

Biometric-based medical watermarking system for verifying privacy and source authentication

Nada Fadhil Mohammed*, Majid Jabbar Jawad, Suhad A. Ali

Department of Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq

majid_al_sirafi@yahoo.com, suhad_ali2003@yahoo.com

**Corresponding Author: Nfm.computers@gmail.com*

Abstract

Two important requirements in the e-health care system are ensuring the authenticity of the source from which data is received and preserving the privacy of patients' medical record. Medical records must only be accessed and modified by the authentic source. Any modification of medical records may lead to misdiagnosis and consequently, negatively affect the life of the patient. So, the privacy of medical record and the authenticity of the sender source must be satisfied. This research focused on a watermarking technique's ability to satisfy the above requirements. A watermarking system based on biometrics is presented in which the sender's iris code is programmed as a key for sender authentication. In addition, patient record privacy and the iris code is preserved by encrypting it using the chaotic encryption method. Experimental results showed that the proposed system satisfied the two security requirements.

Keywords: Biometric system; chaotic; medical image watermarking; privacy; source authentication.

1. Introduction

Recently, the efficiency of health care services has grown rapidly due to the implementation of telemedicine applications. These play a significant role in the growth of the healthcare sector. Hospitals and health centers have a large amount of electronic medical data that have is stored in massive databases. The transmission of this electronic medical information between different parties is became a typical way for diagnosing and scientific purposes (Zhang and Liu, 2010).

However, protecting the privacy of electronic medical information is an extremely important issue and is becoming more of a concern. Avci (2016) and Aparna and Kishore (2018a;): have devised a set of principles to meet the security requirements:

1. Medical records must only be accessed by authorized parties (confidentiality);
2. Medical records must not be modified during transmission (integrity); and,
3. Medical records and/or images of patients must be sent and received from verified sources to and receivers (authenticity).

In fact, e-health information requires astringent security mechanisms. Different techniques of digital

watermarking can be used to protect medical data. It can provide authentication, tampering detection, privacy control, etc. Because of these benefits, there is a need for medical watermarking (MW).

Digital watermarking is a technique for hiding metadata called watermark in digital data called host without affecting the quality of it for several purposes (Abdallah, Ben Hamza and Bhattacharya, 2007; Abdallah, Hamza and Bhattacharya, 2010). A watermark may be visible or invisible. It is a secret to unauthorized users and is robust against attacks. Some watermarking algorithms are based on a spatial domain, whereas others are based on a frequency domain within which the host is transformed into a frequency domain, and the watermark is embedded at these frequency coefficients. The frequency domain has been preferred in comparison to the spatial domain because it gives a high degree of robustness against attacks.

This research outlines a watermarking technique that is combined with a biometric recognition system. It provides privacy protection and ensures source verification of medical images. A biometric authentication code (a sender physician's iris code) and encrypted patient data are utilized as watermarks.

2. Literature review

Several watermarking algorithms have been proposed to deal with authentication and confidentiality requirements of medical images. Sharma, Singh and Ghrera (2015) proposed a watermarking system that used two-frequency domains: Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). To embed the watermark, the cover medical image was segmented into a Region of Interest (ROI) and a Region of Non Interest (RONI). The method used two watermarks-a hospital logo image and electronic patient records (EPR-embedded in the NROI. To increase security, the RSA and MD5 were applied on both watermarks before embedding it into the NROI. This method was appropriate because it a thief to change a patient's identity and secure the publication of medical documents on an open channel medical application.

Balamurugan and Senthil (2016) put forth a reversible watermarking system. The system used a fingerprint biometric as a watermark for authentication, a symmetric public key for cryptosystem to provide high confidentiality, and a reversible watermarking for verifying integrity.

Singh, Dave and Mohan (2015) presented a secure multiple watermarks scheme. In the embedding activity, the scheme was based on two decomposition mechanisms: DWT and Singular Value Decomposition (SVD). The watermarks consisted of a hospital logo image and electronic patient record (EPR). They were inserted into the 1st and 2nd level of the DWT, respectively. EPR was encrypted before embedding to

increase the robustness and security of the scheme.

Thakur *et al.* (2018) proposed a system in which a patient's report status was hidden into the medical image as a watermark. It was used to verify annotation, authentication, and identification. A chaos-based encryption algorithm was carried out on the watermark to enhance confidentiality. A subjective measurement was used to measure any tampering that could occur on the watermarked image through transmissions on the channel. This is a crucial measurement in healthcare data protection. Robustness and security requirements were satisfied in the proposed system.

