Hindawi
Scientific Programming
Volume 2021, Article ID 5559191, 22 pages
https://doi.org/10.1155/2021/5559191

Research Article

Crypto-Watermarking Algorithm Using Weber's Law and AES: A View to Transfer Safe Medical Image

Sondes Ajili,[1] **Mohamed Ali Hajjaji**,[1,2] **and Abdellatif Mtibaa**[1]

[1]*Université de Monastir, Laboratoire d'Electronique et de Microélectronique, Monastir LR99ES30 5000, Tunisia*
[2]*Higher Institute of Applied Sciences and Technology, University of Sousse, Sousse, Tunisia*

Correspondence should be addressed to Mohamed Ali Hajjaji; daly_fsm@yahoo.fr

Received 15 January 2021; Revised 1 May 2021; Accepted 6 August 2021; Published 16 August 2021

Academic Editor: Sebastiano Fabio Schifano

Copyright © 2021 Sondes Ajili et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose a novel method for medical image watermarking in the DCT domain using the AES encryption algorithm. First, we decompose the original medical image into subblocks of 8×8. Besides, we apply the DCT and the quantization, respectively, to each subblock. However, in the DCT domain, an adequate choice of the DCT coefficients according to the quantization table in the middle frequencies band is performed. After that, we embed the patient's data into the corresponding medical image. The insertion step is carried out just after the quantization phase. To increase the robustness, we encrypt the watermarked medical images by using the AES algorithm based on chaotic technique. Arnold's cat map is used to shuffle the pixel values, and a chaotic Henon map is utilized to generate an aleatory sequence for the AES algorithm. The shuffled watermarked image is encrypted using the modified AES algorithm. The constant of Weber is used to choose the suitable visibility factor for embedding a watermark with high robustness. To control identification, after application of attacks, we use the serial turbo code for correction of the watermark to recover the data inserted. The average peak signal-to-noise ratio (PSNR) of the medical images obtained is 61,7769 dB. Experimental results demonstrate the robustness of the proposed schema against various types of attacks.

1. Introduction

Recently, the rapid development of communication technologies and multimedia resulted in the transmission of great amount of multimedia data (image, audio, videos, etc.). Sometimes this multimedia information is sensitive in nature such as medical imaging. Then, it must be protected against modification and reproduction. Therefore, it is essential to find an efficient method able to protect sensitive information from unauthorized use. Typical mechanisms given these security aspects are cryptography [1, 2] and watermarking [3, 4].

The watermark digital image, which deals with the incorporation of special data (watermark) in a roof deck, is the most viable solution to the problems of intellectual property and content authentication. The main requirements of a watermarking technique are imperceptibility, robustness, and security [5, 6].

Digital watermarking techniques are classified in many ways [7–10] but one of the most important classifications of a watermarking system is based on whether the watermark is embedded directly by manipulating pixels of the cover image or by transforming the cover image into the frequency domain by various transformation tools (FFT, DCT, DWT, and KLT) and then embedding the watermark by modifying various frequency coefficients. The former method of embedding the watermark is referred as spatial domain watermarking, while as the latter is known as transform domain watermarking. Spatial domain embedding is very simple, computationally efficient, and has high embedding capacity [11]. However, the spatial domain-based watermarking techniques are not robust to most of the image processing operations. Commonly used transform domain techniques are discrete cosine transform (DCT), discrete wavelet transform (DWT), and Karhunen Loeve transforms (KLT) [12–14].

Conventionally, cryptographic solutions are used to enhance the security of multimedia data [15–17]. In cryptography, the message is scrambled so that it cannot be revealed to third parties malicious. An emerging trend for information security focuses on the combination of cryptographic and steganographic approaches [17]. Steganography differs from cryptography in many ways; among them, the data are not disguised in an unreadable form; therefore, they attract less attention from the opponent. Currently, steganography attracts the attention of researchers, which is growing for various applications. In a typical image-based steganography system, the content of interest is seamlessly inserted into the cover images and then transmitted to the destination without compromising its security and robustness.

In this context, a novel schema of the medical image using cryptography and watermarking algorithm in the DCT domain is showed, which uses constant's Weber to locate the suitable value of the visibility factor for embedding the watermark. The watermark is integrated in the middle frequencies' band. Cryptography has been projected as a complementary mechanism to improve the security of medical images. Experiments and analyses results show that the watermarking method is robust to several attacks.

This manuscript is organized as follows. Section 1 presents the previous works related to watermarking and encryption algorithm. Section 2 is focused to describe the DCT domain, the AES encryption, and the constant of Weber. In Section 3, we detail the proposed approach. Section 4 shows the experiments results of our method and analyses the robustness of this technique against different attacks in Section 5. And, finally, we conclude our paper.

2. Literature Survey

In literature, diverse methods have been tried out for image digital watermarking based on discrete cosine transform. In [18], the authors presented a reversible watermarking algorithm based on integer DCT (IntDCT) for medical image protection. In this paper, the first step consists of dividing the original medical image into nonoverlapping blocks. After that, apply the IntDCT on each block. Calculate the energy of each block, select the blocks adequate with the specific threshold, and create the index of adequate blocks. The watermark image is transformed into the binary sequence by using zigzag scan. Finally, embed the secret message into the selected blocks.

In [19], Shang and Kang have proposed a robust watermarking system for medical image security based on DCT and Arnold transformation. Firstly, this method encrypts the watermark data by using the scrambling technology as pretreatment. Thereafter, apply the DCT transform on the original image. Extract a visual feature vector through graphic DCT transformation. Then, the visual feature vector is combined with the encrypted watermark to generate a binary series by using the hash function. The binary sequence is regarded as the key to exact correctly the watermark.

In [20], the authors have proposed a novel approach of the biomedical watermarking method which combines cryptography with frequency domain watermarking. This algorithm permits to embed EPR (electronic patient records) in the original image by using DCT watermarking and RSA encryption algorithm. The first step consists of converting the EPR to cipher text through the RSA algorithm and then transformed to a binary message to form the watermark. After that, the watermark is converted into its corresponding frequency domain component by using DCT. This information is saved at the higher portion of the original image along with the ciphered keys. On the contrary, the ROI (region of interest) of the infected region is detected by using a contour detection algorithm and combination of region growing. Finally, this binary image (obtained ROI) is transformed using DCT to create another watermark data, and it is saved at the lower part of the original image.

Chittaranjan et al. [21] have proposed a double encryption system in the DCT domain. This algorithm has been used cross-chaos map and Arnold cat map for encrypting the watermark image twice. After that, the encrypted image is embedded into the DCT domain. The same authors have also proposed in [22] a comparative analysis of the watermarking system in DCT and DWT domain using enhanced playfair cipher. The proposed preprocessing stage is implemented in diverse transform domain techniques to embed ownership information in the original media. The encrypted image is formed by applying modified playfair cipher to the watermark image which will be further hidden in cover media using DWT and DCT.

The authors in [23] proposed a new blind digital watermarking system based on DCT. This algorithm consists of spreading the original watermark to a number which is more faithful to the image. Next, preprocess the original image by applying the first level of DCT transform to the image and select a portion of transform coefficients. After that, apply the second level of DCT transform to the coefficient image and choose the image feature vector. Finally, embed the spread watermark vector into the image feature vector.

In [24], the authors proposed a blind image watermarking method based on DCT with spread spectrum technique. This method divides the original image into nonoverlapping blocks. Then, each block is changed into the frequency domain by using DCT transform. The medium band of coefficients in the frequency domain of each block is used to embed the watermark.

In [16], the authors proposed an approach based on the new left data mapping (LDM), pixel repetition method (PRM), RC4 encryption, and checksum calculation. The PRM is used to scale the image. Binary secret data is encrypted using the RC4 encryption algorithm; then, the encrypted data is grouped into 3-bit blocks and converted to decimal equivalents. Before integration, these decimal digits are coded by LDM. A fragile logo is integrated into the cover images in addition to the EHR to facilitate early detection of tampering.

The paper in [25] presented two different watermarking algorithms for medical images in the transform domain. In first technique, a digital watermark and electronic patient record have been integrated in both regions, region of interest and region of noninterest. In the second technique, the region of interest is kept intact for remote diagnosis purposes and the region of noninterest is used to mask the digital watermark and the EPR. In either algorithm, a discrete cosine transform based on an 8×8 block was used.

In [26], the authors proposed a medical image watermarking system based on discrete wavelet transform. Before the incorporation of the watermark, a medical image is subjected to a comprehensive DWT. The Haar wavelet was used for this purpose. The LH subband has been divided into 8×8 blocks. The coefficients of each 8×8 block (LH) are compared and, if necessary, swapped to incorporate the binary digit "1" or "0."

3. The Fundamental Theory

This part is a fundamental theory for the selected tools: DCT, Weber's constant, AES, Arnold's cat map, and key generation using the chaotic Henon map which are used in this work.

3.1. The Discrete Cosine Transform (DCT). Discrete cosine transform transforms the space domain into its frequency components. The DCT decomposes the image into various frequency bands. The DCT decomposes the image into various frequency bands. Data hiding may be added into low, mid, or high frequency. Frequency bands of 8×8 block of DCT transform is illustrated in Figure 1. The secret data is hidden in middle band frequency of DCT coefficient blocks. The formulae for calculating 2D DCT in the watermarking system is defined by equation (1) and inverse 2D DCT transformation is given by equation (2):

$$\begin{cases} c(u,v) = \dfrac{1}{4}\alpha(u)\alpha(v)\displaystyle\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\dfrac{(2x-1)\pi u}{2N}\cos\dfrac{(2y-1)\pi v}{2N}, \\ \alpha(u) = \alpha(v) = \begin{cases} \sqrt{\dfrac{1}{N}}, & \text{for } u \text{ and } v = 0, \\ \sqrt{\dfrac{2}{N}}, & \text{for } u \text{ and } v = 1, 2, \cdots N-1, \end{cases} \end{cases} \tag{1}$$

$$\begin{cases} f(u,v) = \dfrac{1}{4}\alpha(u)\alpha(v)\displaystyle\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} u(x,y)\cos\dfrac{(2x-1)\pi u}{2N}\cos\dfrac{(2y-1)\pi v}{2N}, \\ \alpha(u) = \alpha(v) = \begin{cases} \sqrt{\dfrac{1}{N}}, & \text{for } u \text{ and } v = 0, \\ \sqrt{\dfrac{2}{N}}, & \text{for } u \text{ and } v = 1, 2, \ldots, N-1. \end{cases} \end{cases} \tag{2}$$

