Journal of Computer and Communications, 2021, 9, 1-21
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Robust Non-Blind Watermarking for Biomedical Images Based on Chaos

Noura Alexendre[1], Ntsama Eloundou Pascal[1], Simo Thierry[1], Welba Colince[2]

[1]Department of Physics, University of Ngaoundere, Ngaoundere, Cameroon
[2]Department of Energy Renouvelable, School Petroleum of Kaele, University of Maroua, Maroua, Cameroon
Email: nouraalexendre@gmail.com, pentsama@yahoo.fr, simothierry51@yahoo.fr, welbacolince@yahoo.fr

How to cite this paper: Alexendre, N., Pascal, N.E., Thierry, S. and Colince, W. (2021) A Robust Non-Blind Watermarking for Biomedical Images Based on Chaos. *Journal of Computer and Communications*, **9**, 1-21.
https://doi.org/10.4236/jcc.2021.92001

Received: October 14, 2020
Accepted: December 31, 2021
Published: February 3, 2021

Abstract

The advent of the Internet in these last years encouraged a considerable traffic of digital images. In the sanitary field, precisely in telemedicine branch, medical images play a very important role for therapeutic diagnoses. Thus, it is necessary to protect medical images data before transmission over the network to preserve their security and prevent unauthorized access. In this paper, a secure algorithm for biomedical images encryption scheme based on the combination of watermarking technique and chaotic function is proposed. In the proposed method, to achieve high security level performances, a non-blind hybrid watermarking technique with audio signal, Discrete Wavelet Transform is used; smoothness is also used as selected criteria; the iterations obtained by the chaotic sequences are essential and allow a good realization of the encryption process. One of the main advantages of chaos-based encryption schemes is the generation of a large number of key spaces to resist brute force attacks from the encryption algorithm. The experimental results presented in this paper attest to the invisibility and robustness of the proposed algorithm combining watermarking and chaos-based encryption.

Keywords

Biomedical Image, Watermarking, Wavelet Transform, Chaotic Encryption, DCT

1. Introduction

During these last years, the fast evolution of the communication techniques and treatment of information have facilitated the sharing of the pictures in communication channels. The means of security bet in place to guarantee the protection of these information present possibilities of flights, diversion and modification

[1]. The surveillance of these risks introduces the protective need of the medical information. These consequences, audible, concern an individual and particularly his health integral part of his private life [2]. Watermarking consists to insert in host image, information (mark) invisible and indelible and to tempt to recover it after the picture possibly underwent the treatments. The insertion of the mark can be carried out in several domains. The main ones are: the space domain and the frequency domain. The first domain concerns the direct modification of the pixel values, precisely on Low Weight Bits (LSB). It is used a lot because of its simplicity, but it has a major drawback, and it is not robust enough to attacks [3]. The frequency domain, on the other hand, makes use of numerous reversible transforms, such as the discrete cosine transform (DCT), the discrete wavelet transforms (SWT) and the smooth contour transform (TC), all of which allow the image to be converted into its frequency representation. The integration of the mark in the frequency domain has an enormous advantage: it is resistant to attacks (robustness), but its realization remains very complex, and this is the conclusion reached by the researchers [4].

The cryptography is also one of the solutions to the security of data in a confidential manner. It consists in returning incomprehensible information (ciphering). Encoded information is called cryptogram. The transformation which permits the ciphering and decoding of information is mathematical functions called algorithms. The field of the application of cryptography remains very varied [5]. The cryptography has the following objectives:

- Confidentiality means to return unintelligible information, to all no one not having the key.
- The authentication allows the recipient to ascertain the identity of the emitter.
- The integrity allows the recipient to ensure that the content of the message has not been falsified since its consignment.
- The non-repudiation guarantees that the two individuals would not know how to deny their implication in the transaction.
- The access control is the faculty to limit and to control the access to systems and applications of the links of the communication.

Let's note that, the security of the information encoded rests on the invulnerability of the ciphering algorithm and the key confidentiality [6]. Two main algorithms of encryption exist: the symmetrical algorithm when the same key is used for encryption and decryption and the so-called asymmetric algorithm, because of the use of different keys. According to the use of these keys, we count the standards algorithms of ciphering as, AES, RSA, DSA, and IDEA etc. Next to these standards methods are some encryption methods which exist based on chaos that is used more and more. This paper presents a method of medical images security by associating watermarking and encryption in order to assure confidentiality of their transmission.

This paper is organized as follows: An introduction is mentioned firstly; sec-

tion two is based to related work; the third section presents recalls theory of Discrete Wavelet transform (DWT) and Discrete Cosine Transform (DCT). The section four describes the proposed method. Results and discussions are presented in section five. The last section presents the conclusion.

Numerous different approaches for watermarking methods and image encryption can be found in the scientific literature [7], use watermarking to provide confidentiality of some images. In the same way [8], proposed a technique of watermarking for authentication, the method use wavelet decomposition. Many others researchers as Puech *et al.* [9], proposed a robust watermarking algorithm with a combination of AES encryption to promote the confidentiality and integrity of medicals images. Gokcen *et al.* [10], proposed a robust chaotic digital image Watermarking Scheme based on RDWT and SVD. [11] [12] [13] and [14], have make use of watermarking to insert the information of patient.

Some others researchers as [15] [16] [17] [18] have apply many transformations as wavelet, wavelet packet transform, discrete cosine transform, Zernike moments in their proposed watermarking scheme.

[19] proposed security technique based on watermarking and encryption for digital imaging and communication in medicine, including partial encryption methods. [20] proposed algorithm for coding, to determine a set of selective blocks for steady embedding. [21] had proposed a scheme which incorporates the concept of modular arithmetic and chaos theory, for image encryption and decryption. [22] used DCT to propose a blind watermarking algorithm; the phase of extraction is focused to the statistical properties of embedded sequence. [23] proposed a watermarking algorithm, where watermark is embedded in the most significant frequency of DFT of the host image. [24] proposed a watermarking scheme based on Wavelet Discrete Transform (DWT) and Logistic map to generate a binary watermark. Their proposed algorithm is blind watermarking algorithm. [25] proposed an efficient and secure algorithm, by associating chaos encryption and compression, the encryption is proceeding by diffusion and confusion properties.

Of the above works, we note that watermarking can be used to provide authentication, it also helps of adding necessary and personals information confidentially. In medicine milieu the combination of watermarking and encryption is essential to attempt two important criteria of medicals images security which are authentification and confidentiality. Robustness against attacks, imperceptibility, high capacity watermark embedding, security, reversibility and rapidity are also other criteria that we try to satisfy during the transmission of biomedical images all over the network transmission channels. The proposed algorithm in this paper satisfies some of these criteria.

2. Preliminaries

2.1. Wavelet Discrete Transform (DWT)

Wavelet transform 2D, all as the other transformed Fourier 2D, cosine 2D is

used extensively in signal processing, its application took a remarkable flight from the years 1980 with the works of Morlet, Meyers, Daubechies and Mallat. Discrete wavelet transform is characterized at time by its limit temporal and frequential (compact support). The decomposition of a signal $x(l)$ to place through filters and gets itself in a following manner

$$Y_h(l) = \sum_{l=-\infty}^{+\infty} x(l) h(2i-l) \tag{1}$$

$$Y_g(l) = \sum_{l=-\infty}^{+\infty} x(l) g(2i-l) \tag{2}$$

$h(l)$ and $g(l)$ are respectively High and low filters

$$\begin{aligned} H(\omega) &= \sum_{l=-\infty}^{+\infty} h(l) \mathrm{e}^{-j\omega} \\ G(\omega) &= \sum_{i}^{+\infty} g(l) \mathrm{e}^{-j\omega} \end{aligned} \tag{3}$$

$H(\omega)$ and $G(\omega)$ will be orthogonal

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \tag{4}$$

The obtained coefficients are:

$$c[j-1,k] = \sum_{l=-\infty}^{+\infty} h[n-2k] c[j,n] \tag{5}$$

$$d[j-1,k] = \sum_{l=-\infty}^{+\infty} g[n-2k] c[j,n] \tag{6}$$

The image which is a signal of two dimension, its application of 2D wavelet transform gives a dyadic decomposition of this one with the help of a couple of quadratic mirrors filters (QMF)a being a High pass filter (HS) and the other a low pass (L). The use of does one coins sampling by a factor 2, permitting to get four sub- bands, one under-strip low frequency (LL) and three under-strips high respective frequencies (LH, HL,HH),representing, orientations with very specific vertical, horizontal and diagonal Face [26].

