International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 6, December 2017, pp. 3385~3394
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i6.pp3385-3394

New Watermarking/Encryption Method for Medical Images Full Protection in m-Health

Mohamed Boussif[1], Nourredinne Aloui[2], Adnene Cherif[3]
Department of Physics, Faculty of Sciences of Tunis, Farhat Hached University, Tunisia

Article Info

Article history:

Received Feb 15, 2017
Revised Jun 19, 2017
Accepted Jul 2, 2017

Keyword:

Medical images
Security
Watermarking
Encryption
Embedded systems
m-Health

ABSTRACT

In this paper, we present a new method for medical images security dedicated to m-Health based on a combination between a novel semi reversible watermarking approach robust to JPEG compression, a new proposed fragile watermarking and a new proposed encryption algorithm. The purpose of the combination of these three proposed algorithms (encryption, robust and fragile watermarking) is to ensure the full protection of medical image, its information and its report in terms of confidentiality and reliability (authentication and integrity). A hardware implementation to evaluate our system is done using the Texas instrument C6416 DSK card by converting m-files to C/C++ using MATLAB coder. Our m-health security system is then run on the android platform. Experimental results show that the proposed algorithm can achieve high security with good performance.

Corresponding Author:

Mohamed Boussif,
Department of Physics, Faculty of Sciences of Tunis,
Farhat Hached University,
El Manar, PB 2092, Belvedere, Tunisia.
Email: boussifmohamed1989@gmail.com

1. INTRODUCTION

The evolution of telemedicine has facilitated the sharing and remote access of patient data from m-Health (mobile health) platform which is one of the fastest growing areas of healthcare computing [1]. In particular, the medical images requires new means for security which can be adapted to this novelty (m-Health) to satisfy these classic terms: Confidentiality, Authentication, Integrity, and Availability. DICOM (Digital Imaging and Communications in Medicine) offers a low level of security, because the security of medical imaging within the DICOM system currently relies on old techniques which include the AES (Advanced Encryption Standard) and the 3DES (Triple Data Encryption Standard) and those two algorithms have a very high complexity. To solve this, many researchers have proposed different solution, between watermarking and encryption or the hybridization of both of them. Many methods have been proposed in the literature such as: Zhenxing Qian and Xinpeng Zhang [2] where the authors have proposed a reversible data hiding in encrypted domain.

A secure dissemination and protection of multispectral images based on encryption of watermarking image have been proposed by Sangita Zope-Chaudhari et al [3], Xiaochun Cao et al [4] proposed a high capacity reversible data hiding in encrypted domain, A robust watermarking method for compressed image in encrypted domain have been proposed by A. V. Subramanyam et al [5]. Dalel Bouslimi et al [6] have proposed a combined encryption watermarking system. Hitendra Suryavanshi et al [7] have proposed a digital image watermarking method using the wavelet transform. Nidhi Sethi et al [8] have proposed a cryptographic system for digital images. Barlian Henryranu Prasetio et al [9] have proposed simple algorithm for image encryption. G Rosline NesaKumari et al [10] have proposed an image watermarking scheme using chaotic system.

The rest of this paper is organized as follows. In Section 2, we present the proposed methods which is implemented in Section 3. Section 4, present the experimental results and the security analyze of the proposed algorithms. Before concluding in Section 6, we discuss the results which are compared with other methods in Section 5.

2. PROPOSED WATERMARKING/ENCRYPTION SYSTEM

In this section, we present the proposed security system for medical images. We start by the encryption process then the first proposed watermarking and the second proposed watermarking. we end with the combination of these three proposed aproachs.

2.1. Proposed imaging encryption schema

As shown in Figure 1, the encryption method manipulates the imaging by dividing it into blocks of 8x8 pixels. The i-th encrypted block is the exoring between the i-th block to be encrypted with the i-th block k. We obtain the block k by:

1) In the first block, i.e. i=1 the block k is initialized by the matrix product of the key K_E and, the addition of its transposed and V.
2) when, i>1, we obtain the block k using the function F which has as parameter, the sum of previous encrypted block, current block and the previous block k.