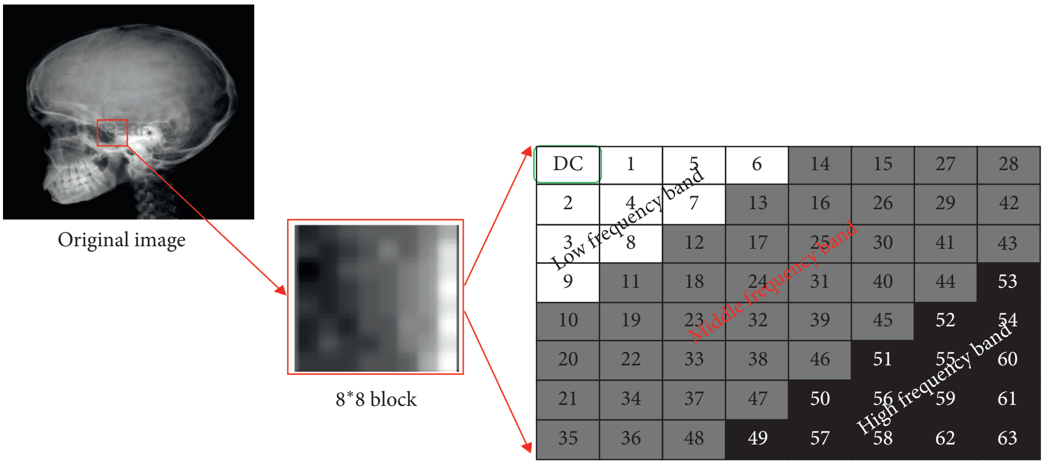
3.2. Weber's Constant. Weber's constant has been applied for watermark authentication by Ekta and Suneja [27]. Weber declared that the ratio of augmentation threshold to the intensity is constant [28]. Chen et al. [29] have been using Weber's law to describe Weber's descriptor. It is based on two components: orientation (λ) and differential excitation (χ) of a pixel. To calculate the differential excitation value χ of the pixel (x_i, y_j) possessing intensity $f(x_i, y_j)$, its difference is computed with intensity of the eight neighbours (shown in Figure 2). Then, the ratio of differences relative to the intensity of current pixel (x_i, y_j) is assessed. The inverse tangent is next applied on this ratio, as given in the following equation:

$$\chi(x_i, y_j) = \mathrm{arc}\,tan\left(\sum_{a=-1}^{1}\sum_{b=-1}^{1}\frac{\left(f\left(x_i+a, y_j+b\right) - f\left(x_i, y_j\right)\right)}{f\left(x_i, y_j\right)}\right). \tag{3}$$

The value of the differential excitation $\chi(x_i, y_j)$ is comprised between $[-\pi/2, \pi/2t]$. If the numerator together with denominator in this ratio assesses to zero, in that case, $\chi(x_i, y_j)$ is taken as zero. The value of the differential excitation $\chi(x_i, y_j)$ may be negative or positive. Indeed, The value of differential excitation $\chi(x_i, y_j)$ is positive, if the intensity of the current pixel is lower than the intensities of the neighbours of current pixels.

Diverse other medical images are used in the approved experiments in the watermarking process, with diverse classified zones' numbers as exposed in Figure 3. These figures illustrate medical images with textures. Figure 3(b) divided into four different zones where the watermark can be embedded with several different visibility factors. Figure 3(d) is partitioned into five zones. In each image, the value of the visibility factor, where the watermarks have to be embedded, changes with different zones.

3.3. Arnold's Cat Map. In the 1960s, Vladimir Arnold discovered two-dimensional invertible chaotic maps. The effect of the map was proved using a cat image, which is why it is called Arnold's cat map [30]. In the matrix form, Arnold's cat map is defined as follows:



DC	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Figure 1: Three frequency bands of 8 × 8 DCT blocks.

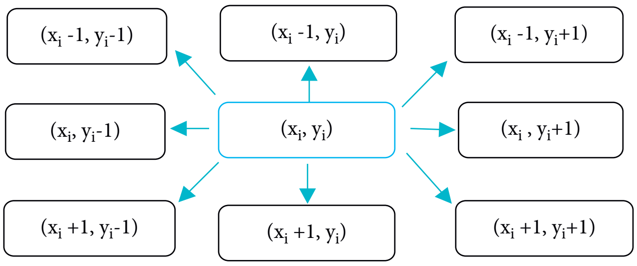


Figure 2: Neighbouring order of pixel (x_i, y_j).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & c\,d+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \operatorname{mod}(M), \tag{4}$$

where d and c are positive integer constants and $n = 0, 1, 2, 3, \ldots$. For a medical image, (x_n, y_n) is an actual pixel value for the medical image at the specified position and (x_{n+1}, y_{n+1}) is the transformed pixel value for the medical image. After execution of N iterations, there are T positive integers such that $(x_{n+1}, y_{n+1}) = (x_n, y_n)$. The period T depends on the size of the input medical image and parameters d and c. Arnold's cat map is very efficient for pixel value mixing since it is a simple transformation using a single mode operation. Nevertheless, it has some security weakness, and an attacker can reproduce the original information by iterating the map repeatedly. Therefore, the AES algorithm and the chaotic key generator have been applied to realize higher level diffusion properties and confusion in the encryption.

3.4. Key Generation Using Chaotic Henon Map.

In 1978, Henon discovered a discrete-time dynamical scheme that exhibited chaotic behavior [31], which is described as

$$x_n = 1 + \lambda\left(x_{n-2} - x_{n-3}\right) + a x_{n-2}^2. \tag{5}$$

It depends on two primordial parameters: λ and a. The pseudorandom behavior of the Henon map has values of $\lambda = 0.3$ and $1.07 \le a \le 1.09$. In our work, the concept of exploitation of a key generator founded on a Henon chaotic map is presented to improve the encryption quality of the AES algorithm without changing the actual implementation. This results in higher confusion and diffusion properties with efficiency and expectable performance. The proposed key generator produces variable length secret keys of diverse sizes (128, 192, and 256 bits), as supported in the AES block encryption algorithm. The single secret key, K_s, is defined as

$$K_s = b_1, b_2, b_3, \ldots, \frac{b_r}{8}. \tag{6}$$

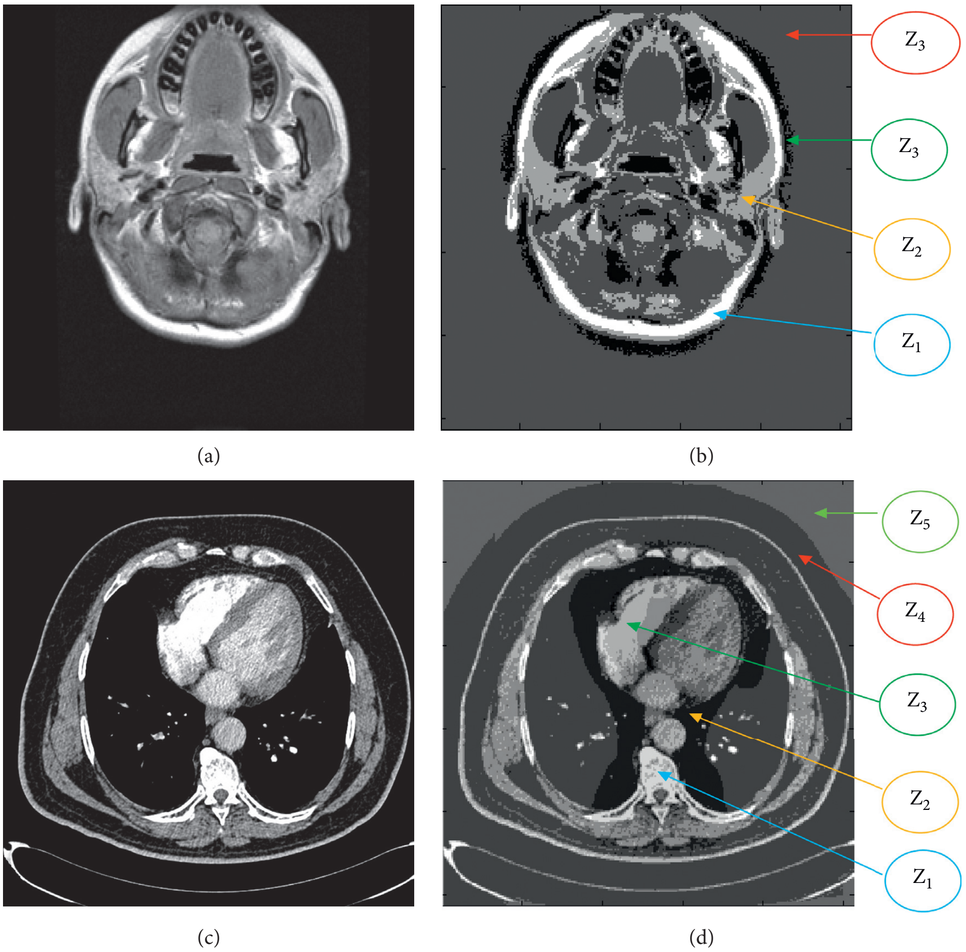
Here, r is the size of key K_s in bits. A secret key (with a length of 128, 192, or 256 bits) is suitable and long enough.

3.5. AES (Advanced Encryption Standard).

AES is one of the most known encryption systems for data protection. Invented in 1998 by Joan Daemen and Vincet Rijmen and proved in 2000 by NIST [32–34], AES encryption has been widely deployed thanks to its high performance. In effect, AES is reliable which offers high level security, high robustness, wide portability, fast, and easy to implement. Recently, many encryption systems have previously been developed founded on AES for data security.

Different extensions have been established for the AES algorithm by diverse researchers. Nowadays, the AES algorithm is capable of being modified or used to support variable length information and keys. AES tolerates a 128, 192, or 256 bits data length that can be separated into 4 operation blocks organized in 4 × 4 matrix of bytes array (called a state). For encryption and decryption processes, the key and data blocks are passed through N_r rounds ($N_r = 10$, 12, or 14), which are extracted from key size K of length ($N_k = 4$, 6, or 8, respectively) in our approach, and $N_c = 4$ characterizes the number of columns in a state matrix depending upon the block size (equal to 32 bits).