Aparna and Kishore (2018b) derived an efficient watermarking system in an e-healthcare application based on a biometric. Their system was used to satisfy authenticity, confidentiality, and reliability security requirement. The system utilized a fingerprint for fulfilling authenticity, cryptography for fulfilling confidentiality, and reversibility for fulfilling integrity.

3. Methodology of the medical watermarking system

The proposed watermarking system consisted of two procedures: embedding and extraction/verification.

3.1 Watermark embedding procedure

The watermark embedding procedure was divided into four phases: watermark generation, watermark encryption, image segmentation, and embedding. Figure 1 illustrates the block diagram of the embedding procedure.

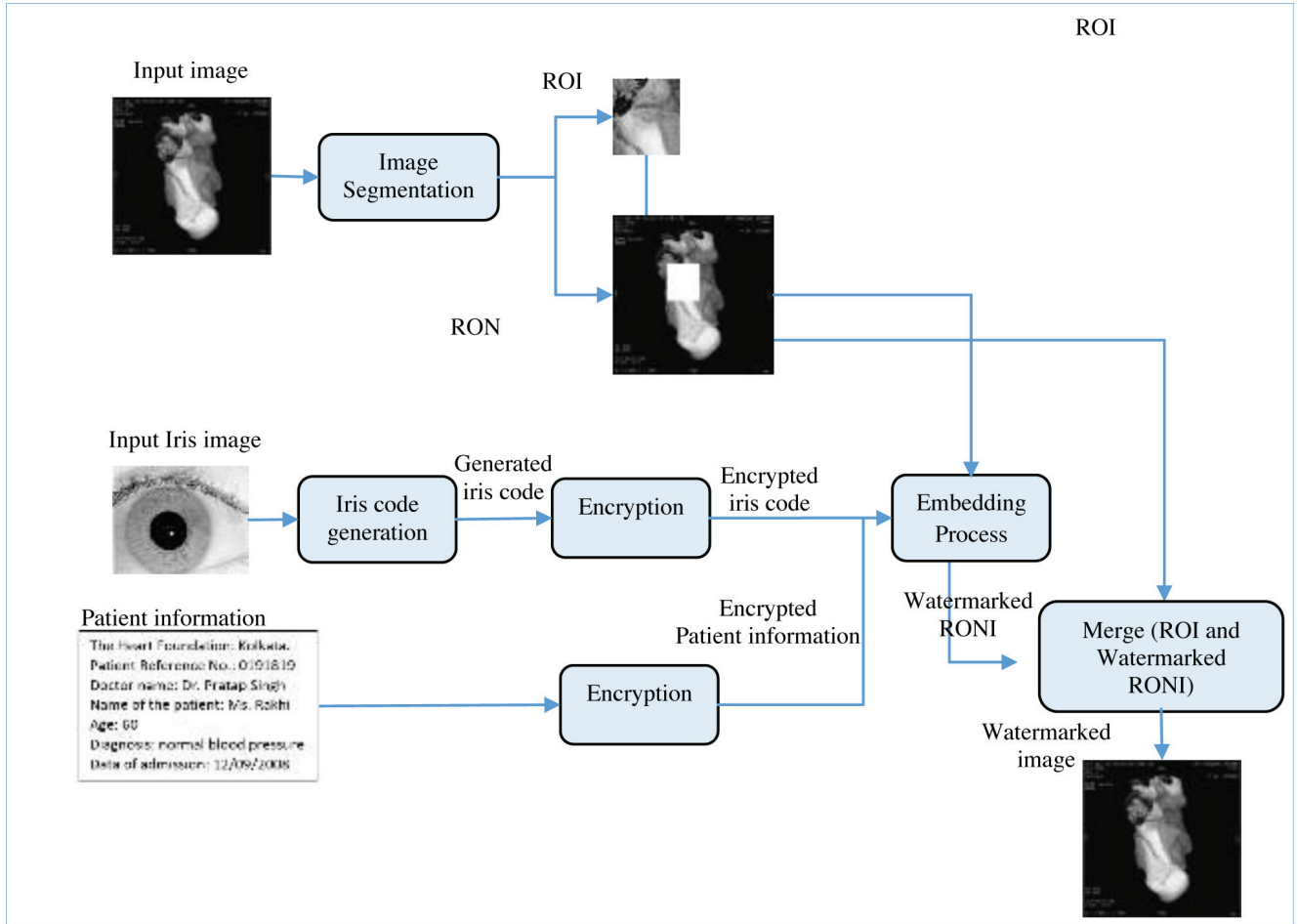


Fig. 1. Embedding procedure

Watermark Generation: Two watermarks were used in the embedding procedure to satisfy different security requirements for medical watermarking. The first was the iris code, which comes from the sending physician. It was used to verify the source authenticity (authentic sender). The second was the patient information watermark used for protecting the privacy of the patient and increasing the system security.