$$B_i^e = B_i \oplus F\left(B_{i-1}^e + B_{i-1}, k_{i-1}\right)$$

$$B_1^e = B_1 \oplus k_1 \quad (1)$$

$$k_1 = \left\lfloor K_E * \left(K_E + v\right)^{'} \right\rfloor \bmod 2^{dep}$$

where B the block to be encrypted, B^e the encrypted block and dep the imaging depth, K_E is a column vector used as key, and the function F is the N rotations of the operand on the right (ROR), the exoring of selected part (sub-block of size n_1) of block key and it's symmetric (also sub-block of size n_1), either 1 bit. F depend of the angle $B_{i-1}(l,c) + B_{i-1}^e(l,c)$ by$64/[n_1]^2$. The expression of F is defined as the following:

$$F\left(B_i^e, k_i\right) = N_i ROR\left(k_i(l,c) \oplus S_{k_i(l,c)}\right)$$
$$S_{k_i(l,c)} = k_i(9-l, 9-c) \quad (2)$$

where S the sub-block symmetric of selected sub-block. As shown in Figure 2, we determine the part to change (sub-block of size n_1) using the rest of division of the sum of preview block $B_{i-1}(l,c) + B_{i-1}^e(l,c)$ by$64/[n_1]^2$, which give the position of sub-block. Therefore, the block k is divided on sub-block of size n_1 the fast block is the block number 0 i.e. $k_i(1{:}\,n_1, 1{:}\,n_1)$, it's symmetric the block $k_i(9-1{:}\,9-n_1, 9-1{:}\,9-n_1)$, where the parameter equal n_1 to 0,1,2,4 or 8.

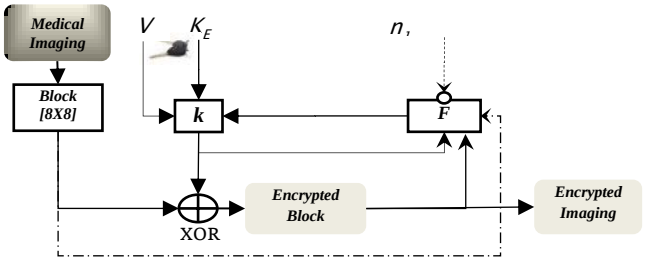

Figure 1. Scheme of the proposed encryption system. n_1 is the parameter of configuration of the system (the mode used in compression is for n_1=0). V and K_E are the key of encryption. F is given in Figure 3

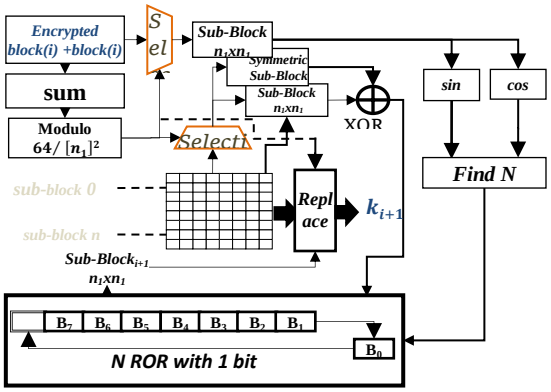

Figure 2. The proposed chaotic system of block key (the function F). The inputs of the system are n_1 and the sum of bloc i and its encrypted block, and the block key k_i, the output is the block key k_{i+1}

2.2. Proposed semi reversible robust hiding method

In this section, we hide the patient information in text form (Name, UID and the doctor report) in the corresponding imaging. We first start by giving the mixing function M which consists in inserting the bits w_i in a pixel of the image (see Figure 3). The expression of this function is:

$$M^{\varphi_i,f}(I_i,w_i)=\begin{cases}2k_i\dfrac{\pi}{f}-\dfrac{\varphi_i}{2f} & \text{if } w_i=1\\ (2k_i+1)\dfrac{\pi}{f}-\dfrac{\varphi_i}{2f} & \text{if } w_i=0\end{cases}$$
$$k_i=r\left(f\times\frac{I_i-\frac{\varphi_i}{2}}{2\pi}\right) \tag{3}$$

where r allow conversion to nearest integer. f and φ_i are the frequency and the i-th dephasing, respectively. $M^{\varphi_i,f}$ the mixing function. I_i and w_i are the pixel to be watermarked and the watermark bit, respectively. k_i is an integer. For writing the mixing function as a single equation we replace k with its expression in equation (3):

$$M^{\varphi_i,f}(I_i,w_i)=\left(\overline{w_i}+2\times r\left(f\frac{I_i-\frac{\varphi_i}{2}}{2\pi}\right)\right)\frac{\pi}{f}-\frac{\varphi_i}{2f} \tag{4}$$

where $\overline{w_i}$ is the complement of w_i. Now, we simplify the equation (4) to find the final mixed function as following:

$$M^{\varphi_i,f}(I_i,w_i)=\frac{\pi}{f}\left[\left(\overline{w_i}+2r\left(f\frac{I_i-\frac{\varphi_i}{2}}{2\pi}\right)\right)-\frac{\varphi_i}{2\pi}\right] \tag{5}$$

The reciprocal function of the mixing function which is used to extract the watermark from the image is given by the next equation:

$$w_{ex_i}=M^{-1^{\varphi_i}}(I_i)=\cos\left(f\times I_{w_i}+\frac{\varphi_i}{2}\right) \tag{6}$$

where I_{w_i} and w_{ex_i} are the i-th watermarked pixel and the i-th extracted watermark, respectively.