As shown in Figure 4, the AES encryption method is defined as numerous iterative transformation rounds (called a round function). Transformation rounds are created on the key size, which is utilized to calculate the number of rounds (N_r rounds). The encryption method converts the information blocks into unreadable information blocks. The round function consists of numerous suboperations called



(a) (b)

(c) (d)

Figure 3: (a) Original medical images. (b) Four classified zones. (d) Five classified zones.

AddRoundKey, ShiftRows, ByteSub, and MixColumns transformation. The round function is applied after the initial AddRoundKey operation, which depends on the secret key. Correspondingly, the decryption method uses the same order to transform the encrypted information blocks into the actual information blocks using the same secret key.

4. Proposed Approach

In this section, we explain the proposed algorithm for embedding the totality of the patient's data in a medical image. Before the insertion, the patient's data undergoes many steps with the aim at increasing the level of integration and better ensuring its extraction after applying different attacks. The insertion procedure is done by adding to the image frequency components, proper to the original image data related to the patient. Equation (7) explains the integration procedure of the watermark on the image frequency coefficients:

$$\sigma'_i = \sigma_i + \alpha \times W_i, \tag{7}$$

with σ_i being the i^{th} old coefficient to support the watermark, σ'_i being the i^{th} new watermarked coefficient, W_i being the i^{th} bit to hide, and α being named often as the visibility factor. Indeed, α is an important factor in the watermarking system. If this factor is big, we win in terms of the robustness; however, we lose in terms of imperceptibility and vice versa.

The global proposed schema process is shown in Figure 5.

4.1. Preparation of the Watermarking Space. In our algorithm, we propose to use the frequency transformed domain on the original medical image for integration of the watermark. First, the original image is divided on subblocks of 8×8 pixels. Second, applying the discrete cosine transform on each subblock of 8×8 pixels to obtain a subblock of 8×8 coefficients. Third, the quantization step is applied to a different transformed block. Each quantized transformed block includes three parts: the first part contains the low frequency, the second encloses the midrange frequency, and the latest represents the high frequency. It is interesting to choose a medium frequency band providing good compromise between minimal degradation of the image quality and maximum resistance to several attacks. On the contrary, we apply Weber's low to the original medical image in order to obtain the suitable visibility factor of each region of the image. Our essential goal consists of enhancing the robustness of our proposed algorithm.

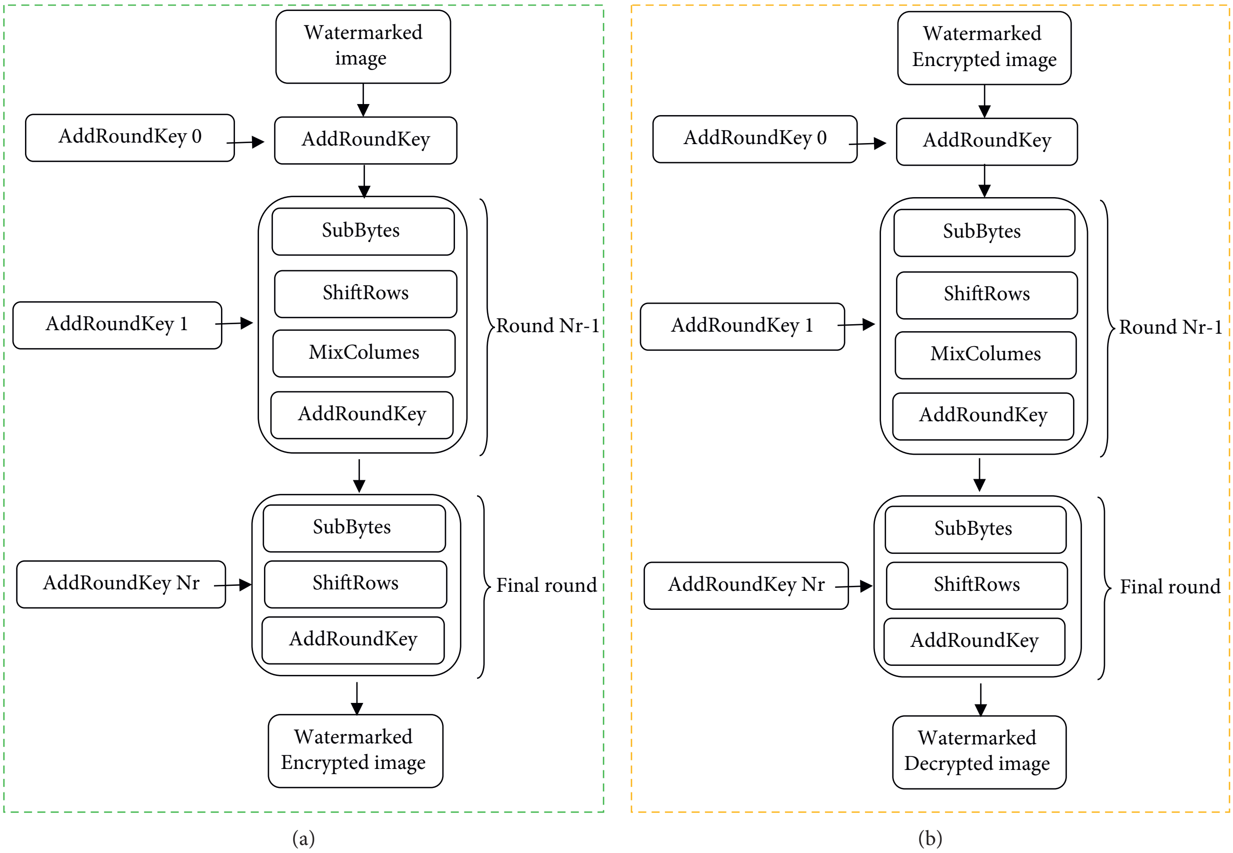


Figure 4: (a) AES encryption process. (b) AES decryption process.

Figure 6 presents the different stages for the preparation of the space where the watermark will be hidden.

4.2. Preparation of the Watermark. The computation steps of the preparation of watermark (information inserting) are realized as follows.

Step 1: generate a signature (sized of 160 pixels) detained by the hospital center; the principal aim is to control the authenticity of the data of patient. The SHA-1 (Secure Hash Algorithm) is useful [35].

Step 2: converting the rest of the patient's data into a binary sequence.

Step 3: the sequence and the signature are concatenated to get the message. This message will be inserted in the transformation domain of the image.

Figure 7 summarizes the diverse stages to follow to prepare the watermark to be inserted.

4.3. The Embedding Process. Our proposed approach is based on the discrete cousins transform for hiding the watermark. The embedding process, as shown in Figure 8, is described as follows.

Step 1: by using Weber's low, select the suitable visibility factor α_i of each subblocks sized 8×8.

Step 2: the quantization step is applied on each transformed subblock sized 8×8.

Step 3: select the maximum value located in the midrange of the quantified transformed subblocks.

Step 4: the i^{th} value of the binary message W is multiplied by the visibility factor α_i related to the subblock to be watermarked. Then, the result of multiplication is added with the maximum value of the quantified transformed subblock X_i to obtain the watermarked subblock Y_i.

Step 5: perform the inverse discrete cousins transform to obtain the watermarked image.

Step 6: apply the AES algorithm encryption.

4.4. Encryption Process. The encryption step consists of a combination of the AES and chaotic techniques in goal to enhance the security of the proposed method. The desired results have been realized in three steps:

Step 1: shuffling using Arnold's cat map

Step 2: key generation using a chaotic Henon map

Step 3: running the encryption operation using the AES algorithm

The proposed encryption process supports variable length keys (128, 192, and 256 bits). It takes the employer

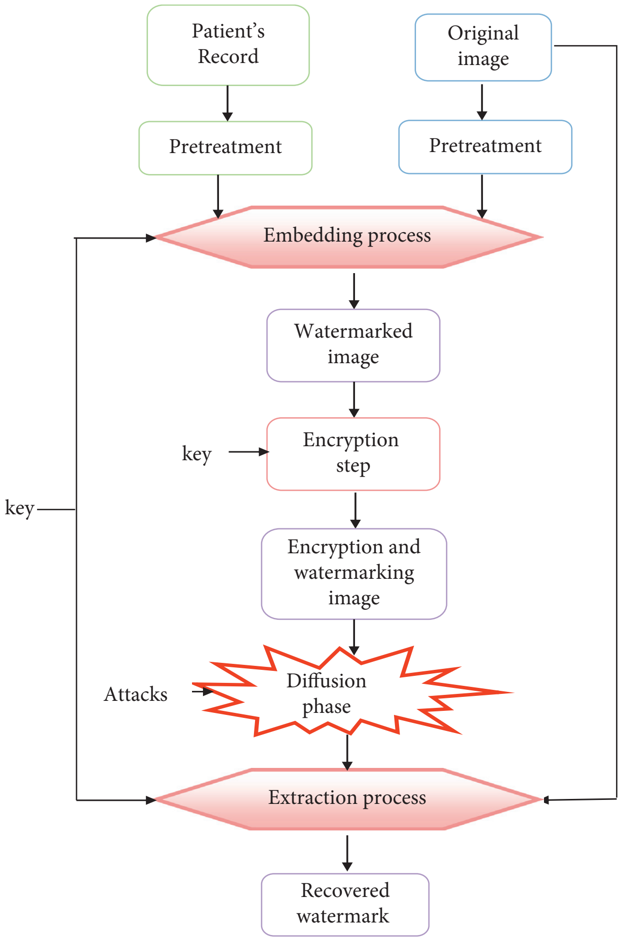


Figure 5: Global proposed schema.

defined secret key and the watermarked medical image as inputs and produces a scrambled, unclear, and unreadable watermarked medical image. Due to the random and chaotic key generation method, the encryption process is more complex, secure, and complicated in structure. The encryption step is easy to implement, simple, and understandable. The block diagram of the encryption process is shown in Figure 9.

4.5. The Extraction Process. In general, the extraction step follows the reverse stages with respect to the insertion.

Step 1: using Arnold's cat map to shuffle the watermarked encrypted image.

Step 2: key generation using a chaotic Henon map and running the decryption operation using the AES algorithm

Step 3: the AES algorithm to decrypt the watermarked encrypted image.

Step 4: applied the discrete cosine transform on the watermarked and original images.

Step 5: after applying the quantification step, the quantified subblocks of the watermarked and original images are carried out.

Step 6: selecting the maximum value situated in the medium frequency of each quantified subblocks. Then, extract the different bits of each subblocks by using the inverse of expression (7).

