band of the DWT transform.

3.3. Embedding process

The detailed steps of the embedding process are presented: the DWT is employed to decompose the input image into region-of-interest (ROI) and region-of-non-interest (RONI) regions to help us in selecting the appropriate coefficients to hide the watermark, as illustrated by (10).

$$[LL\ HL\ LH\ HH] = dwt2\ (I) \tag{10}$$

As the sub band (LL) encompasses high-energy components of the hoste image, and in order to avoid visible degradation of the watermarked image, it is selected to add their singular values with the ciphred watermark's values. Embedding in this subband is done by the SVD in a double step.

$$U.S1.V^{T} = SVD\ (LL) \tag{11}$$

After the decomposition of the LL sub band by SVD, three matrices are obtained. These consist of the left singular matrix U, the singular value matrix S, and the right singular matrix V. The singular value matrix S is added to the ciphered watermark W to achieve the watermark embedding operation. The embedding rules are used in this step, which are given as (12).

$$S_{new} = S + SFF \times W \tag{12}$$

The watermark is seamlessly inserted into the singular value using a single scaling factor (SFF) to obtain desirable trade-offs between imperceptibility and robustness. A scrambled watermark is reformuled and embedded into the largest singular values of S. The new singular value output will be decomposed again by SVD to generate another singular value which is used to generate a new compressed sub band LL1.

$$U1.S1.V1^{T} = SVD\ (S_{new}) \tag{13}$$

The inverse SVD with the new $S1$ is calculated as given by (14) to reconstruct a novel low frequency approximate coefficient LL1.

$$ISVD(LL1) = U.S1.V^{T} \tag{14}$$

At the end, inverse DWT is correctly applied to adequately obtain the watermarked-compressed image.

$$Watermarked\ (I) = IDWT\ (LL1, HL, LH, HH) \tag{15}$$

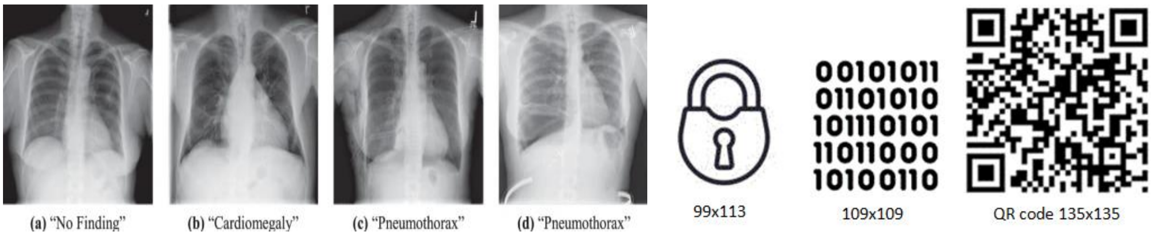
Save (S, $U1$, $V1$, SFF, key, side information) = which is equal to the clef of the algorithm. A person who does not know the secret key cannot correctly retrieve the watermark.

The extraction process does not require the original image, therefore the algorithm is blind. The extraction process will then proceed with the inverse operations executed during the insertion phase. The extracting rules are used in the following steps.

- Step 1: get watermared-compressed image;
- Step 2: the host image undergoes four-subband decomposition through the application of a DWT; DWT $(water\ marked\ image) = (new\ LL, new\ LH, new\ HL, new\ HH)$;
- Step 3: calcule DWT (new LL);
- Step 4: SVD $(newLL) = U2S2V2$;
- Step 5: clacule $S3$ from saved watermarking clef (U1, V1) with inverse SVD $S3 = U1S2V1$;
- Step 6: obtain crypted watermark from saved S, $cry\_watermark = (S3 - S)/SFF$;
- Step 7: decrypte watermark with inverse method used key and side information.