We use a chaotic system to provide the dephasing φ which must be a sequence of real numbers between -π and π depending on the insertion key k_w. φ depend on its previous state and the key k_w. φ_1 is initialized by the rest of the real division of k_w and π. $\varphi_{n\geq 2}$ is equal to the product of preview threshold term and the rest of division $\varphi_{n-1} + i \times k$ by π, the expression of the sequence is given in next expression:

$$\varphi_i = \begin{cases} s_i\left[(\varphi_{i-1} + i \times k_w) \bmod \pi\right] & for\ i \geq 2 \\ k_w \bmod \pi & for\ i = 1 \end{cases} \quad (7)$$

where S_i equal to -1 if $|\varphi_{i-1}|$ superior or equal to $\pi/2$ and equal to 1 if $|\varphi_{i-1}|$ inferior to $\pi/2$.

In the second part of this section, we use the mixing function M given in equation (5) to insert the binary coded text in the transformed image. As shown in Figure 4, the first step, consist to divide the image into blocks of size 8. For each block, we determine the 2D-DCT coefficient, then we select the lowest coefficients where we insert, bit by bit, the watermark which must be converted to binary code. The insertion process consists to add to the preview transformed block $T[block_{n-1}]$ the mixing function of the difference between the transformed block $T[block_n]$ and the preview transformed block $T[block_{n-1}]$, where T is the transformation in DCT-2D. In other words, we obtain the watermarked case of each block by the next expression:

$$W^{\varphi}_{T[B_n]_{i,j}} = T[B_{n-1}]_{i,j} + M^{\varphi_{i,j},f}\left(T[B_n]_{i,j} - T[B_{n-1}]_{i,j}, w_{i,j}\right) \quad (8)$$

where B_n,T, $M$and W are, respectively, the block n,the DCT-2D transformation, the mixing function and the watermarked block. The watermarking process start for $n = 2$, the first block of imaging is used for the watermarking of second block.

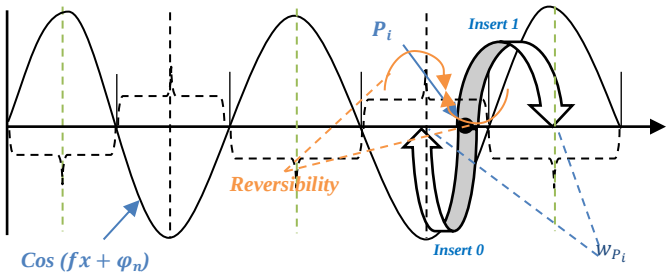

Figure 3. Principe of our mixed function method. P_i is the pixel to be watermarked. $\cos(fx + \varphi_n)$ is th scale of watermarking. We insert 1 if $w_i = 1$, and we insert 0 if $w_i = 0$.w_{P_i} is the watermarked pixel P_i

We have done a semi restitution (semi reversible) of the watermarked imaging, we use the following formula which is based on, the addition of π/f if the extracted bit w_{Ex} equal to 1, the subtraction of π/f if the extracted bit w_{Ex} equal to -1:

$$R^{\varphi}_{W_{T[B_n]_{i,j}}} = T[B_n]_{i,j} + \left[M^{-1^{\varphi_{i,j},f}}\left(T[B_n]_{i,j} - T[B_{n-1}]_{i,j}\right)\right]\frac{\pi}{f} \quad (9)$$

where R and M^{-1} are, respectively, the semi restituted block and the function of extraction which is given in equation (6).