Step 7: concatenate all bits extracted from different subbands to obtain the extract message.

Step 8: apply the decoder algorithm on the binary message by using the serial turbo code.

Step 9: finally, the patient's information is extracted, audited, and eventually corrected.

Figure 10 summarizes the diverse stages to extract the watermark.

5. Performance Measures

The performance of the watermarking/encryption system is evaluated based on these following measures.

5.1. PSNR (Peak Signal-to-Noise Ratio). A PSNR indicates that the host image and the watermarked image are more similar. In fact, this resemblance means that the message inserted is more imperceptible. In general, if the PSNR value of the watermarked image is greater or equal to 27, then the

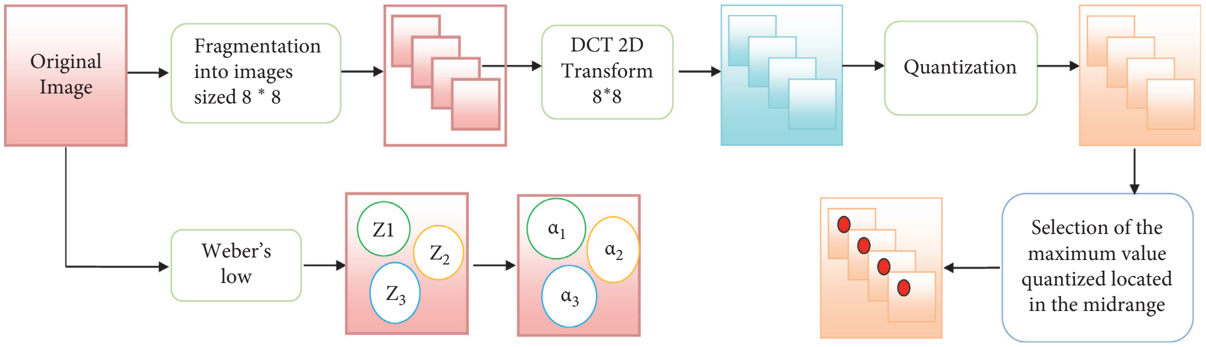

Original Image
Fragmentation into images sized 8 * 8
DCT 2D Transform 8*8
Quantization
Selection of the maximum value quantized located in the midrange
Weber's low
Z1
Z_2
Z_3
α_1
α_2
α_3

Figure 6: Preparation of the watermarking space.

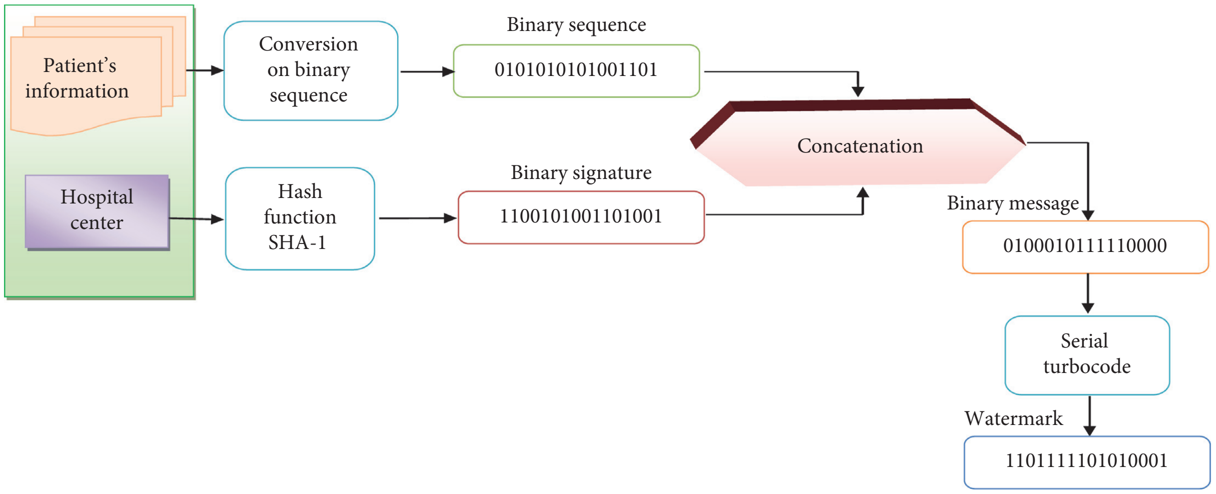


Figure 7: Preparation of the watermark.

PSNR is acceptable [7, 36]. The PSNR is defined by the following equation:

$$(\mathrm{PSNR})_{\mathrm{dB}} = 10 \log_{10}\left[\frac{A \times B \max(I(i,j))^2}{\sum_{i=1}^{A}\sum_{j=1}^{B}\left[I(i,j) - I'(i,j)\right]^2}\right], \quad (8)$$

with $I(i,j)$ and $I'(i,j)$ as the pixel value of the pixel (i,j) in the host and watermarked image and A and B are the width and height of the host image.

5.2. WPSNR (Weighted Peak Signal-to-Noise Ratio). The WPSNR is founded on the comparison between the watermarking image and the host image (pixel to pixel) [12]. WPSNR is defined by the following equation:

$$(\mathrm{PSNR})_{\mathrm{dB}} = 10 \log_{10}\left[\frac{A \times B \max(I(i,j))^2}{\sum_{i=1}^{A}\sum_{j=1}^{B}\left[\left(I(i,j) - I'(i,j)\right)/\left(1 + \mathrm{var}_I(i,j)\right)\right]^2}\right], \quad (9)$$

with var(i,j) as the local variance of pixel (i,j).

5.3. NCC (Normalized Cross-Correlation). The robustness of the watermarking system depends on the correlation factor. Indeed, the resemblance between the original and extracted watermark is detected by the calculus of different distances among the detected and inserted watermark. This measure is performed via the NCC (normalized cross-correlation) [23, 37, 38]. Its value is generally between 0 and 1. Ideally, it should be 1.

5.4. The Entropy. Entropy is a magnitude characterizing the quantity of data contained in an image. In fact, if the dispensing of grey values is very uniform, the information entropy is greater [39, 40]. The entropy $E(s)$ is defined by the following equation:

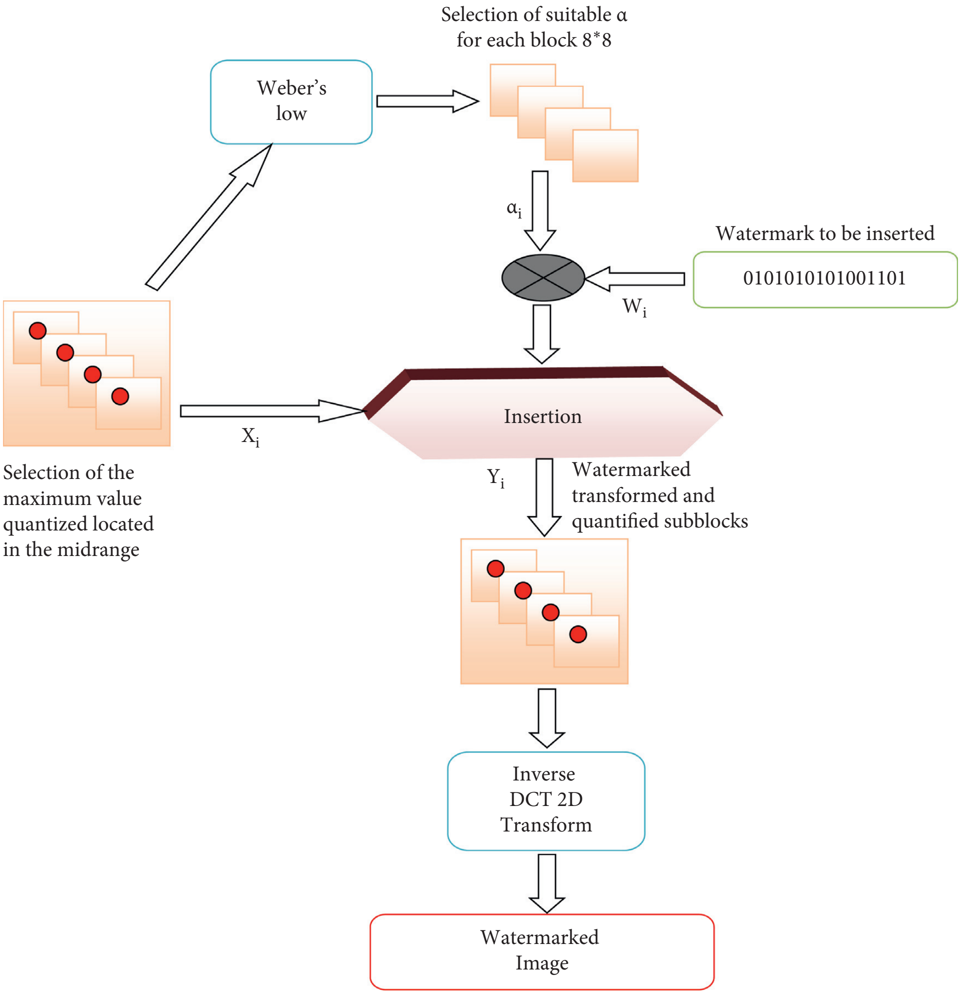

Selection of suitable α for each block 8*8
Weber's low
α_i
Watermark to be inserted
0101010101001101
W_i
Insertion
X_i
Selection of the maximum value quantized located in the midrange
Y_i
Watermarked transformed and quantified subblocks
Inverse DCT 2D Transform
Watermarked Image

Figure 8: Insertion algorithm.