4. RESULTS AND DISCUSSION

The practical tests were be performed with processor specification intel (R) core (TM) 2 duo CPU T6500-2.1 Ghz, 2.00 GB, windows 7 ultimate 64-bit operating system. The experiment was carried out in MATLAB. X-ray images used in this experiment are taken from NIH chest x-ray dataset [22]. The size of each image is 1024×1024 with 8 bit gray-scale values, shown in Figure 2(a) and the multisize watermark logo in BMP format was considered in Figure 2(b). QR code of hospital logo (QR code) is generated by means of zxingQR code generator available at [23]. The performance of any digital image watermarking system in terms of imperceptibility, robustness, and insertion rate, is expressed using well-known metrics, that is the PSNR, the normalized correlation coefficients (NC) and the SSIM [24], [25].



(a) (b)

Figure 2. Medical and watermark images for; (a) x-ray images are employed for the analysis of the proposed scheme and (b) watermarks

4.1. Imperceptibility test

Figure 3 shows the original image, watermark images, the watermarked compressed x-ray image, and extracted watermarks. The scrambled watermark is also presented. It can be seen that the proposed method preserves the perceptual quality of the watermarked image. No degradation is noticeable on the watermarked medical image. In telemedicine, the perceptual quality of the received image is of significant importance, It also indirectly indicates that the watermarking scheme achieves improved watermark invisibility, as depicted in the same figure.

The PSNR and SSIM have been used to measure the distortion between the watermarked compressed image and the original image. To assess the robustness of the proposed scheme, the normalized correlation coefficient (NCC) is employed to examine the correlation between the original watermark and the extracted watermark. A series of tests on x-ray pixel images show that, for a watermark size 135×135 corresponding to a $SSIM = 0.99$, $PSNR \geq 47$, the same test for a watermark of size 99×113 as illustrated in Tables 1 and 2.

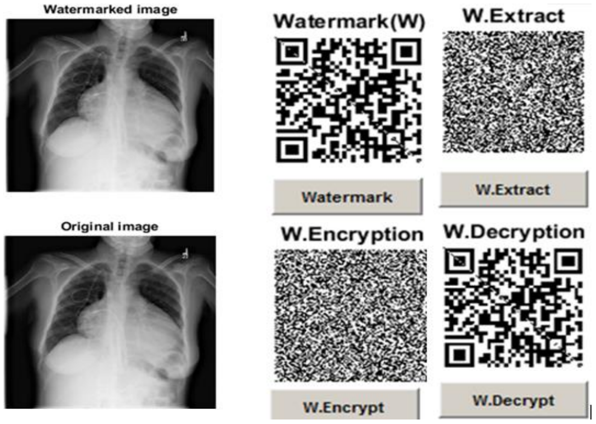


Figure 3. Results of proposed method

Table 1. Test for a watermark size 135×135

Image variable	Image1	Image2	Image3	Image4
PSNR	47.1931	49.1326	47.6024	47.2873
NC	0.9934	0.9948	0.9914	0.9930
SSIM	0.9996	0.9998	0.9998	0.9997

Table 2. Watermark size 99×113

Image	Image1	Image2	Image3	Image4
PSNR	46,916	48,895	47,602	47,287
NC	0.9963	0.9977	0.9928	0.9963
SSIM	0.9999	0. 9999	0. 9999	0. 9999

The simulation experiment shows that the NC is near 1.000 in the case of no attack. Which means that the watermark can be completely extracted without any attack; the PSNR is greater than 47 dB for the watermark sizes of 135×135 and 99×113. In general, when the PSNR is greater than 35 dB, the watermark’s invisibility is better [26]. To estimate the maximum watermark embedding capacity of the original image, the PSNR was adopted to measure the image quality of a watermarked image. Moreover, the effect of variation in the scaling factor on imperceptibility was also studied. There is a trade-off between invisibility and robustness in image watermarking. To maintain a good balance between these qualities, a suitable gain index value should be selected for embedding. The results of the PSNR values are shown in Figure 4. From the presented test, there is not much variation in PSNR values with the variation in the scaling factor (SF).