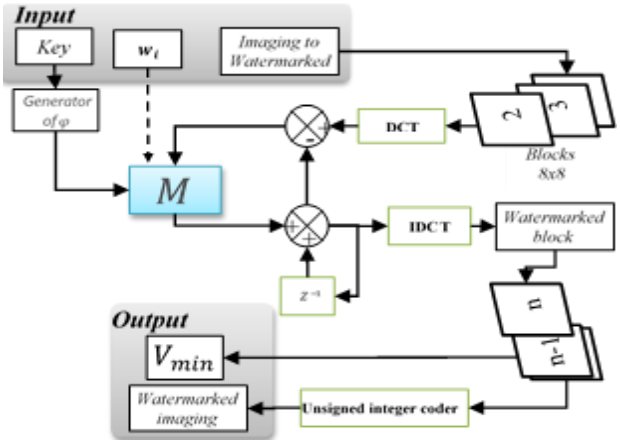

Figure 4. The proposed watermarking method scheme

In the first iteration the return string is initialized by the first DCT block coefficient of image to be watermarked. Therefore, the Insert procedure starts from block number 2. To note that the parameter f must be fixed between 0.3 and 0.9. The expression of M is given in equation (6) and z^{-1} is a retard delay with a block

2.3. Proposed fragile watermarking method

In this section, we use a second watermarking before encryption for integrity check in encrypted domain. So, we insert the imaging entropy, the variable V_{min} and the key K_w. The objectives of this second watermarking are: In the first, hide the key K_w and V_{min} which are used for insertion of medical report in imaging. In the second, securing the imaging in encrypted domain against tamper. Therefore, we use the classical fragile watermarking system which consists to insert the watermark in the LSB bits of imaging [11]-[12]. Since, there are several researches that are worked with the attack of this type of watermarking as in paper [13]-[14] we have obliged to secure this method using a novel proposed method which is based on the choice of pixel to watermarked which is done by a choosing key (we can use the encryption key K_E). To note that the quality in PSNR of image Lena watermarked by 144 bits is equal to 104. The K_w key must be encoded in 16 bits, each of V_{min} and the entropy H_w must be encoded in 64 bits. Therefore, the total bits which must be inserted is equal to 144 bits. The expression of watermarking process can be summarized as follows:

$$\begin{aligned} I_w(L_i, C_i) &= \left[I(L_i, C_i)\, and \left(2^{[dep-1]} - 1\right)\right] or \left[b_i\right] \\ L_i &= i \times fix\left(\frac{M}{l}\right) \\ C_i &= \left(K_E\left(i\, rem 8 + 1\right) + i\right) rem N + 1 \end{aligned} \tag{10}$$

where M and N are the sizes of the imaging to watermarked, respectively. l and dep, are the length of watermark and imaging depth, respectively. L_i and C_i the indices of pixel to watermarked, respectively. I, I_w and b are the imaging to watermarked, the watermarked imaging and the watermark, respectively. The function fix and rem, returns the integer part and integer division rest, respectively. In extractor level, we determine the extracted watermark by as following:

$$w_{ex}(i) = \left[I_w(L_i, C_i)\, and 1\right] \tag{11}$$

where W_{ex} the extracted watermark, the expression of L_i and C_i are given in equation (10). Using the key K_E, we determine the position of watermarked pixel, then, we extract the watermark w_{ex}.

2.4. Proposed combined encryption/watermarking schema

In this section, we combine the three-proposed system: encryption system with the watermarking methods. As illustrated in Figure 5, the medical imaging must be transformed into blocks of size 8x8, for

each block, we hide the patient information (as name, UID, diagnostic reporting) in the medical imaging (hiding method is illustrated in Section 3.2). We insert the key of watermarking K_w, the minimum value of image V_{min} and the entropy H image with the key K_E before the encryption process which consists to encrypt the watermarked image on block of size 8x8(encryption method is illustrated in Section 3.1). The insertion of the key K_w, V_{min} and the entropy are illustrated in Section 3.3. Therefore, the input of our overall Encryption/watermarking system are the medical imaging to watermarking/encryption, patient's information (name, UID, UIDs, diagnostic reporting), the two encryption keys K_E and V, the watermarking key K_w. The output of system is the watermarked encrypted imaging. In the decoding level, i.e. decryption/extraction process, we decrypt the watermarked encrypted imaging with the key K_E. Then, we extract $K_{w_{ex}}$ and the entropy $H_{I_{ex}}$, we verify the integrity of the imaging with the verification of the decrypted image entropy $H_{I_{dec}}$ and the extracted entropy $H_{I_{ex}}$.

$$\text{int}(10^n H_{I_{dec}}) - \text{int}(10^n H_{I_{ex}}) = 0 \quad (12)$$

Finally, if the imaging integrity is verified. we extract the information of patient and the medical reporting with the key $K_{w_{ex}}$. To noted that we have a good configuration for $n = 2$. i.e. we use two digits after comma.