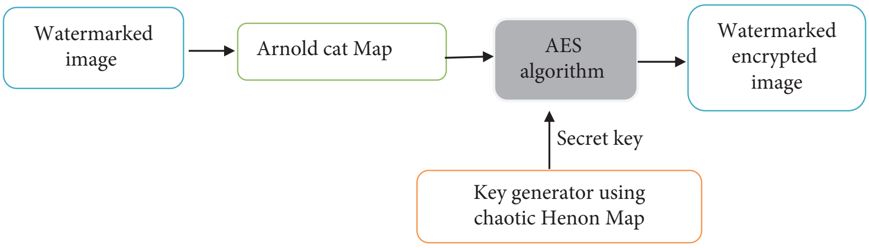

Watermarked image
Arnold cat Map
AES algorithm
Watermarked encrypted image
Secret key
Key generator using chaotic Henon Map

Figure 9: Encryption process.

$$E(s) = -\sum_{i=1}^{N} P(s_i)\log_2[P(s_i)]\text{Bit}. \quad (10)$$

6. Experimental Results and Discussion

6.1. Experiments' Results of the Watermarking Scheme. It is very essential to obtain a good value of NCC, PSNR, and WPSNR regardless of the system or the domain for dissimulated of the signature. In fact, this is particularly true in the domain of the medical imaging. For the validation of our system, we have been using diverse images sized of 512 × 512 pixels (radiographic, echographic, MRI, and mammography images). We obtain, in the literature, an acceptable extracted watermark when the value of the normalized cross-correlation is greater than "0.75" [13, 41, 42]. In the medical imaging domain, the signature is a binary message. So, in the phase of extraction signature, it is necessary to obtain the total of watermark inserted. Otherwise, we obtain a false diagnosis. Indeed, the measuring of the PSNR and WPSNR are acceptable when the rate of PSNR and WPSNR gives a

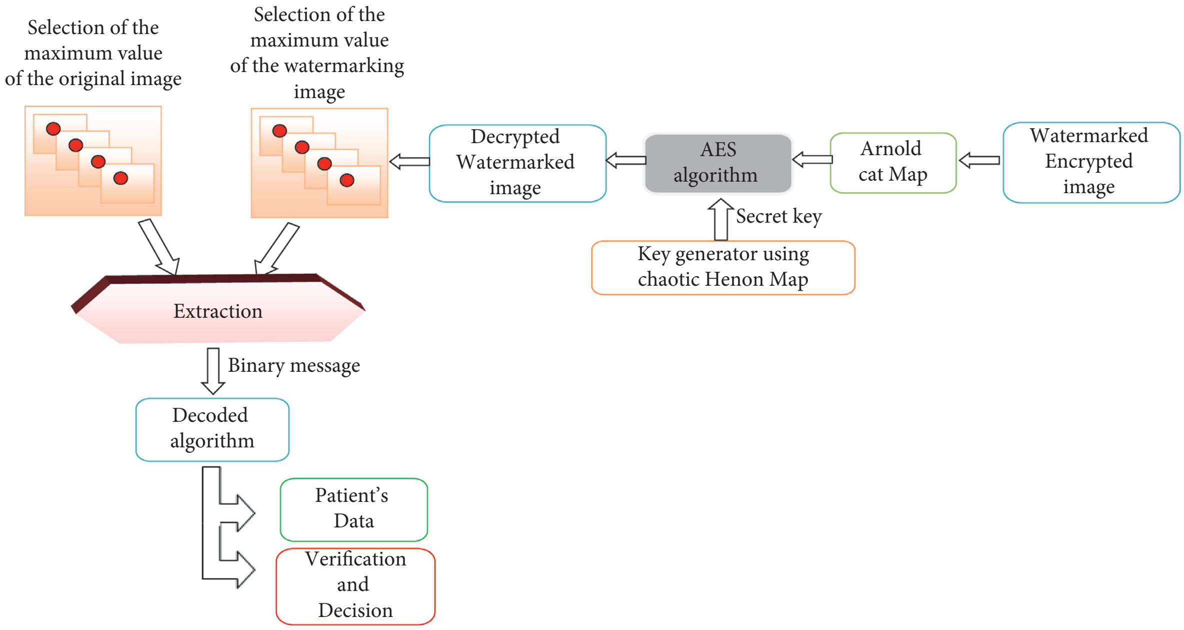

Selection of the maximum value of the original image
Selection of the maximum value of the watermarking image
Decrypted Watermarked image
AES algorithm
Arnold cat Map
Watermarked Encrypted image
Secret key
Key generator using chaotic Henon Map
Extraction
Binary message
Decoded algorithm
Patient's Data
Verification and Decision

Figure 10: Extraction step.

value exceeding 35 dB [8, 14, 43]. We begin analyzing the experimental results by determining the PSNR, NCC, and WPSNR, as shown in Figure 11, without the application of attacks.

Our algorithm will be more robust whether it will be resistant against different types of attacks. After applying several attacks, we extract the embedded signature and compare it with the original signature. The principal goal is to guarantee that the signature is not modified by the applying attacks. Then, regardless of the proposed schema of watermarking, it is important to get an NCC = 1 and a good value of PSNR and WPSNR.

Among the important watermarking constraints is the robustness, next to diverse types of attacks. We have selected to apply the most attacks to analyse the robustness of the schema which are JPEG attacks, filter, Gaussian and impulsive noise, geometric transform, and cropping. Then, after attacking the four types of the medical image, we attempt to extract our signature and calculate the NCC value. Our aim is to conclude the degree of robustness of our schema to resist to diverse attacks. Tables 1–6 show the experimental results of the NCC, WPSNR, and PSNR values between the host and extracted signature after applying of different attacks.

6.2. Experiments Results of the Encryption Schema. The four medical images (IRM, radiologic, echographic, and mammographic) encrypted and transformed into an illegible 2D sequence are exposed on Figure 12. The histogram of the four encrypted and original images is also illustrated.

As the results are shown in Figure 12, the histogram of the encrypted image has a regular intensities' distribution. In fact, on comparing the histogram of the watermarked encrypted image with the histogram of the host image, we find that the probabilities of occurrence of every grey level are uniformly repartees. The computed correlation coefficients were very low, and there was low similarity among the pixel values when the enhanced AES encryption was utilized under the CBC mode of operation. Therefore, the experimental results recommend that the encryption process can generate reliable results and is highly secure for medical imagery with a uniform distribution and maximum dissimilarity of pixel values without leaving any clue for statistical analysis and attacks.

Therefore, the entropy of the encrypted watermarked image is high (close to 8 bits/pixel). The entropy of the encrypted and watermarked medical images is shown in Table 7.

We evaluate the algorithm for four images. For each image, we produce the correspondent encrypted watermarked image utilizing the encryption-system. Subsequently, we evaluate it by calculating the entropy value. Compared with recent works in [44–47], as shown in Table 8, we obtained a good entropy very close to 8 bits/pixel.

6.3. Discussion of the Proposed Schema. In this section, the proposed system is studied by comparing our results to those cited in the section of a review of related works. Comparing the psycho-visual quality of the original and the watermarked medical image, the proposed algorithm provides very good results. In the absence of any type of attack, the PSNR equal to 59.8705, WPSNR equal to 61.9099 for the IRM image, PSNR equal to 60.1150, WPSNR equal to 62.9361 for the mammographic image, PSNR equal to 61.2855, WPSNR equal to 63.8992 for the echographic image, PSNR equal to 63.9774, and WPSNR equal to 69.4409 for the radiographic image are obtained which gives results that are often better than those algorithms previously shown in the related section of the review works.

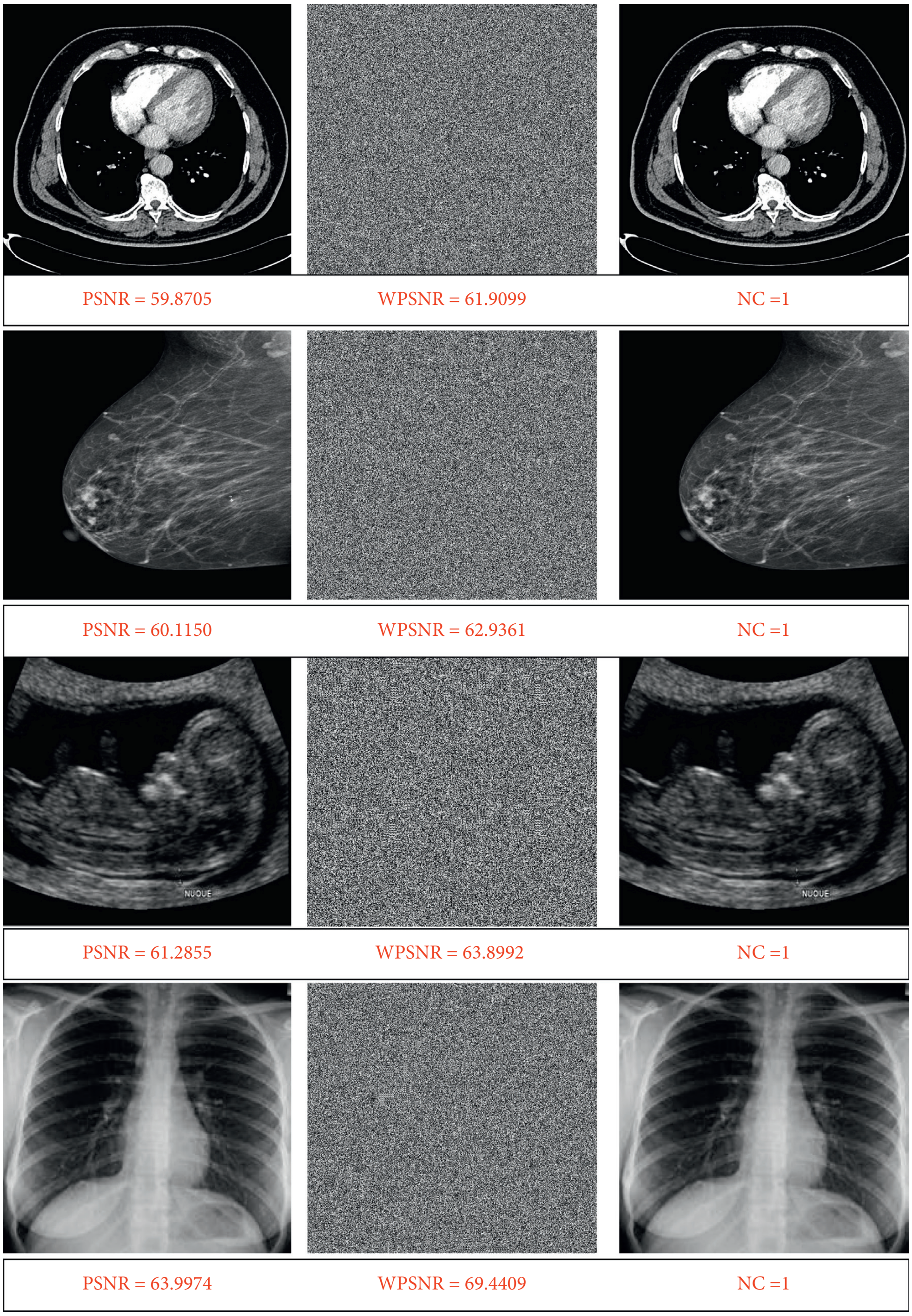


Figure 11: Imperceptibility and robustness of the watermark without attacks. (a) MRI, echographic, radiographic, and mammographic original images. (b) Watermarked encrypted images. (c) Watermarked decrypted images.