Through the analysis and discussions about the PSNR and SSIM performances, in order to evaluate the quality of the SVD compressed image, we also use the energy metric. To calculate the energy, we used the same mathematical formula as in the (7), in used to prove the joint compression insertion technique. For the watermark of size 113×99, we plot a diagram of the energy ratio of singular value, which corresponds to the ratio between the energy of the compressed image and the original image. The obtained experimental results are shown in Figure 5.

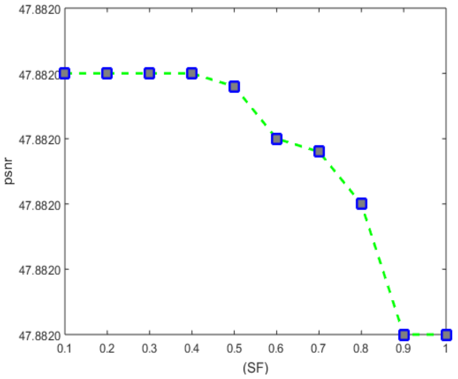


Figure 4. PSNR of tested images

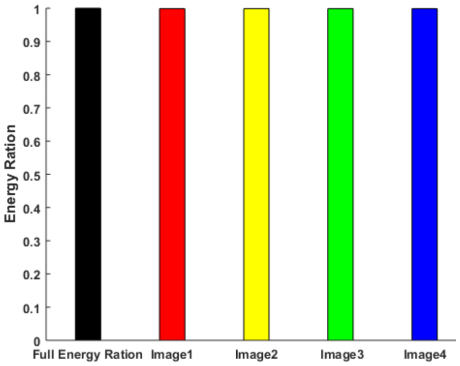


Figure 5. Energy ratio of tested images

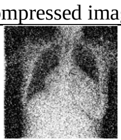
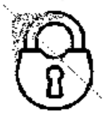
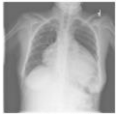
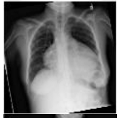
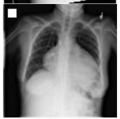
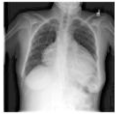
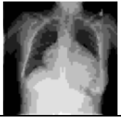
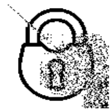
The energy metric is also very accurate and could overcome the weaknesses of SSIM and PSNR. As shown in the graph, 99.89% of the energy is restored (for an average of 4 images), so we recovered almost the same singular value. We can conclude that the singular values of the x-ray image have very good stability, when the encryption watermark is added to the x-ray image, the singular values do not change significantly. Therefore; we can state that the metrics are very precise with regard to SSIM and PSNR.

4.2. Robusteness test

The watermark should be robust against attacks. To investigate the robustness of the algorithm, the watermarked compressed image is subjected to various types of attacks; the following attacks were applied to the watermarked compressed x-ray image: gaussian noise, sharpening, brighness, cropping, and jpeg compression. Detailed results of the obtained NC and PSNR are summarized in Table 3.

Additive white gaussian noise (AWGN) is one of the most common types of noise, and it is responsible for the degradation of the image quality. Noise is generated from several natural sources, for example, electronic sensors. AWGN follows a normal (gaussian) distribution with a zero mean and it is additive in nature. The speckle noise is the most common noise in medical images and it is not easy to remove using the standard denoising methods. To ensure robustness against noise attacks, the algorithm is tested against additive white gaussian noise (0.05) and speckle noise (0.001; SP). From the experimental results, it can be seen that the extracted watermark is very clear, which indicates that the system is very robust to this kind of attack.