2.2. Discrete Cosine Transform (DCT)

It permits to separate the low frequencies from the high frequencies. This decomposition is done by dividing in blocks of 8 × 8 pixels according to the following equation:

$$F(u,v) = a(u)a(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left(\frac{(2x+1)j\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \tag{7}$$

The inverse transform is obtained as:

$$f(x,y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} a(u)a(v)F(u,v) \cos\left(\frac{(2x+1)j\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \tag{8}$$

$$a(u) = a(v) = \frac{1}{\sqrt{2}}$$

With for $u = v = 0$

$$a(u) = a(v) = 1 \quad \text{for} \quad u, v = 1, 2, \cdots, n-1$$

2.3. Relative Smoothness

Measurement of relative smoothness is one of selected applications; it is made by the following relation:

$$R = 1 - \frac{1}{1 + \sigma^2(x)} \tag{9}$$

where, σ is the standard deviation of the gray values. x represent sub block of the image; biggest is relative smoothness better is the smooth of chosen block. In this paper relative smoothness is use as selected criteria for the four sub-images of second level decomposition of host image by wavelet discrete transform [27].

2.4. Watermarking

The watermarking image consists of inserting in an indelible manner, information in a host image then to tempt to recover this information after transfer [28]. The diagrams of watermarking are varied according to their application domain. The insertion of the signature will make itself either in the spatial domain either in the transform domain. In additive diagram, information to insert is added in a picture whereas in a substitutive diagram information to insert is substituted for features of the picture. In our work we use an additive diagram in frequential domain. Equation gives an example:

$$X_{W,K} = X_K + \alpha W_K \tag{10}$$

With W_K marked bock image, X_K, original image block, α mark strength, $X_{W,K}$ watermarked image.

2.5. Vershult Model

The model of Vershult is a model of growth proposed by Pierre François Vershult [29]. This model uses the functions refine to explain the birth rate and the death rate of a population. Putting x as carves of the population; $m(x)$ the death rate and $n(x)$ the birth rate. The size of the population follows the differential equation:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = x\left(n(x) - m(x)\right) \tag{11}$$

If m and n are affine functions respectively increasing and decreasing functions. If, on the other hand, for x tending towards 0 growths is positive, the equation becomes:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = x(a - bx) \tag{12}$$

with a and b two real positive.

Then, by setting $K = a/b$, the Equation (12) becomes:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \alpha X_n\left(1 - \frac{x}{k}\right) \tag{13}$$

The constant K affects solution of this Equation (13):

It is shown that:

- The constant function K is a solution of this equation
- If $x < K$ then the population grows
- If $x > K$ then the population decreases.

The discrete resolution of the transformed Equation (13) is:

$$X_{n+1} - X_n = \alpha X_n \left(1 - \frac{X_n}{k}\right) \tag{14}$$

if we put $\alpha + 1 = \mu$ Equation (14) becomes

$$Y_n = \alpha \frac{X_n}{\mu k} \tag{15}$$

$$Y_{n+1} = \mu Y_n \left(1 - Y_n\right) \tag{16}$$

Equation (16) is call logistic map equation; its behavior varies according to the values of μ:

For μ included between 1 and 3, that means understood between 0 and 2, does the Y_n continuation converge toward $(1-\mu)/\mu$ and does one well recover a continuation (Y_n) convergent toward K

For μ superior to 3, the continuation (Y_n) can, according to the values of oscillation between 2, 4, 8, 16… goes.

For μ equal to 4, the continuation (Y_n) can, according to the values of μ, to oscillate in all senses, producing the chaos thus.

3. Proposed Model

The paragraph below, presents the watermarking scheme associating the logistic map. The block diagram is illustrated in Figure 1; in order to better understand

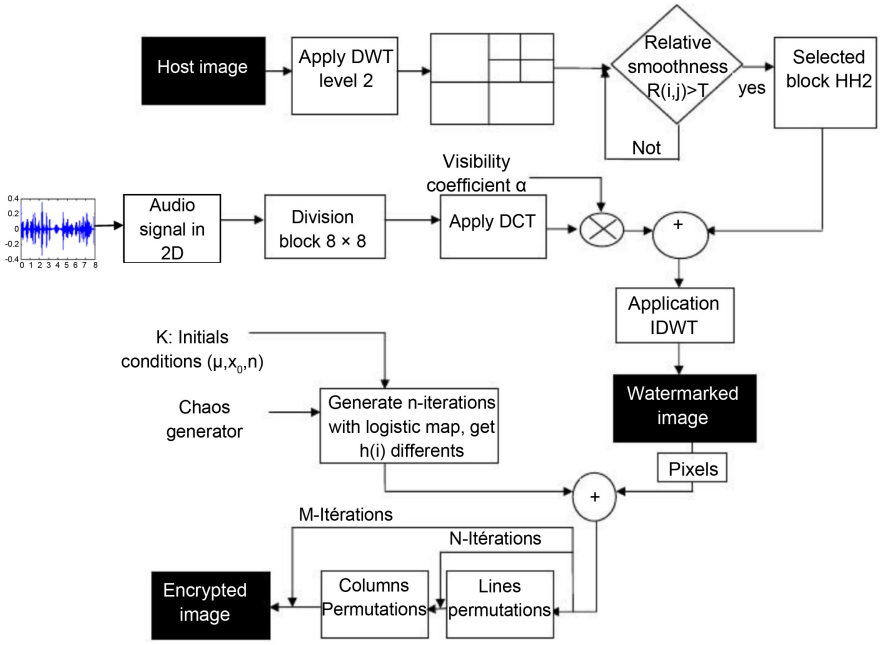


Figure 1. Block diagram of proposed scheme.

the proposed method, we present the algorithms for inserting and extracting the mark described below. The respective sizes of the host images and the mark are: $M \times N$ and $m \times n$.

3.1. Embedding and Encryption Algorithm

Watermark embedding and encryption are described as follows:

Input: Host_object, Watermark

Output: Encrypted_Object

Step 1: Read grey scale Host_object of size $M \times N$.

Step 2: Decompose Host Object using Daubichies wavelet [LL1, HL1, LH1, HH1] = dwt2 (Host_Object, "db")

Step 3: Apply DWT to HL1 sub-band of Host Object, [LL2, HL2, LH2, HH2] = dwt2 (HL1, "db").

Step 4: Calculate relative smoothness (R) of four LL2, HL2, LH2, and HH2, choose the sub-band that has the biggest value of smoothness, HH2.

Step 5: Read audio signal, converted in 2D, call watermark of size $m \times n$.

Step 6: Apply DCT to Watermark W, W_{DCT} = dct2 ("Watermark").

Step 7: Perform embedding Watermark W_{DCT} by sub-band (HH2) of Host_object find in step 4, HH2new = HH2 + αW_{DCT} after resizing.