Table 9 illustrates the NC and PSNR values of our proposed system computed according to four medical images and compared with five recent schemes in attack-free case [48–51]. It can be observed that the NC values are equal to 1 and the average of the obtained PSNR values (61,7769 dB) is moderate. The obtained results are much higher than the reported methods. Therefore, our proposed scheme performs more efficiently depending on the imperceptibility factor.

During the manipulation of watermarked decrypted medical images, these later might be altered by various voluntary and involuntary image processing attacks. Consequently, it is essential to evaluate the robustness of our proposed approach under an attacking environment. For this purpose, a set of four medical images watermarked are subjected against the following attacks: JPEG compression, Gaussian noise, median filter, cropping, and rotation. After applying those attacks, it is necessary to evaluate the PSNR,

Table 1: Evaluation of the NC, PSNR, and WPSNR values for watermarked, decrypted, and attacked images by JPEG compression.

Ratio (%)	PSNR				WPSNR				NC			
	IRM	Radiographic	Echographic	Mammographic	IRM	Radiographic	Echographic	Mammographic	IRM	Radiographic	Echographic	Mammographic
10	31.7765	38.7765	33.9908	31.9809	35.0090	44.0093	39.7122	36.0922	1.000	1.000	1.000	1.000
20	28.1339	35.6670	30.9981	29.0998	33.9770	39.1229	36.0098	34.9980	1.000	1.000	1.000	1.000
30	25.5466	31.0090	28.3119	27.7778	31.9055	35.9888	34.0001	32.9003	1.000	1.000	1.000	1.000
40	24.4451	28.8770	26.0011	25.888	29.0990	32.9910	31.2295	29.6678	1.000	1.000	1.000	1.000
50	23.226	26.8770	25.5223	24.2229	27.5579	32.0099	28.4430	27.9984	1.000	1.000	1.000	1.000
60	20.0010	24.9001	20.8779	20.9333	26.1339	31.1211	26.9001	26.9901	1.000	1.000	1.000	1.000
70	19.0009	22.0997	19.0001	18.0009	25.8321	27.6555	26.7130	24.5411	0.9910	1.000	0.9990	0.7445
80	16.2333	19.7688	16.8880	15.9322	24.1322	27.0771	25.7116	23.9004	0.9978	1.000	0.899	0.7077
90	15.9111	15.7222	14.7999	15.1222	22.0114	25.0008	20.9711	22.4435	0.3880	0.7790	0.5988	0.6900

Table 2: Evaluation of the NC, PSNR, and WPSNR values for watermarked, decrypted, and attacked images by Gaussian noise.

Variance	PSNR				WPSNR				NC			
	IRM	Radiographic	Echographic	Mammographic	IRM	Radiographic	Echographic	Mammographic	IRM	Radiographic	Echographic	Mammographic
0.01	30.9989	34.9770	33.9942	31.9440	36.9888	45.9997	43.8770	37.4625	1.000	1.000	1.000	1.000
0.02	29.7664	33.9997	30.9677	29.8993	35.9920	43.9332	42.8854	35.7700	1.000	1.000	1.000	1.000
0.03	28.2991	33.9211	29.9901	28.9501	34.7770	41.9367	42.3356	35.2100	1.000	1.000	1.000	1.000
0.04	27.4667	31.7004	29.7099	28.8001	34.2330	39.8099	38.9344	34.9991	1.000	1.000	1.000	1.000
0.05	26.1441	30.9996	27.4388	27.9921	32.9888	38.6521	36.9377	33.7880	1.000	1.000	1.000	1.000
0.06	26.0224	29.9821	26.9441	25.9091	31.5220	36.8009	35.9907	31.2711	1.000	1.000	1.000	1.000
0.07	25.9970	28.7005	26.9333	25.0001	29.9932	36.1004	35.4887	29.6811	0.9999	1.000	1.000	0.9999
0.08	24.7001	26.7066	24.6661	24.9907	28.7660	35.9008	34.9881	28.7166	0.8990	1.000	0.9888	0.7556
0.09	20.7760	24.8874	24.0009	22.8861	26.2189	34.8611	31.0995	27.0943	0.6445	0.7999	0.7001	0.7088

Table 3: Evaluation of the NC, PSNR, and WPSNR values for watermarked, decrypted, and attacked images by salt and pepper noises.

Variance	PSNR				WPSNR				NC			
	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic
0.01	32.0998	30.9920	29.8993	30.9677	34.9920	37.9377	30.9901	29.8770	1.000	1.000	1.000	1.000
0.02	29.7778	27.9501	26.9942	29.9888	31.8001	35.9344	29.9932	26.9881	1.000	1.000	1.000	1.000
0.03	26.2229	25.8861	25.9333	28.4387	30.9088	34.8854	27.9322	25.8880	1.000	1.000	1.000	1.000
0.04	25.9809	24.0001	24.9901	28.9544	29.2412	34.4887	26.1122	24.0001	1.000	1.000	1.000	1.000
0.05	24.9333	23.8861	22.9211	27.3991	29.9221	33.9907	25.9006	22.8861	1.000	1.000	1.000	1.000
0.06	23.0019	23.0099	22.9330	25.8001	28.8861	33.0995	25.9081	22.0002	1.000	1.000	1.000	1.000
0.07	22.9982	22.9331	21.0988	25.9651	28.0099	33.9773	25.9122	21.8861	0.8899	1.000	0.7998	0.8777
0.08	22.9252	22.0333	21.9674	24.0900	27.0001	32.1133	24.5913	21.0001	0.4977	0.9988	0.7455	0.4998
0.09	22.4456	21.9008	20.9066	23.8861	27.8861	32.9000	24.9340	20.9033	0.2988	0.6777	0.6998	0.2908

Table 4: Evaluation of the NC, PSNR, and WPSNR values for watermarked, decrypted, and attacked images by median filter.

Filter's window	PSNR				WPSNR				NC			
size	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic
3 × 3	31.7765	38.5579	33.9908	31.9981	31.8922	37.4430	36.9003	31.9770	1.000	1.000	1.000	1.000
4 × 4	26.0090	35.0114	29.9333	26.7999	27.4435	35.1211	26.7765	27.5589	1.000	1.000	1.000	1.000
5 × 5	27.9908	32.0924	27.5411	27.9770	27.9849	30.9981	25.9339	27.0098	1.000	1.000	1.000	1.000
6 × 6	24.9809	32.0008	25.1218	24.0090	25.7765	30.0090	24.5579	25.9859	1.000	1.000	1.000	1.000
7 × 7	24.9003	29.9981	24.0001	24.0922	24.9770	29.0972	23.0008	24.0090	0.9999	1.000	1.000	0.9999
8 × 8	23.1299	29.0090	23.9918	23.5579	23.9988	28.9333	21.9981	23.7765	0.8777	1.000	0.9988	0.7999
9 × 9	23.9003	28.0090	22.9771	23.7765	23.0098	27.9819	21.0077	23.0001	0.6099	0.5877	0.5776	0.6677

Table 5: Evaluation of the NC, PSNR, and WPSNR values for watermarked, encrypted, and attacked images by rotation transform.

Rotation angle	PSNR				WPSNR				NC			
(°)	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic
1	33.7765	34.9908	30.9055	33.9001	33.9223	35.9988	31.7116	33.9003	1.000	1.000	1.000	1.000
3	32.1339	33.5411	29.0811	32.7999	33.9058	34.5223	31.2295	33.9912	1.000	1.000	1.000	1.000
5	31.9910	31.2215	26.3119	31.0100	32 .0228	32.0021	30.0008	32.1322	1.000	1.000	1.000	1.000
10	27.7113	30.0011	24.9112	27.1331	30.9002	31.7715	29.7998	30.0065	1.000	1.000	1.000	1.000
20	23.0008	28.3118	22.4511	23.9900	27.5411	29.9008	28.0677	27.5417	0.9778	1.000	0.9899	0.9999
30	20.5223	26.9003	24.9011	20.7116	25.7997	28.9919	26.1339	25.0039	0.8666	0.9980	0.5900	0.8777
45	20.1322	25.7763	20.5277	20.2295	24.3133	27.9012	24.0014	24.7765	0.5998	0.6668	0.4099	0.6990

Table 6: Evaluation of the NC, PSNR, and WPSNR values for watermarked, encrypted, and attacked images by cropping.

Rotation angle	PSNR				WPSNR				NC			
(°)	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic	IRM	Echographic	Radiographic	Mammographic
16 × 16	45.9001	43.0991	40.9044	44.9881	48.6700	50.8099	46.6777	45.9111	1.000	1.000	1.000	1.000
32 × 32	46.6551	36.0766	30.8990	45.0911	48.3400	43.7900	33.9088	47.2099	1.000	1.000	1.000	1.000
64 × 64	33.9034	30.1209	23.7613	39.6712	38.0177	38.2887	26.9022	39.9509	1.000	1.000	1.000	1.000
128 × 128	19.6711	24.9022	19.0001	20.0355	24.0001	32.0009	23.7070	25.6009	0.5999	1.000	0.9992	0.6988
256 × 256	15.0093	18.0012	11.9002	19.3199	19.0412	26.2009	15.0008	23.9033	0.2006	0.9998	0.6966	0.5666