Watermark 1 (the iris code for the sending physician) was generated in three stages: iris segmentation, iris normalization, and feature encoding. First, the iris segmentation stage was used in order to localize and extract the iris region from the eye image. The automatic segmentation procedure is used for detecting the boundary of the iris part. There is an inner and outer border. Both surround the iris region. At this stage, an automatic segmentation algorithm was employed to localize the iris region of the eye image by detecting the iris region boundaries. The detection of the inner boundary (pupil region) was done by applying the following steps:

Step 1: In order to improve the iris segmentation, smooth the image by applying a mean filter with a window size of 9×9 pixels. This allowed for an attenuation effect of the eyelash.

Step 2: Compute a histogram of a smoothed image, then select the threshold value (th) based on the computed histogram.

Step 3: Convert the smoothed image to a binary image using the equation 1:

$$Bimg(x,y) = \begin{cases} 1 & \text{if } O(x,y) \geq th \\ 0 & \text{otherwise} \end{cases}, \quad (1)$$

where, $O(x,y)$ and $Bimg(x,y)$ are the of intensity value at the location (x,y) of the original image and the resultant binary image respectively, th is the threshold value from Step 1.

Step 4: Apply the connected component process on $Bimg$. The pupil is the largest and darkest region and

other small regions represent reflection points which may appear in the pupil region.

Step 5: Extract the largest region, which represents the pupil region.

Step 6: Compute the center's coordinates according to the following equations:

$$x_p = \frac{1}{N} \sum_{i=1}^N x_i \quad (2)$$

$$y_p = \frac{1}{N} \sum_{i=1}^N y_i \quad (3)$$

Step 7: Compute the radius of pupil R_p by finding the two pixels (x_1, x_2) from the left and right and two pixels (y_1, y_2) from the top and bottom. These pixels represented the first background pixels while moving from the center towards the left, right, top, and bottom directions. After that, two radii (R_1, R_2) from x_1 to x_2 were found, and from y_1 to y_2 according to the following equations:

$$R_1 = 0.5 \times (x_1 - x_2), \quad (4)$$

$$R_2 = 0.5 \times (y_1 - y_2), \quad (5)$$

The radius of pupil R_p could be found by taking the maximum value between R_1 and R_2 using equation 6:

$$R_p = \max(R_1, R_2), \quad (6)$$

The determined parameters of the pupil; (i.e., the radius of the pupil R_p and the center's coordinates of the pupil (x_p, y_p)) were used for the localization of the outer boundary of the iris image. This was carried out by using the circular Hough transform. Next, the segmented iris was plotted as flat and rectangular rather than circular using Dogman's Rubber Sheet Model. This eliminated the problem of differences in the iris size from one person to other. The difference can even occur for the same individual because of the size of pupil, lighting, distance from the camera, etc.

Finally, the feature encoding stage was based on Lifting Wavelet Transform (LWT). LWT was used to extract the characteristics of the iris image texture. The distinguishing features of the iris were the basis of comparison (matching) of any two images. The resultant template was an iris code measuring 514 bits in length, which is presented as the first watermark.

To extract the feature (iris code) from iris, the following sub-steps were carried out:

Step 1: Apply the LWT on the normalized iris image

and decompose the image into four sub-bands. The first one (LL) represented the approximation band, which processed into the next step (level). The other sub-bands (LH, HL, and HH) represented the detail components.

In the proposed method, the LWT was applied to three levels on the normalized iris image measuring 64×512 coefficients. The result was four sub-bands measuring 8×64 coefficients in the third level.

Step 2: Take the average values of details sub-bands in the first level (HH1 and HH2). These values of average, in addition to the values of LL3 sub band, would later represent the feature vector of the input iris image of length 514 bits. The values of the vector were real in the range $[-1, 1]$. These real values were quantized into binary form by using the average value of both LH3 and HL3 sub-bands as the threshold value.

The second watermark (related to patient information) included some valuable information such as patient name, name of the physician, age of patient, and diagnosis result.