Step 8: Apply inverse IDWT to get new $HL1_{new}$, HL1new = idwt2 (LL2, HL2, LH2, HH2new, "db");

Step 9: Apply now inverse IDWT to get Watermarked_Objet, Watermarked_Objet = idwt2 (LL1, HL1new, LH1, HH1, "db");

Display Host_Object, Watermarked_Object, PSNR.

Step 10: Generate chaotic sequence with following parameters: μ = 3.93695629844, and initial x_0 = 0.456

Step 11: Generate n-iterations with logistic map to get $h(i)$ different orbit: $y_{n+1} = \mu y_n (1 - y_n)$;

Step 12: Associate the chaotic sequence with pixels of watermarked;

Step 13: Make permutation in lines, by N-iterations;

Step 14: Make permutation in columns by M-iterations and get encrypted image;

Step 15: Display Encrypted_objet.

3.2. Decryption and Extraction Algorithm

Input: Encrypted Object, Host object,

Output: Extracted Watermark;

Step 1: Read Encrypted Object.

Step 2: Generate chaotic sequence with following parameters: μ = 3.93695629844, and initial x_0 = 0.456

Step 3: Generate n-iterations with logistic map to get $h(i)$ different orbit: $y_{n+1} = \mu y_n (1 - y_n)$;

Step 4: Associate the chaotic sequence with pixels of watermarked;

Step 5: Make permutation in lines and columns, by N-iterations then M-iterations;

Step 6: GetDecrypted_Objet;

Step 7: Decompose Decrypted_Objet using Daubichie wavelet

[LLr, Recover_HLr, LHr, HHr] = dwt2 (Decrypted_Object, "db"),

Step 8: Apply DWT to Recovered_HLr sub-band of Decrypted_Objet, [LL2r, HL2r, LH2r, and HH2r] = dwt2 (Recoverd_HLr, "db").

Step 9: Read HH2 sub-band of Host_object, step 3; step 4 of watermark embedding algorithm.

Step 10: Find Scrambled_Watermark using scale factor α used in watermark embedding algorithm as, Scrambled_Watermark = (HH2r-HH2)/α, get 2D audio son.

Step 11: Apply inverse IDCT to Scrambled Watermark to find final Extracted Watermark, Extracted Watermark = idct2 ("Scrambled Watermark") equal audio son.

Step 15: Display Extracted Watermark.

4. Results and Discussion

Various experiments are carried out to assess the performance of the proposed algorithm, in terms of robustness against attacks and imperceptibility. Four gray-scale images obtained in medical image center of regional hospital of Ngaoundere and Douala in Cameroon have been used. These images are respectively named "Scanner image", "Radiologic image", "Echo graphic image", "Mammographic image"; these images are the same size (512 × 512). The use of the audio signal as a brand is indeed information about the patient (name, surname, diagnosis, etc.) (Figure 2).

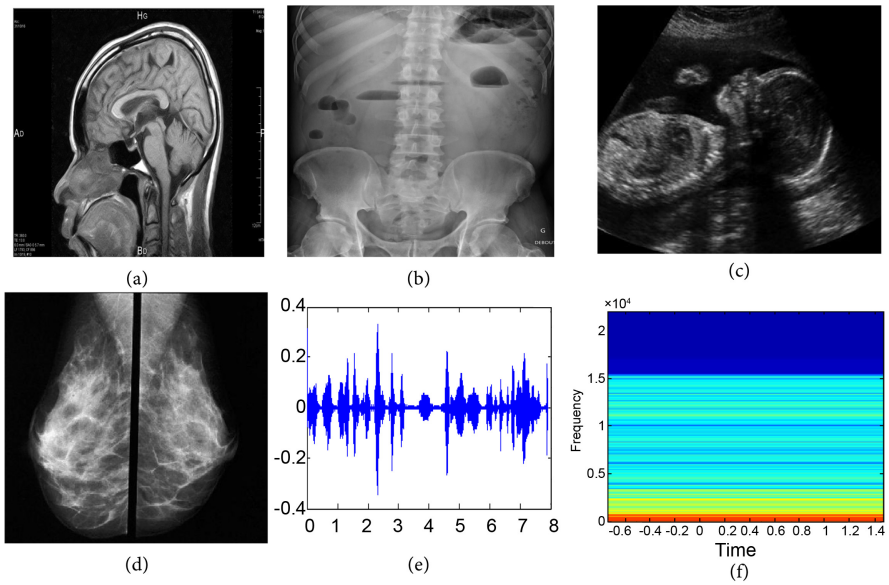


Figure 2. (a) Scanner image, (b) Radiologic image, (c) Echographic image, (d) Mammographic image, (e) Watermark signal, (f) Spectrogram of watermark signal.

4.1. Test of Imperceptibility: PSNR and SSIM

In order to show the differences between the original and watermarked images, the signal-to-noise ratio (PSNR) and the structural similarity index (SSIM) are used [30]. The PSNR indicates the destruction rate while the SSIM is used to express the level of similarity ([31] [32]). These two metrics are used after embedding process.

Peak-Signal-To-Noise-Ratio (PSNR) is defining as follow:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255\times 255}{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[I_1(x,y)-I_2(x,y)\right]^2}\right) \tag{17}$$

where I_2 is watermarked image and I_1 is original image. Bigger the PSNR is better the watermark conceals is [33].

The SSIM metric is defined by the following equation:

$$\mathrm{SSIM}(O,W) = \frac{\left(\mu_y\mu_x + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{18}$$

σ_x and σ_y are the mean intensity of x and y. In the same time σ_x^2 and σ_y^2 are respectively variance of x and y [33]. σ_{xy} is the covariance of x and y. The averages of x and y are μ_y and μ_x. Variables C_1 and C_2 are used to stabilize the division with weak denominator. The value of SSIM varies between −1 and 1, where the maximum value, *i.e.*, 1 is obtained for two similar images [33].

Based on the results of this **Table 1**, it can be concluded that the destruction of images is acceptable after embedding process.

4.2. Robustness against Attacks

Bit Error Rate (BER) is one of many metrics use to verified the robustness of the proposed algorithm, we use it, in our case. It's calculated between original watermark and the extracted watermark after applying attacks on the watermarked images [33]. The bit error rate is calculated by:

$$\mathrm{BER}(W, EW) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j) + EW(i,j)}{m\times n} \tag{19}$$

where W is the original watermark and EW is the extracted watermark. m and n are the size of the original watermark [34].

Table 1. Presents the PSNR and SSIM values.

	Watermarked scanner image			Watermarked Radiographic image			Watermarked Image Echo graphic Image			Watermarked image mammographic		
	A	PSNR	SSIM	α	PSNR	SSIM	α	PSNR	SSIM	α	PSNR	SSIM
0.1	0.1	59.60	0.98	0.1	61.32	0.97	0.1	55.76	0.99	0.1	62.87	0.99
0.2	0.2	58.12	0.99	0.2	61.06	0.98	0.2	55.07	0.98	0.2	62.01	0.97
0.4	0.4	57.86	0.97	0.4	59.44	0.99	0.4	54.01	0.97	0.4	61.23	0.97
0.6	0.6	56.21	0.98	0.6	59.17	0.98	0.6	53.32	0.9	0.6	59.14	0.98

Another statistic parameter use is Normalized Correlation (NC) which measures the similarity and difference between original watermark and extracted watermark. Generally, NC obtained between 1 and 0.7 is acceptable [35].