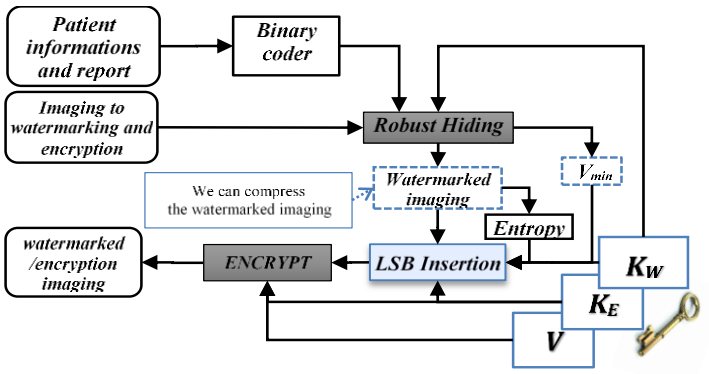

Figure 5. Proposed combined Watermarking/Encryption scheme

Robust Hiding is illustrating in Section 3.2. LSB Insertion is illustrating in Section 3.3. encrypt is illustrating in Section 3.1. Binary coder is the binary representation of ASCII code of each character. K_w is the watermarking key. K_E and V are the key of encryption

The watermarking/encryption schema proposed in this paper must be can merged with JPEG compression, because it's very used in standard DICOM, we describe the merging of JPEG schema, which is given in paper [15], as following steps: a) we hide the report and the information of patient in imaging as illustrated in Section 3.2, but, without inverse transformation IDCT. b) We quantify the watermarked coefficients of DCT with a uniform quantization. c) we insert the entropy of quantified coefficients and the K_w key in the quantified imaging. d) we encode the watermarked quantified imaging with Huffman coding. e) We encrypt the Huffman coding data, as illustrated in Section 3.1, with $n_1 = 0$.

3. IMPLEMENTATION ON EMBEDDED SYSTEMS

To implement the proposed schema on embedded system one must pass through the next three steps: In the first step, we implement the algorithm in Matlab tool. In the second step, after fixation of parameter and optimization of program, we convert the Matlab function to C/C++ code. In the final step, we use this function in the main project which allows the crypto-watermarking of medical images.

3.1. Build C/C++ functions from m-files functions

In this part, we convert m-files to C/C++ static library code using the application Coder of Matlab tool. In the first, we need to simplify the MATLAB code to be adapted to the embedded system, therefore, we must fixe all type of input and output variable of each function.

3.2. Implementation on C6416 DSK card

To implement the proposed system on card DSK C6416, we use CCS tool which allow debug C/C++ code in the card. In the first, we prepare the DSP/BIOS for real time data exchange (RTDX) which consist to allocate the memory in off-ship We use a first program which allow the initialization of all variable to zeros, then, charge the off-chip the imaging and the keys.

3.3. Implementation on Android OS

To implement the proposed system on Android OS, we use Android NDK (in Android Studio) tool which allows implement the parts C/C++ builder in Section IV.B on our application.

4. EXPERIMENTAL RESULTS AND SECURITY ANALYZE

Experiments were conducted on four sets of medical images of different modality, sizes and depth: Magnetic Resonance imaging (modality MR) of 560×560 pixels and 12-bit depth, Computed Tomography imaging (modality CT) of 512x512 pixels and 12-bit depth, Digital Radiography imaging (modality DX) of 2022x1736 pixels and 14-bit depth, Secondary Capture imaging (modality SC) of 224x176 pixels and 16-bit depth. Some samples of our dataset are given in Figure 6. Let us recall that for images encoded on 8, 12, 14 or 16 bits, our proposed watermarking/encryption system manipulates blocks of 8x8 pixels.