Watermark encryption: The generated watermarks were encrypted to increase system security and protect patient privacy. The encryption consisted of two steps:

Step 1: Apply the scrambling on the template bits to change bit locations according to the equation 7:

$$New_loc = (key * old_loc) \bmod length(template) + 1, \quad (7)$$

where key is a primary secret key between 1 and the length of the template, and $old_loc = 1 \dots length(template)$.

Step 2: Alter the values of the bits according to the following sub steps:

Step 2.1: Generate a random sequence (Seq) using quadratic map using equation 8:

$$Seq_{n+1} = (r - Seq_n)^2, \quad (8)$$

where r is a chaotic parameter and n : number of iterations.

The length of the sequence will be the same as the data length to be encrypted. Then convert the range of the generated sequence (Seq) to the range $[-1, 1]$ using equation 9:

$$New_{seq} = [(((Seq - old_{min}) * New_{rang}) / (old_{rang} - new_{min}))], \quad (9)$$

Step 2.2: Generate a *bipolar_template* depending on the random values of the sequence generated in Step 2.1. The *bipolar_template* is defined as:

$$\text{bipolar_template}(I) = \begin{cases} \text{New}_{Seq}(I) & \text{if } (\text{template}(I) = 1) \\ \text{New}_{Seq}(I) * -1 & \text{if } (\text{template}(I) = 0) \end{cases}, \quad (10)$$

For $I=1$ to length (*template*).

Step 2.3: Convert the generated *bipolar_template* to binary *Encrypted_template* by adding a constant value of 0.5 to each value and round the result as follows:

$$\text{Encrypted_template} = \text{round}(\text{bipolar_template} + 0.5), \quad (11)$$

These steps were applied to encrypt the patient information image and the iris code of the sending physician. Finally, the encrypted iris code and encrypted patient information were combined and embedded in the RONI of the image.

ROI/RONI segmentation: The input medical image was separated into two regions: the Region of Interest (ROI), which is very significant for medical diagnoses, and the Region of Non-Interest (RONI), which is less important for diagnosis. The watermark was hidden in the RONI.

Embedding process: In this process, the watermark was inserted into the RONI. The RONI was split into non-overlapping blocks of with a size of $2*2$. Then each bit was embedded in a block of the RONI whose number was selected randomly using equation 12. This method of selection was based on the assumption that the number of bits in the watermark is less than the number of the blocks in the RONI.

$$B_{RONI} = (\text{key} * \text{idx}) \bmod NB + 1, \quad (12)$$

where B_{RONI} is the block number of RONI, *key* is a secret prime number between 1 and *NB*, *idx* is the current index of watermark bit to be embedded, and *NB* is the number of blocks in the RONI.

The following steps describe the embedding process:

Step 1: Segment the input image into two regions: ROI and RONI.

Step 2: Split the RONI into non-overlapping blocks of $2*2$ pixels.

Step 3: For each bit in the watermark, repeat Steps 3.1 to 3.4.

Step 3.1: Embed each bit of the watermark in a block of RONI whose number was randomly selected using the equation 12. Selection was based on the assumption that the length of the watermark is less than the number of blocks in the RONI.

Step 3.2: Apply DWT on the selected block.

Step 3.3: Quantize LL by using equation 13:

$$q = \text{floor}\left(\frac{LL}{Q_s}\right), \quad (13)$$

where, Q_s is a scaling factor.

Step 3.4: Embed one watermark bit in the LL band of each mapping block as follows:

$$LL = \begin{cases} (q * Q_s) + \left(\frac{Q_s}{2}\right) & \text{if } \text{mod}(qn, 2) = W(\text{idx}) \\ ((q + 1) * Q_s) + \left(\frac{Q_s}{2}\right) & \text{otherwise} \end{cases} \quad (14)$$

Step 3.5: Applying the inverse of DWT on the watermarked block.

Step 4: Reconstruct the blocks of the RONI to get the watermarked RONI.

Step 5: Merge the ROI with the watermarked RONI to get the watermarked medical image.

At this point, the watermarked medical image could be sent through the network to different medical practitioners at remote locations.

3.2 Watermark extraction and verification procedure

This procedure is divided into the following phases: the ROI/RONI segmentation, extraction operation, and decryption processing. Figure 2 illustrates the block diagram for this procedure.

ROI / RONI segmentation: The watermarked image is segmented into ROI and RONI.

Extraction operation: To extract the watermarks from the RONI, the following steps were applied:

Step 1: Split the RONI into non-overlapping blocks measuring $2*2$ pixels.

Step 2: Repeat Steps 2.1 to 2.4 until all watermark bits are extracted.