Another statistic parameter use is Normalized Correlation (NC) which measures the similarity and difference between original watermark and extracted watermark. Generally NC obtained between 1 and 0.7 is acceptable.

$$\mathrm{NC} = \frac{\sum_{i=0}^{n} \mathrm{Or\_watermark} \times \mathrm{Ex\_watermark}}{\left(\sum_{i=0}^{n} \mathrm{Or\_watermark} \times \sum_{i=0}^{n} \mathrm{Ex\_watermark}\right)^{\frac{1}{2}}} \tag{20}$$

Or_watermark is original watermark, Ex_watermark is extracted watermark.

Table 2 shows SSIM and BER results after applying cropping 20% and salt & pepper attacks on the watermarked images.

Table 2. Presents the BER, NC and SSIM values.

Attacks	Watermarked scanner image			Watermarked Radiographic image			Watermarked Image Echo graphic Image			Watermarked image mammographic		
	BER	NC	SSIM	BER	NC	SSIM	BER	NC	SSIM	BER	NC	SSIM
No attack	1.00	1.00	0.98	0.92	0.94	0.97	0.86	0.95	0.99	1.00	0.99	0.99
Gaussian filter [2 × 2]	0.34	0.93	0.97	3.06	0.34	0.93	0.97	0.96	0.98	0.61	0.91	0.97
Gaussian filter [5 × 5]	0.84	0.82	0.92	0.44	0.84	0.82	0.92	0.92	0.97	0.23	0.97	0.97
Gaussian noise [0.001]	0.54	0.92	0.98	0.77	0.54	0.92	0.98	0.94	0.9	0.74	0.93	0.98
Gaussian noise [0.1]	0.45	0.67	0.89	0.33	0.45	0.67	0.89	0.65	0.71	0.81	0.65	0.77
Salt & pepper (density = 0.01)	0.69	0.54	0.78	0.77	0.69	0.54	0.77	0.69	0.54	0.77	0.79	0.64
Salt & pepper (density = 0.1)	0.78	0.45	0.89	0.66	0.73	0.65	0.88	0.78	0.45	0.89	0.66	0.55
Resizing (scale = 0.3)	0.67	0.81	0.89	0.87	4.67	0.89	0.89	3.67	0.81	0.82	0.67	0.88
Resizing (scale = 0.1)	0.31	0.78	087	0.78	3.11	0.78	0.87	3.11	0.78	0.87	0.91	0.75
Median filter [3 × 3]	0.67	0.98	0.93	0.98	0.67	0.98	0.93	0.67	0.98	0.93	0.87	0.98
Median filter [5 × 5]	2.44	0.90	0.96	0.90	2.44	0.90	0.96	2.44	0.90	0.96	0.44	0.88
Rotation 10˚	4.27	0.89	0.91	0.89	4.27	0.89	0.91	4.27	0.89	0.91	0.89	0.88
Rotation 30˚	3.49	0.87	0.78	0.87	4.41	0.84	0.79	3.49	0.73	0.78	0.91	0.78

4.3. Comparison of Obtained Results

In this section we use many different types of attacks (like Gaussian), image processing attacks (resizing, rotation) and hybrid attacks (like salt & pepper and Gaussian filter)to demonstrate the robustness of the suggested watermarking algorithm on the watermarked images and then extracts the embedded watermarks. The average results of these tests are shown in **Table 2**. In the above table, focused of obtained results SSIM, NC and BER tests, we can conclude that the presented watermarking approach has better robustness against attacks in the embedding and the extracting processes of the proposed approach [35].

Tests results of our scheme are compare with the results of two other researchers scheme ([36] [37]), these results are better than the two others methods.

Figure 3 and **Table 3** show the results under different scale factor, the results of PSNR in our case are superior to 50 which denoted the robustness and the imperceptibility of the proposed scheme.

The difference and one advantage of our scheme is the use of audio logo which is transform in 2D then DCT transformed. This watermark is not easily recognizable.

4.4. Results of Obtained Watermarked and Encrypted Images

In this section, we present the obtained visual results after the conjoint phase of watermarking and encryption of the proposed algorithm. **Figures 4-7** show that effectively the watermark is invisible and the encryption is realized. The two mains objectives for medical images security, imperceptibility and confidentiality are satisfied.

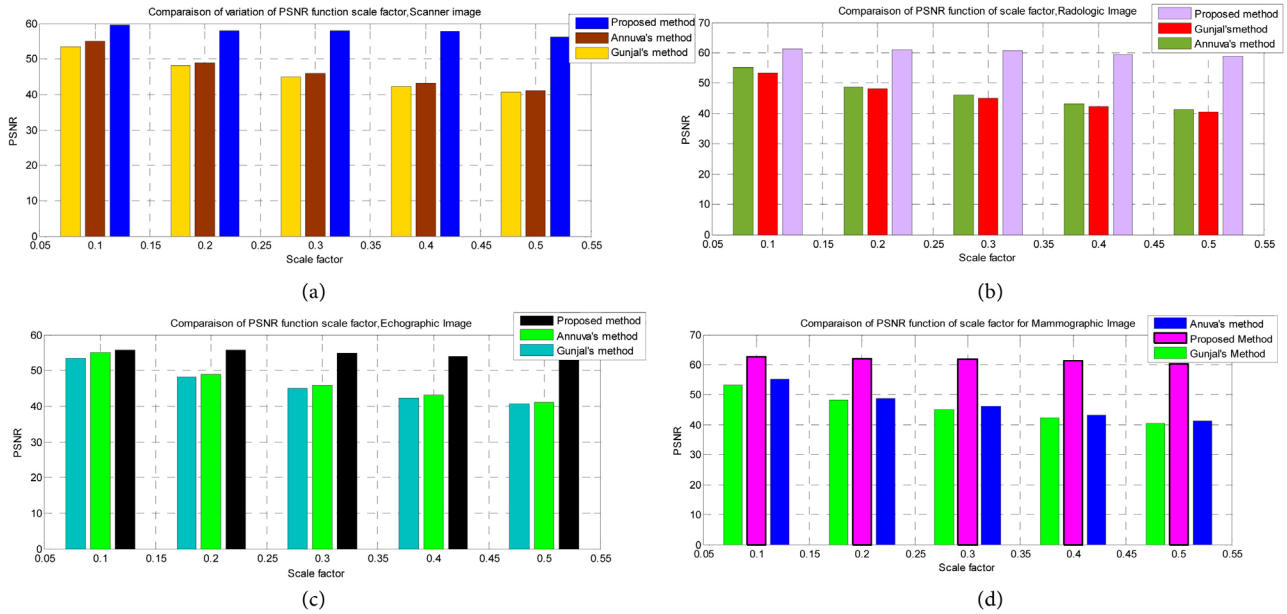
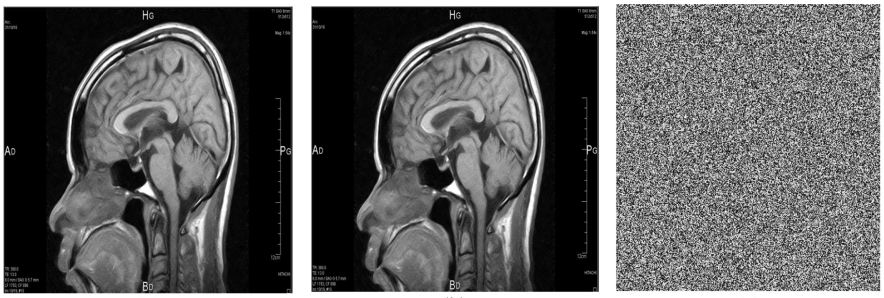


Figure 3. Diagram variations of PSNR with scale factor for different watermarked images, (a) Watermarked scanner image, (b) Watermarked radiographic image, (c) Watermarked echographic image, (d) Watermarked mammographic.

Table 3. Comparison of proposed Scheme with Sunjay *et al.* [38].