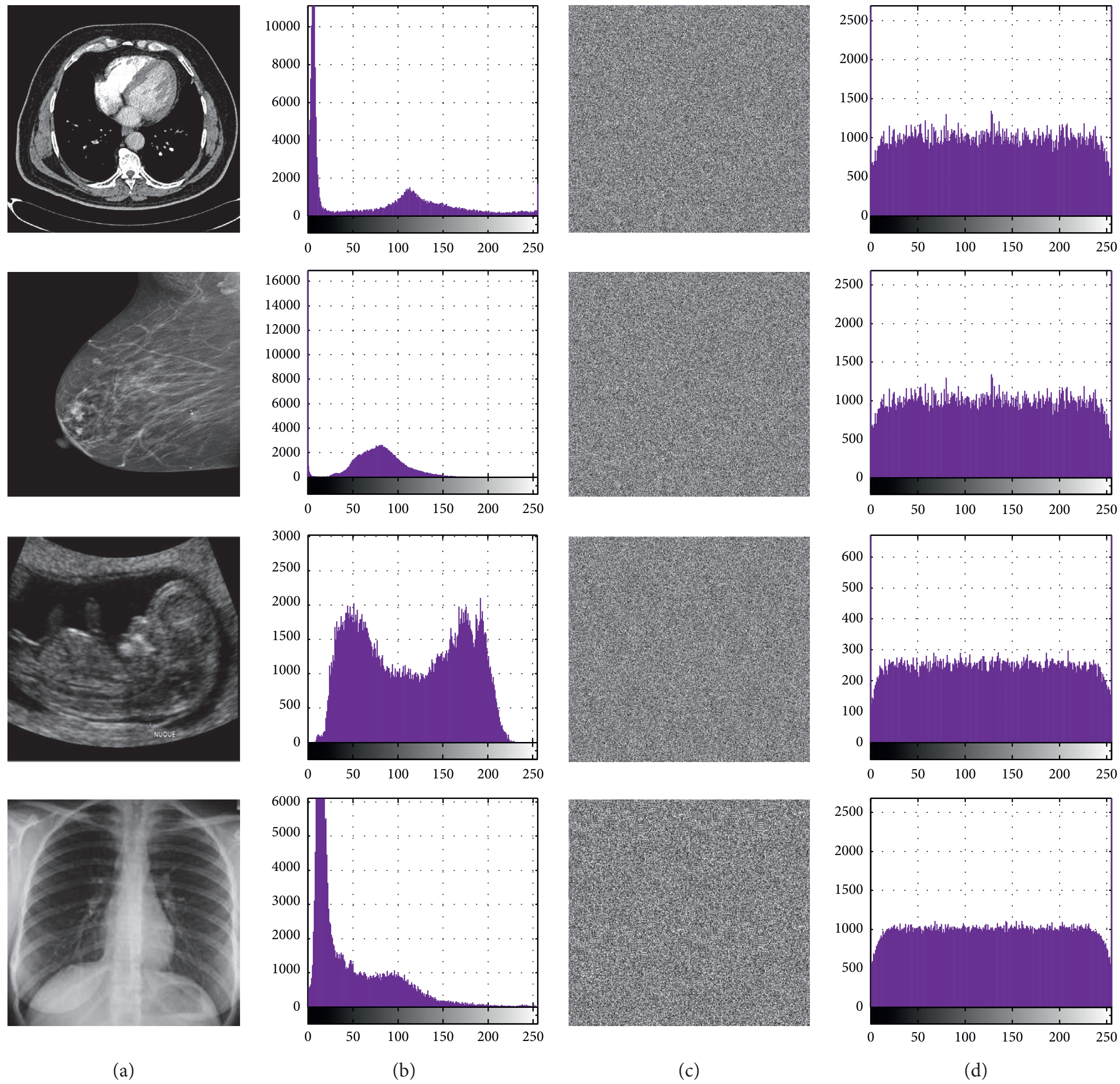


Figure 12: (a) Original images. (b) Histograms of the original images. (c) Watermarked and encrypted images. (d) Histograms of the watermarked encrypted images using AES under CBC.

WPSNR, and NCC. Among the most serious attacks, we apply the JPEG attack. The result is very effective against this kind of attacks. In fact, the results presented in Table 1 show that, from a compression rate equal to 60%, we were able to correctly extract our watermark (NC = 1). Out of this value, the recovery of the watermark is not complete, and then, there will be an erroneous diagnosis. Detection by correlation between the extracted and inserted watermark made our approach robust against several attacks, while keeping the visual appearance of the image after watermarking.

To evaluate our method against the Gaussian noises, we obtained very promising results. As the results already presented in Table 2, the approach that we have proposed has proven its performance. Indeed, the recovery of the watermark is equal to 100% (the signature is extracted correctly from the 500 signatures) for a variance equal to 0.07; beyond this value, the recovery of the watermark is not total. We validate the results obtained above that our approach has proven its robustness against this type of attack.

We also tested our system against salt and pepper attack. It is remarkable, as the results presented in Table 3, that data recovery is complete until a density value equal to 0.07. Beyond this value, the recovery of the watermark is not complete. As the values of PSNR and WPSNR, the results have proved that we have kept the image quality during watermarking. The detection by correlation between the signature extracted and that inserted argued the robustness of our approach against salt and pepper attack.

We are testing our system against the median filter [52, 53]. The test is evaluated with various sized windows (from (3 × 3) until (9 × 9)) (Table 4). In fact, the recovery of

Table 7: Entropy related to the encrypted and the watermarked medical images.

Image test	Key size	Mode	Entropy
MRI	256	CBC	7.9991
Mammographic	256	CBC	7.9998
Radiographic	256	CBC	7.9998
Echographic	256	CBC	7.9999

Table 8: Comparative study of entropy values for medical images.

Previous works	MRI	Mammographic	Radiographic	Echographic
Ref. [44]	7.9977	—	—	—
Ref. [45]	7.1100	—	7.9881	7.8471
Ref. [46]	5.3894	—	7.7072	7.6468
Ref. [47]	—	7.9961	—	—
Our work	7.9991	7.9998	7.9998	7.9999

Table 9: Comparison of PSNR (dB) and NC value of the proposed scheme with existing schemes.

Schemes	Test images	PSNR	NC
Ref. [48]	MRI	48.5362	0.9932
	Radiographic	43.2518	1.0000
Ref. [49]	MRI	48 .7200	—
Ref. [50]	MRI	48.9900	0.9230
	Radiographic	55.0600	0.9692
	Echographic	47.1800	0.9827
Our work	MRI	59.8705	1.000
	Mammographic	60.1150	1.000
	Radiographic	61.2855	1.000
	Echographic	63.9774	1.000

Table 10: Comparison of NC with existing systems.

Attacks		NC				
	Test images	Ref. [50]	Ref. [49]	Ref. [50]	Ref. [51]	Our work
JPEG compression	MRI	0.5945	0.5487	0.8734	0.8734	1.000
	Mammographic	—	—	0.7525	0.7525	1.000
	Radiographic	0.7125	—	0.8337	0.8337	1.000
	Echographic	0.6404	—	0.8793	0.8793	1.000
Cropping	MRI	—	—	—	—	1.000
	Mammographic	—	—	—	—	1.000
	Radiographic	—	—	—	—	1.000
	Echographic	—	—	—	—	1.000
Median filter	MRI	0.9700	—	0.8766	0.8766	1.000
Mammographic	Mammographic	—	—	0.8051	0.8051	1.000
	Radiographic	0.9538	0.5439	0.8689	0.8689	1.000
Echographic	Echographic	0.9607	—	0.8826	0.8826	1.000
Rotation	MRI	—	—	0.8869	0.8869	1.000
	Mammographic	—	—	0.8045	0.8045	1.000
	Radiographic	—	0.5439	0.8653	0.8653	1.000
	Echographic	—	—	0.8881	0.8881	1.000
Salt and pepper	MRI	0.5817	—	—	—	1.000
	Mammographic	—	—	—	—	1.000
	Radiographic	0.0132	0.9503	—	—	1.000
	Echographic	0.7532	—	—	—	1.000

our signature is equal to 100% (extracted correctly the watermark in the presence of this attack type) up to coefficients (6×6). The detection by correlation between the extracted and inserted signatures made our approach robust against attack by a median filter, while keeping the visual appearance of the image after watermarking.

We tested the robustness against the rotation attack. For a value of rotation angle greater than 10, the recovery of the watermark is not complete, and then, there will be an erroneous diagnosis.

We also tested our method against the cropping attack. As the results presented in Table 6, the approach that we have proposed has proven its performance. In fact, the recovery of the watermark is equal to 100% (NC = l) up to a window size (64 × 64); beyond this value, the recovery of the watermark is not total. We validate the results obtained above that our approach has proven its robustness against this type of attack.

Table 10 gives the results compared with those obtained with the approaches described in papers [49–51].

7. Conclusion

The present work is a new robust joint encryption/watermarking algorithm using the discrete cosine transform and the advanced encryption standard. The main contribution of this manuscript consists in improving the two principal factors existing in all watermarking systems (imperceptibility and robustness). In order to enhance the factor of imperceptibility, we chose to hide the watermark in the medium frequency of the DCT Transform. Weber's law is used to determine the suitable visibility factor for each subblocks of the image. To do so, we came across several stages. The original medical image is subdivided into subblocks sized 8 × 8. After that, the DCT is applied on each subblocks, and the quantization phase is then used in order to determinate the space of watermark insertion. The AES encryption algorithm is used together with the serial turbo code to improve the robustness of our contribution. We obtained a good result in terms of the watermark extracted which is comparable to the original (NC = 1). To evaluate the performance of our system, the proposed method is applied on medical images. Various tests are performed, such as JPEG compression, geometric transformation, and adding noise. The results show that our proposed algorithm is very robust against these various types of attack [40, 54–59].

Data Availability

The obtained results used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] D. Whitfield and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on information theory*, vol. 22, no. 6, pp. 644–654, 1976.

[3] A. Michael and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, Norwood, MA, USA, 2002.

[4] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, Morgan Kaufmann, Burlington, MA, USA, 2002.

[5] S. Ajili, M. A. hajjaji, and M. Abdellatif, "Combining ciphering & watermarking method for secure medical image transform," in *Proceeding of the 2nd International Conference on Automation, Control, Engineering and Computer Science (ICACE)*, Sousse, Tunisia, March 2015.

[6] S. Ajili, M. A. Hajjaji, and M. Abdellatif, "Combining watermarking and encryption algorithm for medical image safe transfer: method based on DCT," *International Journal of Signal and Imaging Systems Engineering*, vol. 9, no. 4-5, pp. 242–251, 2016.

[7] M. Hajjaji, M. Gafsi, and A. B. Abdelali, A. Mtibaa, FPGA implementation of digital images watermarking system based on discrete haar wavelet transform," *Security and Communication Networks*, vol. 2019, Article ID 1294267, 17 pages, 2019.

[8] M. Hajjaji, M. Gafsi, and A. Mtibaa, "Discrete cosine transform space for hiding patient information in the medical images," in *Proceedings of the IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS'19)*, Gammarth, Tunisia, May 2019.