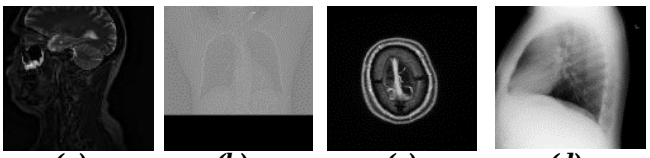

Figure 6. Samples of our images test sets. (a) Modality MR imaging. (b) Modality CT imaging. (c) Modality DX imaging. (d) Modality SC imaging

We decided to use the peak signal to noise ratio (PSNR) in order to measure the distortion between an imaging I and its watermarked imaging I_{wdec}:

$$PSNR(I, I_{wdec}) = 10Log_{10}\left(\frac{\left[2^{dep}-1\right]^2}{MSE}\right)$$
$$MSE(I, I_{wdec}) = \frac{1}{L}\sum_{k=1}^{L}\left[I(k) - I_{wdec}(k)\right]^2 \quad (13)$$

where L corresponds to the number of pixels of the image I, and dep corresponds to its depth. We decided to use the entropy H to measure the pixel variation for an image I, for a source, which is a discrete random variable I with 2^{dep} symbols, each symbol I_i has a probability P_i to appear, the entropy H of the I source is defined as:

$$H(I) = -\sum_{i=1}^{n} P_i \log_2(P_i) \quad (14)$$

We use the correlation coefficients NC to measure the distortion between the watermark w and the extracted watermark w_{ex}:

$$NC(w, w_{ex}) = \frac{Cov(w, w_{ex})}{\sigma_w \sigma_{w_{ex}}} \quad (15)$$

where $Cov(x, y)$ the covariance of x and y. σ_x is the standard deviation of x. Where $\bar{x}$ the average value of x. p_i the probability of x_i.

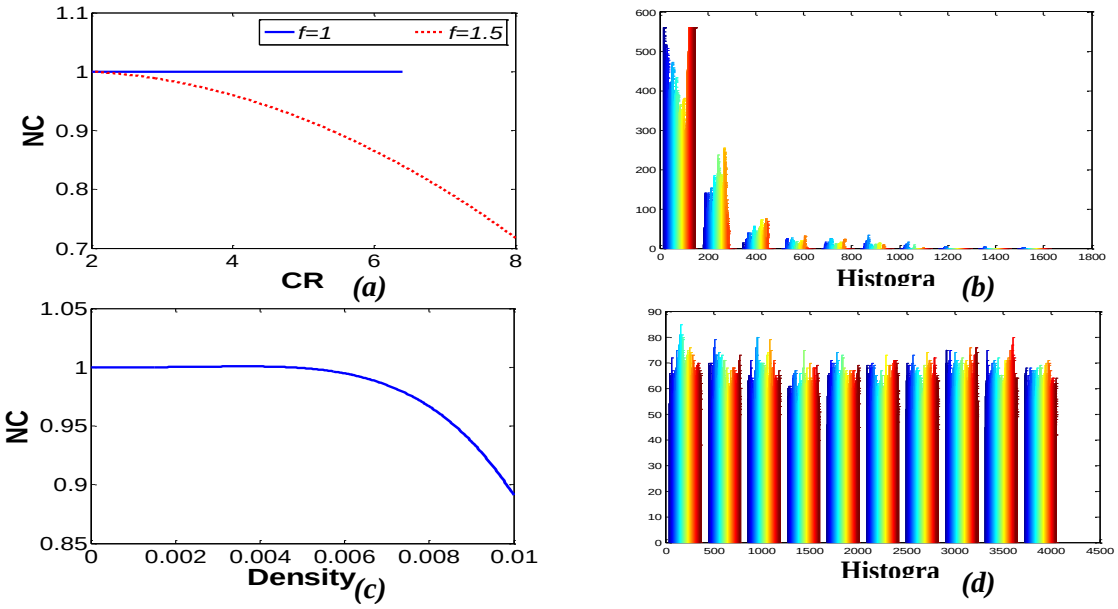

Figure 7. watermarking and encryption simulation. (a) Watermarking robustness to JPEG compression for f = 1 and f = 1.5. (b)Original imaging histogram. (d)encrypted imaging histogram for $n_1 = 2$. (c) Watermarking robustness to "salt & pepper" noise for f = 0.1

$$Cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)$$
$$\sigma_x=\sqrt{E\left[x^2\right]-E[x]^2}$$
$$E[x]=\sum_{i=1}^{n}x_i\,p_i \qquad (16)$$

The resistance of the proposed technique to differential attack is evaluated by comparing ciphered images obtained by the encryption of two minimally different plain images. It is desired that such ciphered images are substantially different. This is measured by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI), which are defined by:

$$NPCR = 100\frac{\sum D_{i,j}}{W\times H}$$
$$UACI = 100\sum\frac{\left|I_{1(i,j)}-I_{2(i,j)}\right|}{W\times H\times(2^d-1)} \qquad (17)$$

where I1 and I2 are the two ciphered images whose plain images have only one pixel difference; the grayscale values of the pixels at position (i,j) of I1 and I2 are, respectively, denote das I1(i,j) and I2(i,j); W and H correspond to the width and the height of the ciphered image, respectively; D(i,j) equal to 1 if I1(i,j) deferent to I2(i,j), 0 otherwise.