Attacks	Sanjay *et al.* [38]		Proposed Algorithm	
	PSNR	NC	PSNR	NC
Median Filtering	34.95	0.92	36.24	0.94
Salt and Pepper Noise addition	25.23	0.99	27.15	0.89
Resizing	34.84	0.92	31.10	0.98
Brightness adjustment	29.04	0.93	31.10	0.98
Cropping	11.55	0.83	13.01	0.81
Rotation	10.86	0.92	12.01	0.93

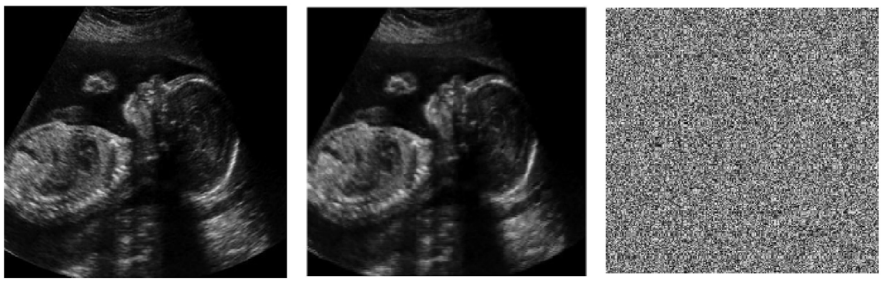


(a) (b) (c)

Figure 4. (a) Host scanner image, (b) Watermarked image, (c) Encrypted image.

(a) (b) (c)

Figure 5. (a) Host radiographic image, (b) Watermarked image, (c) Encrypted image.

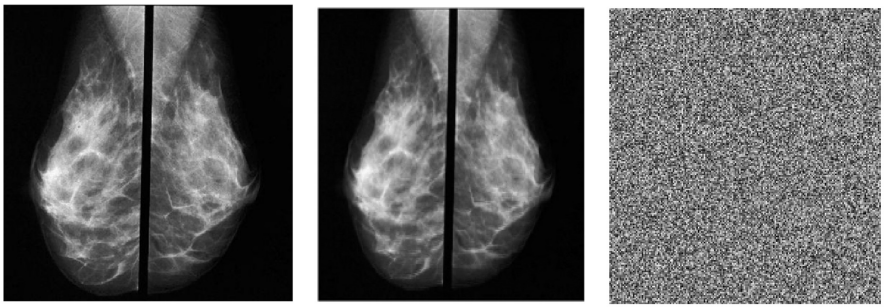


(a) (b) (c)

Figure 6. (a) Host echographic image, (b) Watermarked image, (c) Encrypted image.

4.5. Security Analysis, Key Sensitivity Test

The secret key sensitivity is an essential characteristic for a good encryption-system; it guarantees the safety and robustness against exhaustive attacks.



(a) (b) (c)

Figure 7. (a) Host mammographic image, (b) Watermarked image, (c) Encrypted image.

The largest key space is very important, because of failure brute-force attacks. Secret key for our proposed scheme is 3.93695629844, representing initial values of Logistic map, having 10^{-11} precision [38]. When a change of 1 digit is made in the secret key, the result is very different in term of encrypted and decrypted image 2 [39]. **Figures 8-11** show the results of key space analysis of our tests images.

4.6. Histogram Analysis

To get information about statistical properties of encrypted image, histogram analysis is a better way to obtain this information. Histogram of the encrypted image gives the distribution of pixels. **Figure 12** shows the histograms of the original images used, and **Figure 13** shows the histograms of these same encrypted images, where we note a uniform distribution, reflecting a good encryption.

4.7. Correlation Coefficient Analysis

Correlation analysis is very essential for the encryption phase and is carried out between the different pixel pairs of the original and encrypted images.

The correlation coefficients are calculated by the following formulas:

$$cov(u,v) = E\left(u - E(u)\right)\left(v - E(v)\right) \tag{21}$$

$$r_{uv} = \frac{cov(u,v)}{\left(\sqrt{D(u)}\right)\left(\sqrt{D(v)}\right)} \tag{22}$$

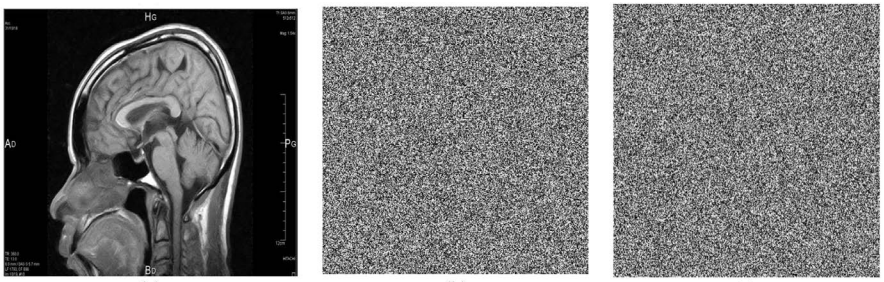
where u and v are intensities values of two adjacent pixels, r_{uv} is the correlation coefficient. $cov(u,v)$, $E(u)$ and $D(u)$ are given as follows

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i \tag{23}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}\left(u_i - E(u)\right)^2 \tag{24}$$

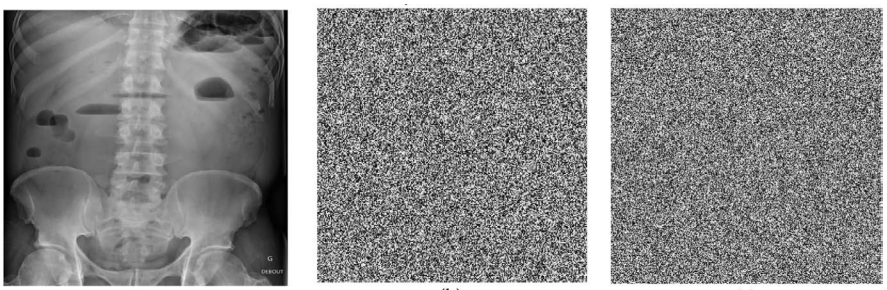
$$cov(u,v) = \frac{1}{N}\left(u_i - E(u)\right)\left(v_i - E(v)\right) \tag{25}$$

The pixels of an original image are strongly correlated in the horizontal,



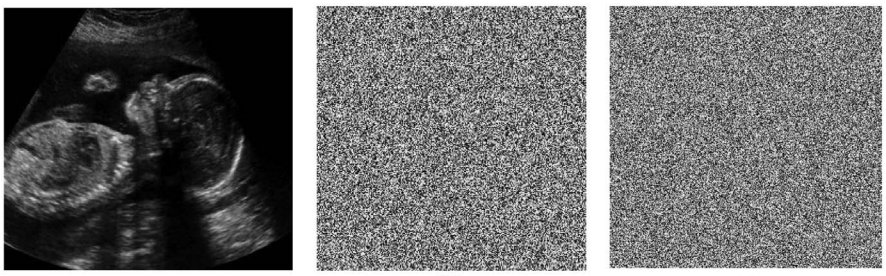
(a) (b) (c)

Figure 8. Test key sensitivity of image scanner: (a) Original image, (b) Encrypted image with the key = 3.93695629844, (c) Encrypted image with the key = 3.93695629845.