Table 3. Robustenesse test

Attacks	Attacked watermarked compressed image	PSNR	NC	Recovered watermark
Gaussian noise AWGN (density=0.05)		33.8758	0.9748	
Brightness		39.1731	0.9921	
Rotation 5		39.4272	0.9928	
Cropping		30.167	0.9933	
Jpg quality 50% size of attacked image12.6 K		30.4888	0.9770	
Jpg quality 1% size of attacked image 3.75 K		15.5673	0.6833	

In the case of a brightening attack on the watermarked image; the image is still clear, which shows that the robustness of this attack is relatively strong. The clarity of the watermark is maintained effectively, even in the presence of potential attacks like noise, cropping, and brightening. It is very common to carry out a darkening attack on the watermarked image. The darkening of the image means that the color scale of the image has changed. Such an attack is very common, but our system resists to this attack and cannot cause substantial damage. Although the watermarked image is darkened, the watermark seems unaffected, the extracted image is still clear, and the decrypted watermark is exactly the same as the original image, which shows that the robustness to this attack is relatively strong.

Despite the contrast-increasing attack on the watermarked compressed image, the image is still clear, which shows that the robustness against this attack is relatively strong. We carry out the contrast reduction attack on the carrier image, and we notice that the image is still clear, which shows that the robustness to this attack is relatively strong as well. The results of the proposed algorithm under compression attacks give the best correlation between the original and extracted watermark. The algorithm only uses the largest singular value and can extract the watermark blindly; in order to embed watermark image, LL subbands were chosen. It enables us to achieve greater robustness against a compression attack, where high frequencies in the image are deleted. The results show that even with a significant attack that removes part of the watermarked image, the mark may still be properly extracted with a very satisfactory quality. Cropping attack is the most common type of attack. Robustness against cropping attacks is a crucial key to evaluate validity of a watermarking system [27]. The watermark extracted from the partially cropped watermarked image is almost the same as the original image, indicating that the image is relatively recoverable with a good NC.

To demonstrate the effectiveness of the proposed method, comparison with similar work for x-ray images watermarking are presented in Table 4. The symbol '/' means that the NC values were not reported for these attacks. As illustrated in Table 4, we can easily deduce that the NC results of the proposed scheme are near-ideal as compared to the other reported techniques, which indicate the successful watermark extraction with minimal distortions. This necessary measure was appropriately applied when comparing the originally inserted mark with the mark extracted from the attacked watermarked compressed image.

While comparing our method to similar recent research works for x-ray image watermarking shown in Table 4, the first thing that we can deduce is that the proposed method on the average gives an $NC = 0.96$ which is more robust than that of all reported methods, as it succeeded in overcoming all attacks with a clear difference than in [28] which average $NC = 0.91$. For sharpening and histogram equalization attacks, our scheme and those in [28] and [29] perform much more better than the others. A cropping attack removes a part of the image and replaces it with white or black color, however, an attacker may replace the cropped part with a meaningful object to disguise malicious behavior, the information of the watermark should be safe and difficult to tamper or forge. The experimental results indicate that by improving the robustness with respect to the cropping, our approach performs better than all other methods when the cropping attack is around 50%, keeping in mind that extraction of the watermark does not necessitate the presence of the original image in our method. So, our algorithm has better robustness to resist the cropping attack than all methods. The main objective of our method is to improve robustness against geometric and compression attacks where the image authentication and tampering detection are critical for the medical field. Through previous experiments, we were able to extract the watermark clearly, although jpg quality was 1% (Table 3).

Table 4. Comparing the robustness of our watermarking approach with recent similar works

	Thanki *et al*. [28]	Zermi *et al*. [29]	Alshanbari [30]	Aparna and Kishore [31]	Proposed
Histogram equalization	0.9689	0.9713	/	/	0.9940
Gaussian noise (0, 0.01)	0.7129	0.9604	0.7941	0.6027	0.9922
Sharpening (0.2)	0.9408	0.9875	0.7321	/	0.9789
Average filtering (3×1)	0.9538	0.9665	0.7287	0.7892	0.9815
Cropping (50%)	0.7895	0.7505	/	0.7505	0,8349
JPEG compression(30)	0.7374	0.8832	0.751	/	0.9750
Salt and pepper noise (2%)	0.7054	0.9221	/	0.6004	0.9670