[9] S. Ajili, M. Hajjaji, B. Bouallegue, and A. Mtibaa, "Joint watermarking encryption image for safe transmission: application on medical imaging," in *Proceedings of the 2014 Global Summit on Computer & Information Technology (GSCIT)*, pp. 1–6, Sousse, Tunisia, 2014.

[10] M. Hajjaji, A. B. Abdellali, N. Farhani, M. Gafsi, and A. Mtibaa, "Real time implementation of numerical watermarking system using xilinx system generator," in *Proceedings of the 16th International Conference on Sciences and Techniques of Automatic Control & Computer Engineering—STA'2015*, Monastir, Tunisia, December 2015.

[11] I. Afzal, S. A. Parah, N. N. Hurrah, and O.Y. Song, "Secure patient data transmission on resource constrained platform," *Multimedia Tools and Applications*, pp. 1–26, 2020.

[12] M. Hajjaji, E. B. Bourennane, A. B. Abdelali, and A. Mtibaa, "Combining Haar wavelet and Karhunen Loeve transforms for medical images watermarking," *BioMed Research International*, vol. 2014, Article ID 313078, 15 pages, 2014.

[13] S. Ajili, M. Hajjaji, and A. Mtibaa, "Hybrid SVD-DWT watermarking technique using AES algorithm for medical image safe transfer," in *Proceedings of the 16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pp. 69–74, Monastir, Tunisia, July 2015.

[14] M. Hajjaji, A. Albouchi, and A. Mtibaa, "Combining DWT/KLT for secure transfer of color images," in *Proceedings of the IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS'19)*, Gammarth, Tunisia, May 2019.

[15] M. gafsi, N. Abbassi, M. Hajjaji, J. E. Malek, and M. Abdellatif, "Xilinx Zynq FPGA for hardware implementation of a chaos-based cryptosystem for real-time image protection," *Journal of Circuits, Systems, and Computers*, 2021.

[16] S. A. Parah, J. A. Kaw, P. Bellavista et al., "Efficient security and authentication for edge-based internet of medical things," *IEEE Internet of Things Journal*, 2020.

[17] K. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[18] L. Gao, T. Gao, G. Sheng, Y. Cao, and L. Fan, "A new reversible watermarking scheme based on Integer DCT for medical images," in *Proceedings of the Wavelet Analysis and*

Pattern Recognition (ICWAPR), pp. 33–37, IEEE, Xi'an, China, July 2012.

[19] Y. Shang and Y. Kang, "Medical images watermarking algorithm based on improved DCT," *Journal of Multimedia*, vol. 8, no. 6, pp. 796–801, 2013.

[20] P. Koushik and K. Subhajit, "A new combined crypto-watermarking technique using RSA algorithm and discrete cosine transform to retrieve embedded EPR from noisy biomedical images," in *Proceedings of the International Conference on Condition Assessment Techniques in Electrical Systems*, pp. 368–373, IEEE, Kolkata, India, December 2013.

[21] P. Chittaranjan, V. Saxena, and A. K. Bisoi, "Non blind digital watermarking technique using DCT and cross chaos map," in *Proceedings of the International Conference on Communication, Devices, and Intelligent Systems*, pp. 282–285, IEEE, Kolkata, India, December 2012.

[22] P. Chittaranjan, B. J. Saha, and K. K. Kabi, "Comparative analysis of digital watermarking scheme using enhanced playfair cipher in DCT & DWT," in *Proceedings of the Communication and Networking Technologies (ICCCNT)*, pp. 1–6, IEEE, Hefei, China, November 2014.

[23] H. Guan, Z. Zeng, J. Li, and S. Zhang, "A novel robust digital image watermarking algorithm based on two-level DCT," in *Proceedings of the 2014 International Conference on Information Science, Electronics and Electrical Engineering*, pp. 1804–1809, Sapporo, Japan, April 2014.

[24] A. Ustubioglu, G. Ulutas, and M. Ulutas, "DCT based image watermarking method with dynamic gain," in *Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 550–554, Prague, Czech Republic, July 2015.

[25] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimedia Tools and Applications*, vol. 76, no. 8, pp. 10599–10633, 2017.

[26] S. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "On the realization of robust watermarking system for medical images," in *Proceedings of the 2015 Annual IEEE India Conference (INDICON)*, March 2015.

[27] W. Ekta and A. Suneja, "A robust watermark authentication technique based on Weber's descriptor," *Signal Image and Video Processing*, vol. 6, no. 1, pp. 1–14, 2012.

[28] A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice-Hall, Hoboken, NJ, USA, 1989.

[29] J. Chen, S. Shan, C. He et al., "WLD: a robust local image descriptor," *IEEE Pattern Analysis and Machine Intelligence*, vol. 32, no. 9, pp. 1705–1720, 2010.

[30] Z.-H. Guan, F. Huanga, and W. Guanb, "Chaos-based image encryption algorithm," *Physics Letters*, vol. 153–157, 2005.

[31] E. Petrisor, "Entry and exit sets in the dynamics of area preserving Henon map," *Chaos, Solitons & Fractals*, vol. 17, no. 4, pp. 651–658, 2003.

[32] N. F. Pub, "Advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, pp. 441–0311, 2001.

[33] M. Gafsi, N. Abbassi, M. Hajjaji, J. Malek, and A. Mtibaa, "Improved chaos-based cryptosystem for medical image encryption and decryption," *Scientific Programming*, vol. 2020, Article ID 6612390, 22 pages, 2020.

[34] M. Dridi, B. Bouallegue, and M. A. Hajjaji, "An enhancement crypto-compression scheme for image based on chaotic system," *International Journal of Applied Engineering Research*, vol. 11, no. 7, pp. 4718–4725, 2016.

[35] U. S. Government Standard, "Federal information processing standards publication," *Secure Hash Standard*, vol. 180, no. 2, 2002.

[36] Naini and P. Monshizadeh, *Digital Watermarking Using MATLAB*, INTECH Open Access Publisher, London, UK, 2011.

[37] M. Gafsi, M. Hajjaji, J. Malek, and A. Mtibaa, "Efficient encryption system for numerical image safe transmission," *Journal of Electrical and Computer Engineering*, vol. 2020, Article ID 8937676, 12 pages, 2020.

[38] M. Hajjaji, M. Dridi, and A. Mtibaa, "A medical image crypto-compression algorithm based on neural network and PWLCM," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 14379–14396, 2019.

[39] M. J. Mateo, D. J. Callaghan, and C. P. Donnell, "Comparison between red-green-blue imaging and visible-near infrared reflectance as potential process analytical tools for monitoring syneresis," *Journal of Dairy Science*, vol. 93, no. 5, pp. pp1882–1889, 2010.

[40] M. Dridi, M. Hajjaji, B. Bouallegue, and A. Mitbaa, "An enhancement medical image compression algorithm based on neural network," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 5, 2016.

[41] M. Gafsi, S. Ajili, M. Hajjaji, and A. Mitbaa, "XSG for hardware implementation of a robust watermarking system," in *Proceedings of the 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, Sousse, Tunisia, December 2016.

[42] M. Dridi, M. A. Hajjaji, and A. Mtibaa, "Hardware implementation of encryption image using xilinx system generator," in *Proceedings of the 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, Sousse, Tunisia, December 2016.

[43] A. Khalifa and S. Hamad, "A robust non-blind algorithm for watermarking color images using multi-resolution wavelet decomposition," *International Journal of Computer Application*, vol. 37, no. 8, pp. 33–39, 2012.

[44] M. Brindha, "Confidentiality, integrity and authentication of DICOM medical images," in *Proceedings of the 2018 2nd International Conference on Inventive Systems and Control (ICISC)*, IEEE, Coimbatore, India, January 2018.

[45] H. Abdel-Nabi and A.-H. Ali, "Efficient joint encryption and data hiding algorithm for medical images security," in *Proceedings of the 2017 8th International Conference on Information and Communication Systems (ICICS)*, IEEE, Irbid, Jordan, April 2017.

[46] A. Al-Haj and H. Abdel-Nabi, "Digital image security based on data hiding and cryptography," in *Proceedings of the 2017 3rd International Conference on Information Management (ICIM)*, IEEE, Chengdu, China, April 2017.

[47] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 22787–22808, 2018.

[48] Y. Gangadhar, V. S. Giridhar Akulab, and P. Chenna Reddy, "An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation," *Biomedical Signal Processing and Control*, vol. 43, pp. 31–40, 2018.

[49] F. Y. Shih and X. Zhong, "High-capacity multiple regions of interest watermarking for medical images," *Information Sciences*, vol. 367, pp. 648–659, 2016.

[50] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on

FDCuT–DCT," *Engineering Science and Technology*, vol. 20, pp. 1366–1379, 2017.

[51] S. Vellaisamy and V. Ramesh, "Inversion attack resilient zero-watermarking scheme for medical image authentication," *IET Image Processing*, vol. 8, no. 12, pp. 718–727, 2014.

[52] M. Gafsi, S. Ajili, M. Hajjaji, J. Malek, and A. Mtibaa, "High securing cryptography system for digital image transmission," in *Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunication, SETIT*, Hammamet, Tunisia, December 2018.

[53] M. Ali Hajjaji, E. B. Bourennane, A. Mtibaa, and G. Ochoa-Ruiz, "A digital watermarking algorithm based on quantization of the DCT: application on medical imaging," in *Proceedings of the International Conference on Control, Decision and Information Technologies, CoDIT*, Hammamet, Tunisia, May 2018.

[54] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060–3063, 2010.

[55] V. Bhat, I. SenguptaI, and A. Das, "An audio watermarking scheme using singular value decomposition and dither-modulation quantization," *Multimedia Tools and Applications*, vol. 52, no. 2, pp. 369–383, 2011.

[56] R. O. Preda and N. D. Vizireanu, "Quantisation-based video watermarking in the wavelet domain with spatial and temporal redundancy," *International Journal of Electronics*, vol. 98, no. 3, pp. 393–405, 2011.

[57] J. Dong, J. Li, and Y. Duan, "A robust watermarking algorithm for encrypted medical images based on DCT encrypted domain," in *Proceedings of the International Conference on Electronic Science and Automation Control*, Zhengzhou, China, October 2015.

[58] M. Gafsi, "High securing and fast encryption algorithm for safe digital image transmission," in *Proceedings of the 8th International Conference*, Qingdao, China, March 2018.

[59] M. Dridi, M. Hajjaji, B. Bouallegue, and A. Mitbaa, "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Processing*, vol. 10, no. 11, pp. 830–839, 2016.