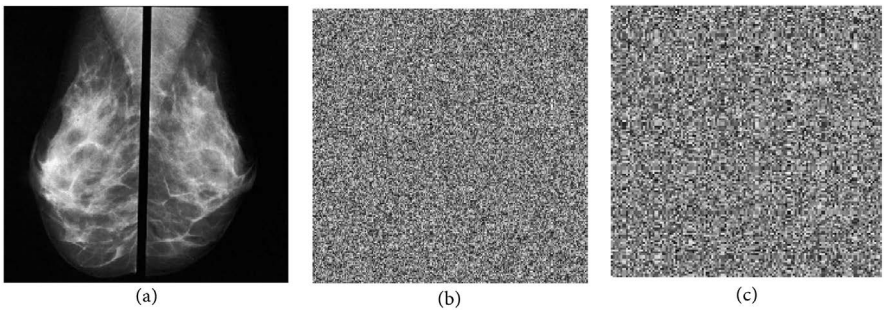
(a) (b) (c)

Figure 9. Test key sensitivity of image radiographic: (a) Original image, (b) Encrypted image with the key = 3.93695629844, (c) Encrypted image with the key = 3.93695629845.



(a) (b) (c)

Figure 10. Test key sensitivity of image Echographic: (a) original image, (b) Encrypted image with the key = 3.93695629844, (c) Encrypted image with the key = 3.93695629845.



(a) (b) (c)

Figure 11. Test key sensitivity of image Mammographic: (a) original image, (b) Encrypted image with the key = 3.93695629844, (c) Encrypted image with the key = 3.93695629845.

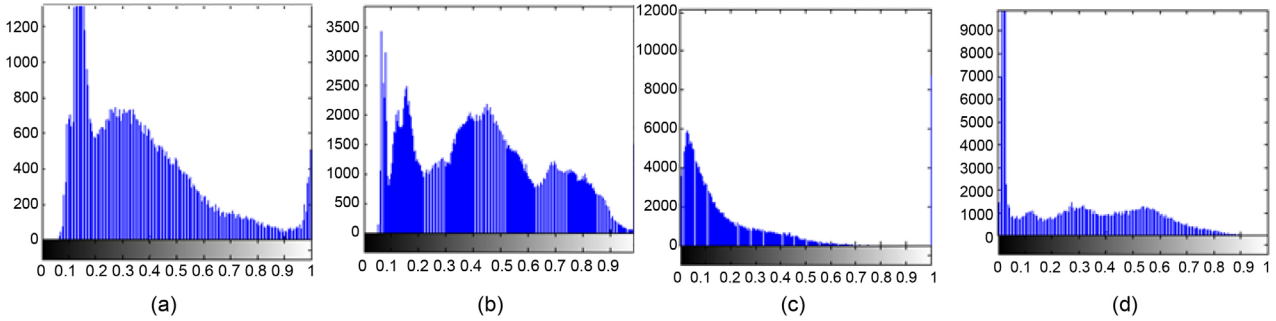


Figure 12. Histograms analysis: (a) Histogram of original scanner image, (b) Histogram of original radiographic image, (c) Histogram of original echographic image, (d) Histogram of original mammographic image.

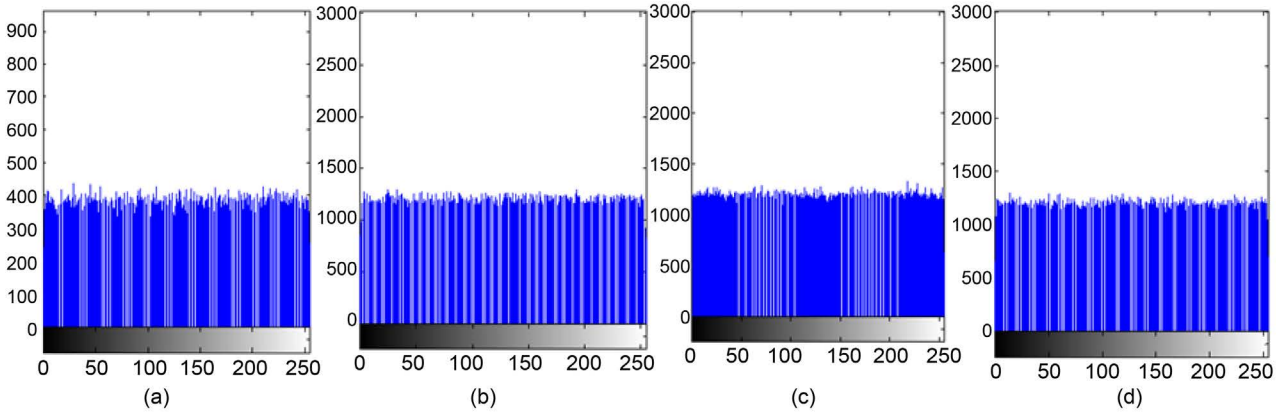


Figure 13. Histograms analysis: (a) Histogram of encrypted scanner image, (b) Histogram of encrypted radiographic image, (c) Histogram of encrypted echographic image, (d) Histogram of encrypted mammographic image.

vertical and diagonal directions. In order to know whether a cryptographic system should produce encrypted images without any correlation between adjacent pixels. Adjacent pixel correlation coefficients for horizontal, vertical and diagonal directions respectively, were calculated. **Figure 14** shows the results of the horizontal correlation of the original image and **Figure 15** shows the encrypted image.

It's remarkable in **Figure 14**. The pixels are concentrated in a particular area of original image. It means that the correlation is important, but in case of **Figure 15**, the pixels are not concentrated in one part of encrypted image means that the correlation is low. Some correlation coefficients are mentioned in following **Table 4**. The values of correlation coefficients are very less under 1. These give a conclusion that the encryption algorithm is very robust.

4.8. Differential Analysis

This test gives the sensibility of encrypted image referred to original image. For this, we encrypted both images (I_{01}, I_{02}) which are different by one pixel, and then Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are calculated. NPCR represents the amount of pixels changed when one pixel is change [39].

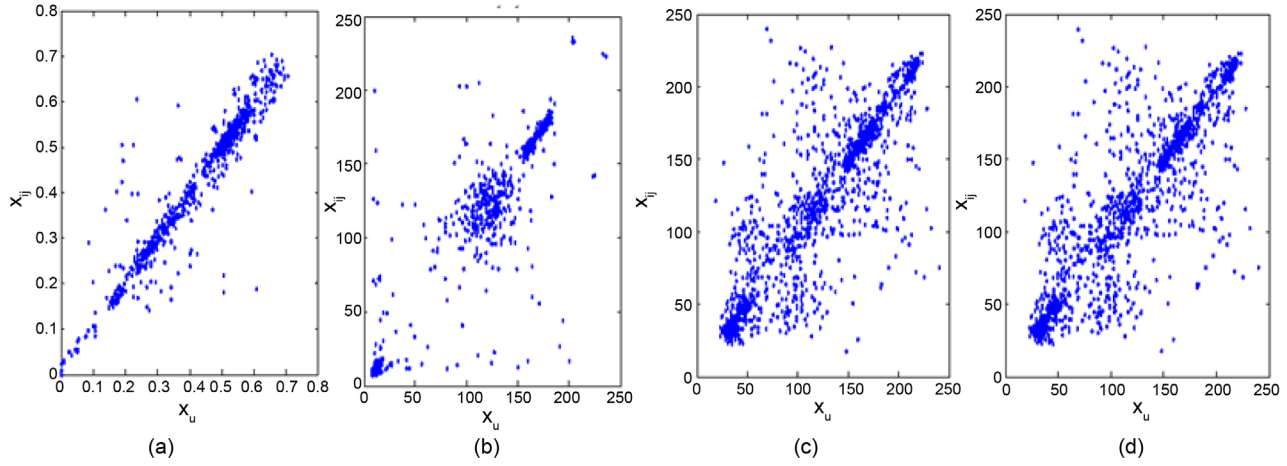


Figure 14. Correlation analysis: (a) Correlation analysis original scanner image, (b) Correlation analysis original radiographic image, (c) Correlation analysis original Echographic image, (d) Correlation analysis original mammographic image.