5. CONCLUSION

This paper introduces a blind x-ray image watermarking scheme within a joint crypto-compression system. The scheme involves the insertion of a multisize watermark into the most suitable DWT-SVD blocks. This strategy contributes to achieving high robustness while preserving the overall image quality. The safety of watermark is greatly improved when 1D logistic map modulation is carefully applied. To improve the performance of watermark recovery, a chaotic diffusion was added before compression. The security level was increased by chaotic scrambling and XOR operations. The experimental results reveal that even after undergoing various attacks, the extracted watermarks remain visually recognizable, and all recovered watermarks closely resemble the original watermark. The average NC value is greater than 0.9, which is considered a good result when compared to other related techniques. We also obtained a PSNR of a compressed-watermarked image equals approximately to 47 dB. Therefore, we can conclude that our method is robust against different simulated attacks, especially in the case of the compression and geometric attacks. In addition, the evaluation results exhibit the best results of the proposed technique for the fidelity metric of the x-ray image with the compressed watermarked image, due to limited bandwidth and preserved their integrity. We also use the energy metric which is very accurate and could beat the weaknesses of SSIM and PSNR. The proposed method inserts the watermark and compresses the image at the same time, it can be used in high demanding fields. A real time implementation of the proposed scheme might be performed in futur work.

REFERENCES

[1] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Computer Science Review*, vol. 27, pp. 45–60, 2018, doi: 10.1016/j.cosrev.2017.11.003.

[2] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of Digital Imaging*, vol. 26, no. 2, pp. 326–343, Apr. 2013, doi: 10.1007/s10278-012-9527-x.

[3] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, pp. 891–899, Sep. 2012, doi: 10.1109/TITB.2012.2207730.

[4] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 167, p. 107286, Feb. 2020, doi: 10.1016/j.sigpro.2019.107286.

[5] K. Amine, K. Redouane, and M. Bilel, "A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine applications," *Multimedia Tools and Applications*, vol. 82, no. 5, pp. 7901–7915, 2023, doi: 10.1007/s11042-022-13649-7.

[6] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Processing: Image Communication*, vol. 47, pp. 160–169, 2016, doi: 10.1016/j.image.2016.05.021.

[7] C. C. Lin, T. L. Lee, Y. F. Chang, P. F. Shiu, and B. Zhang, "Fragile Watermarking for Tamper Localization and Self-Recovery Based on AMBTC and VQ," *Electronics (Switzerland)*, vol. 12, no. 2, p. 415, Jan. 2023, doi: 10.3390/electronics12020415.

[8] A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: a survey," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30165–30197, Aug. 2021, doi: 10.1007/s11042-020-08801-0.

[9] A. Anand and A. K. Singh, "Hybrid Nature-Inspired Optimization and Encryption-Based Watermarking for E-Healthcare," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 2033–2040, 2023, doi: 10.1109/TCSS.2022.3140862.

[10] K. Wirsing, "Time Frequency Analysis of Wavelet and Fourier Transform," in *Wavelet Theory*, IntechOpen, 2021. doi: 10.5772/intechopen.94521.

[11] L. Wang and H. Ji, "A Watermarking Optimization Method Based on Matrix Decomposition and DWT for Multi-Size Images," *Electronics (Switzerland)*, vol. 11, no. 13, 2022, doi: 10.3390/electronics11132027.

[12] A. Daham, M. Ouslim, Y. Hafed, and W. Djaber, "Robust Watermarking Method to Secure Medical Images Applied to Ehealth," in *2022 13th International Conference on Information and Communication Systems, ICICS 2022*, IEEE, Jun. 2022, pp. 379–385. doi: 10.1109/ICICS55353.2022.9811160.

[13] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 1002–1013, 2009, doi: 10.1016/j.csi.2008.09.031.

[14] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "A New Chaotic Image Watermarking Scheme Based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020, doi: 10.1109/ACCESS.2020.2978186.

[15] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "An FPP-resistant SVD-based image watermarking scheme based on chaotic control," *Alexandria Engineering Journal*, vol. 61, no. 7, pp. 5713–5734, Jul. 2022, doi: 10.1016/j.aej.2021.10.052.