As shown in Figure 8. (b), (d), (f), (h) the visual aspect of images, in encrypted domain, is completely noisy. For verify the sensitivity of the encryption method, we decrypt the imaging test which minimally wrong key, we conclude that unique the encryption key can decrypt the encrypted images, also, in Figure 7(d), the histogram of encrypted imaging shows that the distribution of color in encrypted imaging is identical, which suggests that a statistical analysis would not be effective for the evaluation of the original images content. As shown in Table 1, the entropy, NPCR, and UACI of encrypted imaging is approach to 8,100, and 33, respectively. Therefore, the proposed encryption system can robust to entropy and differential attack.

As shown in Figure 8 (a), (c), (e), (g), the watermark is imperceptible and the average PSNR of watermarked images is equal to 55 (see Table 1). The robustness of the proposed watermarking system is evaluated by applied the JPEG compression and Noise attack, as shows in Figure 7(a), the normalized correlation coefficient NC close to 1, so, the watermarked compressed imaging MR is robust against JPEG compression for ratio factors equal to 6.4 the quality factor equals to 16%. Also, we test the proposed algorithm with noise attack, we conclude that the proposed robust to this type of attack (see Figure 7(c)).

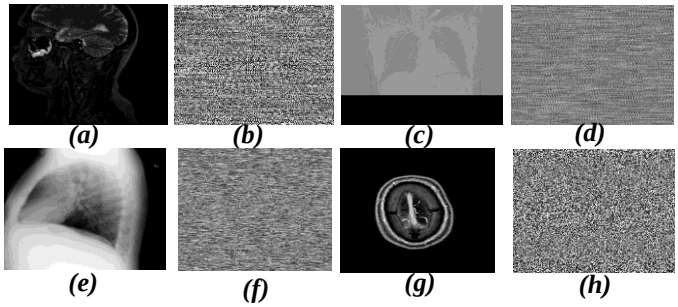

Figure 8. (a), (c), (e) and (g) are the watermarked images for the images in figure 6(a), (b), (c), (d), respectively, (b), (d) (f) and (h) are the encrypted watermarked images for the images in figure 6(a), (b), (c), (d), respectively

Table 1. Experimental results obtained with f=0.5, Capacity equal to 0.125 and $n_1 = 2$

Samples	a	b	c	d
PSNR of watermarked images	60.1307	41.6410	42.2410	59.3536
Original images entropy	3.1730	4.8459	4.4224	1.4572
Encrypted watermarked images entropy	7.9417	7.7238	7.0066	7.7140
NPCR	99.8964	99.9676	99.8478	99.8796
UACI	33.4545	33.7878	33.7686	33.1889
PSNR of semi Restituted imaging	83.3452	61.9835	63.6543	80.6547

The fragile watermarking method, which assure integrity in encrypted domain. is validate by applied on the ciphered imaging more attacks such as the clopping, add noise. Table 2 shows that the proposed watermarking is fragile center all attacks type.

Table 2. Integrity test of encrypted watermarked imaging with usual attacks

Attack	Extracted entropy	Decrypted watermarked imaging entropy	$abs\ of\ int(100 \times H_{I_{dec}}) - int\left(100 \times H_{I_{original}}\right)$	Integrity check
Without	1.4572	1.4578	0	Pass
Compression (90%)	-	4.4520	-	Not
Filtering	-	3.4516	-	Not
Contrast adjustment	-	3.1172	-	Not
Clopping (1/8)	1.4572	2.1172	118	Not
Rotation **(**90°**)**	-	4.4578	-	Not
Clopping (1/(512*512))	1.4572	2.1114	66	Not

5. COMPARISON WITH OTHERS PAPERS

In this section, we compare the proposed with Baiying Lei et al [16] where the authors have proposed a reversible watermarking scheme for medical images using the differential evolution. Rayachoti Eswaraiah et al [17] where the authors have proposed a robust medical image watermarking technique. G. Coatrieux et al [18] where the authors have proposed a watermarking method based on image moment signature. Ali Al-Haj et al [19] where the authors have proposed an encryption algorithm for secured medical image transmission. Ekta Walia et al [20] where the authors have proposed a fragile and blind watermarking technique. Bouslimi et al [6] where the authors have proposed a joint encryption/watermarking system. Table 3 shows the comparaison of the proposed method and others method in term of availability, reliability, and confidentiality. therefore, the proposed is more secured than [6] and [16]-[20].