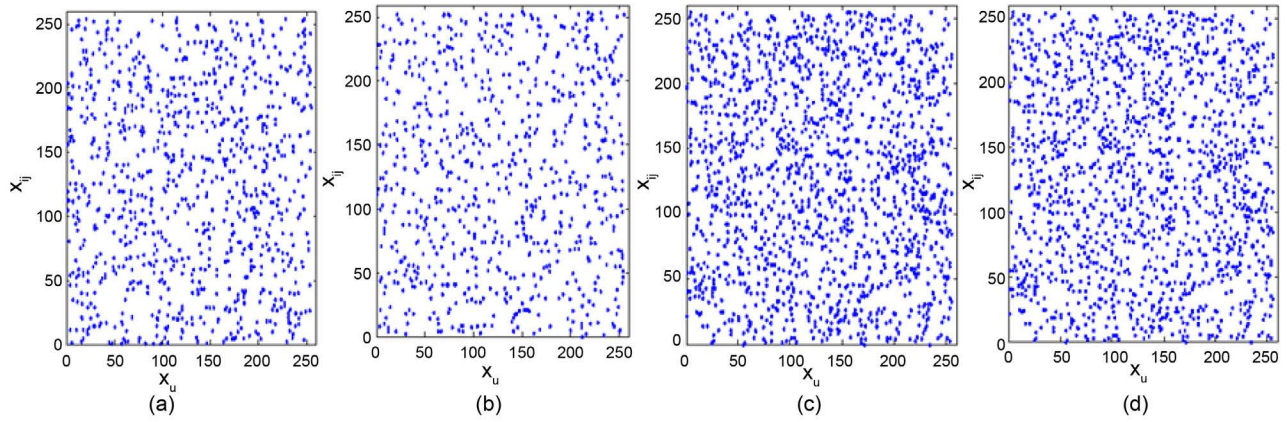


Figure 15. Correlation analysis: (a) Correlation analysis encrypted scanner image, (b) Correlation analysis encrypted radiographic image, (c) correlation analysis encrypted echographic image, (d) Correlation analysis Encrypted image.

Table 4. Correlation coefficients of two adjacent pixels of encrypted images.

Images	Horizontal	Vertical	Diagonal
Scanner image	0.0018	−0.0005	0.0031
Radiographic image	0.0119	0.0067	0.0045
Echographic image	0.0283	0.0044	−0.0033
Mammographic image	0.0018	0.0072	0.0051

$$\mathrm{NPCR} = \frac{\sum_{i=0}^{H}\sum_{j=0}^{L} D_j}{H \times L} \tag{26}$$

$$\text{With} \quad D_{i;j} = \begin{cases} 1 & \text{if } I_{01} \neq I_{02} \\ 0 & \text{if } I_{01} = I_{02} \end{cases}$$

$$\mathrm{UACI} = \frac{1}{H \times L}\sum_{i=0}^{H}\sum_{j=0}^{L} \frac{I_{01}(i,j) - I_{02}(i,j)}{2^8 - 1} \tag{27}$$

Table 5 gives the values obtained after tests for originals images.

The obtained results of NPCR are around 90% for all four tests encrypted images, in the same time results of UACI are around 40%. We can say that our algorithm is really satisfactory in term of robustness and confidentiality, better aspect of medical image security.

4.9. Speed Analysis

Speed of encryption and decryption is also use to characterize scheme. In our case the time results are obtained with computer having the following specifications Dell core Duo E7200 @2GHz, 1.96 GB RAM. Table 6 shows the time of encryption and decryption. This time varies depending on the image used.

4.10. Comparison Analysis

The calculation of the entropy is a statistical parameter of the image. It is given by the following formula:

$$H(m) = \sum_{i=10}^{r-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{28}$$

where $p(m_i)$ represents the probability of pixel m_i. Bits is expression of Entropy. We can have 2^8 bits, where each pixel in the image is represented by 8 bits. Following tables give the comparison of entropy with other methods.

For above tables the pertinence of the proposed method is proved, our method after the phase of frequential watermarking with adding audio signal make encryption by the technique of permutation and confusion, function of numbers of iterations. The main advantage of the proposed method is the sensitivity to initials conditions which in this case are keys of encryption. The same keys are indispensable for decryption phase.

Table 5. NPCR and UACI.

Images	NPCR (%)	UACI (%)
Scanner image	97.56	41.04
Radiographic image	98.55	42.34
Echographic image	98.33	43.56
Mammographic image	99.87	43.02

Table 6. Encrypted and decrypted times.

Images	Encrypted time (s)	Decrypted time (s)
Scanner image	14	31
Radiographic image	17	34
Echo graphic image	15	32
Mammographic image	18	36

5. Conclusion

We have proposed in this paper a method using chaos encryption based to solution of Vershult model combined with non-blind watermarking. This method consists of two mains phases; the first one is the non-blind watermarking associated with an audio signal. The second phase consists of encrypt watermarked image with logistic map knowing initials conditions, number of iterative conditions to generate chaos parameters. The results of PSNR, SSIM, NC, BER and correlation coefficients NPCR, UACI prove the imperceptibility and the robustness of your algorithm. Further research can be done in the following areas to improve the security of the medical images, as far as intelligent reversible watermarking is concerned. In the future, we intend to explore its ability to be robust against a specific attack through its learning mechanism. Reversible watermarking is also susceptible to different attacks in real watermarking applications. We intend to incorporate single attack information in its learning mechanism first and later enhance it to a series of attacks. Another important aspect that could be taken into account is the security of the watermark itself. For this purpose, different encryption strategies, such as Petri reseau encryption, can be employed on the watermark before embedding. Further research could also focus on compressibility. When compression is applied after encryption, the randomness of the ciphertext will greatly reduce the amount of compression achieved.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Michel, D. and William, P. (2001) Transfert sécurisé d'images par combinaison de techniques de cryptographie et de tatouage. *Proc. Colloq. Compression Représentation Des Signaux Audiovisuels*, *CORESA*'01, Dijon, Novembre 2001, 1-5.

[2] William, P. and Jose, M.R. (2006) Transfert sécurisé d'images médicales par codage conjoint: Cryptage sélectif par AES en mode par flotet compression JPEG, Traitement, 2006.

[3] Mei, X.J. and Sukangand, L. (2009) A Digital Watermarking Algorithm Based on DCT and DWT. *Proceedings of the 2009 International Symposium on Web Information Systems and Applications*, Nanchang, 22-24 May 2009, 104-107.

[4] Mitra, M.S.G. and Gunjan, P. (2012) A Multi-Resolution Watermarking Based on Contourlet Transform Using SVD and QR Decomposition. *International Conference on Recent Advances in Computing and Software Systems*, Chennai, 25-27 April 2012, 135-140. https://doi.org/10.1109/RACSS.2012.6212712

[5] Noura, H. (2012) Conception et simulation des générateurs,crypto-systèmes et fonctions de hachage basés chaos performants, Université de Nantes, France.

[6] Al-Maadeed, T.A. and Ali, A. (2013) A New-Based Image-Encryption and Compression Algorithm. *Journal of Electrical and Computer Engineering*, **2012**, Article ID: 179693. https://doi.org/10.1155/2012/179693

[7] Mousavi, S.M. and Naghsh, A. (2014) Watermarking Techniques Used in Medical Images: A Survey. *Journal of Digital Imaging*, **27**, 714-729. https://doi.org/10.1007/s10278-014-9700-5

[8] Qiwei (2012) A Novel DWT Based Blind Watermarking for Image Authentication. *International Journal of Network Security*, **14**, 223-228.