[16] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information (Switzerland)*, vol. 11, no. 2, p. 110, Feb. 2020, doi: 10.3390/info11020110.

[17] N. Wang, C. Li, H. Bao, M. Chen, and B. Bao, "Generating Multi-Scroll Chua's Attractors via Simplified Piecewise-Linear Chua's Diode," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 12, pp. 4767–4779, Dec. 2019, doi: 10.1109/TCSI.2019.2933365.

[18] Y. Wu, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, p. 013014, Mar. 2012, doi: 10.1117/1.jei.21.1.013014.

[19] D. Rosiyadi, S. J. Horng, P. Fan, X. Wang, M. K. Khan, and Y. Pan, "Copyright protection for E-government document images," *IEEE Multimedia*, vol. 19, no. 3, pp. 62–73, 2012, doi: 10.1109/MMUL.2011.41.

[20] L. Kocarev and S. Lian, "Chaos-Based Cryptography: Theory, Algorithm and Applications," *Berlin: Springer-Verlag*, 2011.

[21] R. A. Sadek, "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges," *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 7, pp. 26–34, 2012, doi: 10.14569/ijacsa.2012.030703.

[22] Kaggle, "NIH Chest X-ray Dataset | Machine Learning Datasets", [Online]. Available: https://datasets.activeloop.ai/docs/ml/datasets/nih-chest-x-ray-dataset/

[23] Zxing, QR code generator from the ZXING Project, http://zxing.appspot.com/generator (accessed Sep. 5, 2012).

[24] K. Sehra *et al.*, "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.2021.3079319.

[25] A. Hata *et al.*, "Effect of Matrix Size on the Image Quality of Ultra-high-resolution CT of the Lung: Comparison of 512 × 512, 1024 × 1024, and 2048 × 2048," *Academic Radiology*, vol. 25, no. 7, pp. 869–876, 2018, doi: 10.1016/j.acra.2017.11.017.

[26] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7491–7513, 2020, doi: 10.1007/s11042-019-08423-1.

[27] H. Li, Z. Li, Z. Du, and Q. Wang, "Digital Image Watermarking Algorithm Using the Intermediate Frequency," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 14, no. 4, p. 1424, 2016, doi: 10.12928/telkomnika.v14i4.4064.

[28] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1366–1379, 2017, doi: 10.1016/j.jestch.2017.06.001.

[29] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "A lossless DWT-SVD domain watermarking for medical information security," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 24823–24841, 2021, doi: 10.1007/s11042-021-10712-7.

[30] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools and Applications*, vol. 80, no. 11, pp. 16549–16564, 2021, doi: 10.1007/s11042-020-08814-9.

[31] 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, doi: 10.1049/iet-ipr.2018.5288.

BIOGRAPHIES OF AUTHORS

Daham Abderrahmane is associate professor, Department of Computer Science, Bechar University, April 2012-present. Engineer in Computer Science, Department of Computer Science, (CUB-Algeria), 2001-2006. Magister option: computer vision and pattern recognition in intelligent systems laboratory (USTO-Algeria) 2007-2011. Fields of research interest is intrusion detection system, telemedicine systems design (EHR, EMR, EPR), medical image processing, cryptography, watermarking, steganography, and internet of medical things (IoMT). He can be contacted at email: daham_abderrahmane@yahoo.fr.

Ouslim Mohamed born in 1961, received the Engineers Degree in Electronics, USTO in 1985. He received the master's degree in Computer Engineering from the Ohio State University (USA) in 1989 and the Ph.D. degree in Electrical and Electronic Engineering from the University of Nottingham (UK) 1997. He is currently a professor in Department of Electronics at Université De Sciences Et Technologied'oran-MB and a member of Microsystems and Embedded Systems Lab (LMSE). His research interests include wireless sensor networks, biometrics, image processing, and embedded systems. He can be contacted at email: ouslim@yahoo.com.