Table 3. Comparison with others proposed methods

METHODS	Availability in embedded system (m-Health)	REAL TIME	RELIABILITY	CONFIDENTIALITY
Baiying Lei et al [16]			✓	
Rayachoti Eswaraiah et al [17]			✓	
G. Coatrieux et al [18]			✓	
Ali Al-Haj et al [19]				✓
Ekta Walia et al [20]			✓	
Bouslimi et al [6]			✓	✓
Proposed	✓	✓	✓	✓

6. CONCLUSION

In this paper, a novel watermarking/encryption system for full security of medical images dedicated to embedded system, which can be used in m-Health, have been proposed for goal safe transferring of imaging medical, the experimental results testify the good security provided by our algorithm, therefore, it has a good perspective for medical images application and can be used in m-Health.

REFERENCES

[1] Constantinescu L. and J. Kim, "SparkMed:A Framework for Dynamic Integration of Multimedia Medical Data into Distributed m-Health Systems," *IEEE Transactions on Information Technology in Biomedicine*, pp. 40-52, 2011.

[2] Z. Qian and X. Zhang, "Reversible Data Hiding in Encrypted Images with Distributed Source Encoding," in *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 1-13, 2015.

[3] S. Z. Chaudhari, *et al.*, "Secure Dissemination and Protection of Multispectral Images Using Crypto-Watermarking," in *IEEE journal of selected topics in applied earth observations and remote sensing*, pp. 1-7, 2015.

[4] X. Cao, *et al.*, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation," in *IEEE transactions on cybernetics*, pp. 1-12, 2015.

[5] A. V. Subramanyam, *et al.*, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images," in *IEEE transactions on multimedia*, vol/issue: 14(3), pp. 703-716, 2012.

[6] D. Bouslimi, *et al.*, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images," in *IEEE transactions on information technology in biomedicine*, vol/issue: 16(5), pp. 891-899, 2012.

[7] H. Suryavanshi, *et al.*, "Digital Image Watermarking in Wavelet Domain," in *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 3(1), 2014.

[8] N. Sethi and S. Vijay, "A New Cryptographic Strategy for Digital Images," in *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 4(3), 2014.

[9] B. H. Prasetio, *et al.*, "Image Encryption using Simple Algorithm on FPGA," in *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol/issue: 13(4), 2015.

[10] G. R. N. Kumari and S. Maruthuperumal, "Normalized Image Watermarking Scheme Using Chaotic System," in *International Journal of Information and Network Security (IJINS)*, vol/issue: 1(4), 2012.

[11] C. Fei, *et al.*, "Analysis and Design of Secure Watermark-Based Authentication Systems," in *IEEE transactions on information forensics and security*, pp. 43-55, 2006.

[12] X. Li, *et al.*, "Image Integrity Authentication Scheme Based on Fixed Point Theory," in *IEEE transactions on image processing*, pp. 632-645, 2015.

[13] O. Dabeer, *et al.*, "Detection of Hiding in the Least Significant Bit," in *IEEE transactions on signal processing*, pp. 3046-3058, 2004.

[14] Y. S. Chen and R. Z. Wang, "Steganalysis of Reversible Contrast Mapping Watermarking," in *IEEE signal processing letters*, pp. 125-128, 2009.

[15] W. Luo, *et al.*, "JPEG Error Analysis and Its Applications to Digital Image Forensics," in *IEEE transactions on information forensics and security*, pp. 480-491, 2010.

[16] B. Lei, *et al.*, "Reversible watermarking scheme for medical image based on differential evolution," in *ELSEVIER Expert Systems with Applications*, pp. 3178–3188, 2014.

[17] R. Eswaraiah and E. S. Reddy, "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest," in *IET Image Processing*, pp. 615–625, 2015.

[18] G. Coatrieux, *et al.*, "A Watermarking Based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characterization," in *IEEE transactions on information technology in biomedicine*, pp. 1-11, 2013.

[19] A. Al-Haj, *et al.*, "Crypto-based algorithms for secured medical image transmission," in *IET Information Security*, pp. 365–373, 2015.

[20] E. Walia and A. Suneja, "Fragile and blind watermarking technique based on Weber's law for medical image authentication," in *IET Computer Vision*, pp. 9–19, 2013.