[9] William, P. and Michel, D. (2001) Tatouage d'images cryptées pour l'aide au télédiagnostic. Actes Colloq. 18th colloque Trait. Du Signal Des Images, GRETSI, Groupe d'Etudes Du Trait. Du Signal Des Images, Toulouse, France, 2001.

[10] Gokcen, C.L.C. (2016) Robust Chaotic Digital Image Watermarking Scheme Based on RDWT and SVD. *International Journal of Image*, *Graphics and Signal Processing*, **8**, 58-67. https://doi.org/10.5815/ijigsp.2016.08.08

[11] Anand, U.C.N. (1998) Watermarking Medical Images with Patient Information. *Proceedings of the* 20*th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. *Vol.* 20 *Biomedical Engineering towards the Year* 2000 *and Beyond*, Hong Kong, 1 November 1998, 703-706. https://doi.org/10.1109/IEMBS.1998.745518

[12] Coatrieux, G., Puentes, J., Lecornu, L. and Cheze, L. (2005) Low Distortion and Reversible Watermark Application to Angiographic Images of the Retina. *Proceedings IEEE EMBC Conference*, Shanghai, 1-4 September 2005, 2224-2227. https://doi.org/10.1109/IEMBS.2005.1616905

[13] Nyeem, H. and Boles, W. (2014) Digital Image Watermarking: Its Formal Model, Fundamental Properties and Possible Attacks. *EURASIP Journal on Advances in Signal Processing*, **2014**, Article No. 135. https://doi.org/10.1186/1687-6180-2014-135

[14] Nyeem, C.B.W. and Boles, W. (2011) Developing a Digital Image Watermarking Model. *International Conference on Digital Image Computing*: *Techniques and Applications*, Noosa, 6-8 December 2011, 468-473. https://doi.org/10.1109/DICTA.2011.85

[15] Fotopulos, A.N.S. (2001) A Subband-DCT Approach to Image Watermarking. 10*th European Signal Processing Conference*, Tampere, 4-8 September 2000.

[16] Hyung, S.K. (2003) Invariant Image Watermark Using Zernike Moments. *IEEE Transactions on Circuits and Systems for Video Technology*, **13**, 766-775. https://doi.org/10.1109/TCSVT.2003.815955

[17] Thirugnanam, S.A.G. (2010) Wavelet Packet Based Robust Digital Image Watermarking and Extraction Using Independent Component Analysis. *International Journal of Signal & Image Processing*, **1**, 80-87.

[18] Yuan, Y. and Decai, H. (2006) An Integer Wavelet Based Multiple Logo- Watermarking Scheme. *First International Multi-Symposiums on Computer and Computational Sciences*, Hanzhou, 20-24 June 2006, 1-5. https://doi.org/10.1109/IMSCCS.2006.187

[19] Mohamed, M. (2013) A Proposed Security Technique Based on Watermarking and Encryption for Digital Imaging and Communication in Medicine. *Egyptian Informatics Journal*, **14**, 1-13. https://doi.org/10.1016/j.eij.2012.11.002

[20] Mohammad, R.K. (2011) An Effective Chaos-Based Image Watermarking Scheme Using Fractal Coding. *Procedia Computer Science*, **3**, 89-95. https://doi.org/10.1016/j.procs.2010.12.016

[21] Valandar, M., Barani, J. and Ayubi, P. (2019) A Blind and Robust Color Images Watermarking Method Based on Block Transform and Secured by Modified 3-Dimensional Hénon Map. *Soft Computing*, **24**, 771-794.

[22] Barn, M., Bartolli, F. and Cappellini, V. (1998) A DCT-Domain System for Robust Image Watermarking. *Signal Processing*, **66**, 357-372. https://doi.org/10.1016/S0165-1684(98)00015-2

[23] Ruanaidh, T.P. (1998) Rotation, Scale, and Translation Invariant Spread Spectrum Digital Image Watermarking. *Signal Processing*, **66**, 303-317. https://doi.org/10.1016/S0165-1684(98)00012-7

[24] Zhao, W.L. and Chen, G. (2004) A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm. *Chaos Solitons and Fractals*, **22**, 47-54. https://doi.org/10.1016/j.chaos.2003.12.104

[25] Somaya, A.T.A. and Afnan, A. (2012) A New Chaos-Based Image-Encryption and Compression Algorithm. *Journal of Electrical and Computer Engineering*, **2012**, Article ID: 179693. https://doi.org/10.1155/2012/179693

[26] Noura, A., Ntsama, P.E. and Bitjoka, L. (2017) Non-Blind Image Watermarking Scheme Using Bi-Dimensional Empirical Mode Decomposition, Dwt, Dct and Fuzzy Set. *Global Journal of Engineering Science and Researches*, **5**, 32-39.

[27] Gopi, E.S. (2007) Algorithm Collections for Digital Signal Processing Applications Using Matlab, 2007.

[28] Jean, M.R. and William, P. (2003) Sécurisation d'image par crypto-tatouage, CORESA: Compression et Représentation des Signaux. 9*ème Conférence Natl. Compression Représentation Des Signaux Audiovisuels*, Lille, 215-218.

[29] Verhulst, P.F. (1838) Notice sur la loi que la population poursuit dans son accroissement. Correspondance Mathématique et Physique. Books.google.com.

[30] Noura, A., Ntsama, P.E. and Bitjoka, L. (2015) Non-Blind Wavelet Packet Watermarking Scheme Using Radon Transform. *Advances in Computer Science and Engineering*, **15**, 41-55. https://doi.org/10.17654/CS015120041

[31] Wei, X. (2014) Image Encryption Based on Chaotic Map and Reversible Integer Wavelet Transform. *Journal of Electrical Engineering*, **65**, 90-96. https://doi.org/10.2478/jee-2014-0013

[32] Zhang, Y. (2011) Image Encryption with Logistic Map and Cheat Image. 3*rd International Conference on Computer Research and Development*, Shanghai, 11-13 March 2011, 97-101. https://doi.org/10.1109/ICCRD.2011.5763981

[33] Parekh, M., Bidani, S. and Santhi, V. (2018) Spatial Domain Blind Watermarking for Digital Images. In: *Progress in Computing, Analytics and Networking*, Springer, Berlin, 519-527. https://doi.org/10.1007/978-981-10-7871-2_50

[34] Zhou, N.R., Hou, W.M.X., Wen, R.H. and Zou, W.P. (2018) Imperceptible Digital Watermarking Scheme in Multiple Transform Domains. *Multimedia Tools and Applications*, **77**, 30251-30267. https://doi.org/10.1007/s11042-018-6128-9

[35] Valandar, M.Y., Barani, M.J., Ayubi, P. and Aghazadeh, M. (2019) An Integer Wavelet Transforms Image Steganography Method Based on 3D Sine Chaotic Map. *Multimedia Tools and Applications*, **78**, 9971-9989. https://doi.org/10.1007/s11042-018-6584-2

[36] Annuva, C. (2014) Color Image Watermarking Technique by Featuring Joint DWT-DCT Domain in YIQ Color Space. *International Journal of Research in Electronics AND Computer Engineering*, **3**, 1-6.

[37] Gunjal, B.L. (2011) Secured Color Image Watermarking Technique in DWT-DCT

Domain. *International Journal of Computer Science, Engineering and Information Technology*, **1**, 36-44.

[38] Sunjay, R. (2011) A Chaos-Based Robust Watermarking Algorithm for Rightful Ownership Protection. *International Journal of Image and Graphics*, **11**, 471-493. https://doi.org/10.1142/S0219467811004263

[39] Shyamsunder, S. (2011) Image Encryption and Decryption Using Chaotic Maps and Modular Arithmetic. *American Journal of Signal Processing*, **1**, 24-33.