Step 2.1: Extracted each bit in the watermark from a block of RONI whose number was randomly selected using equation 12.

Step 2.2: Apply a discrete wavelet transform (DWT) on the selected block.
 Step 2.3: Quantize LL (using equation 13).
 Step 2.4: Extract one watermark bit from the sub-bands

(LL) of each selected block using equation 15:

$$Extracted_watermark(i) = mod(q, 2) \tag{15}$$
 For $i=1$ to length (*watermark*)

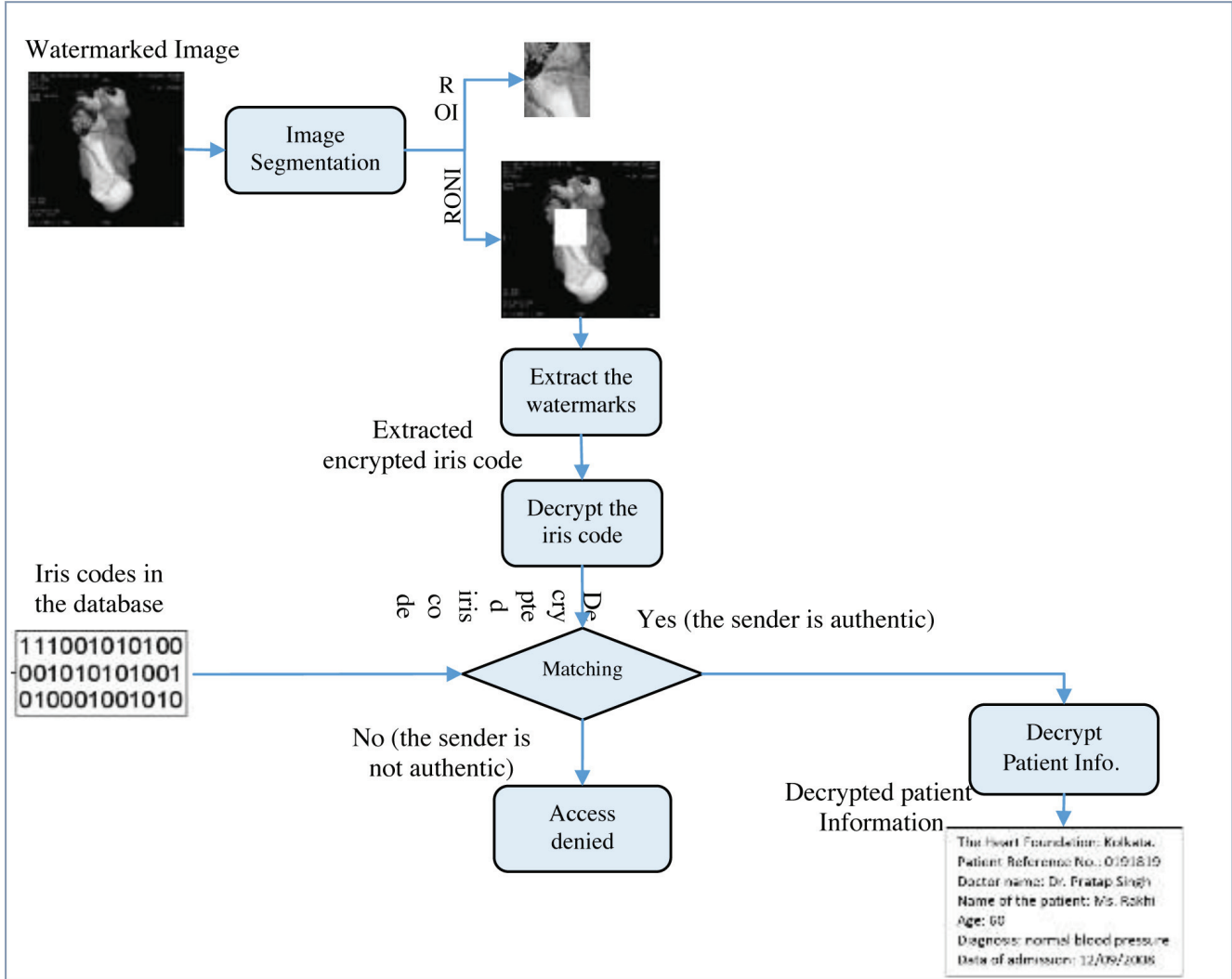


Fig. 2. Extracting and verification procedure

Decryption processing: To perform a verification process, the extracted iris code was decrypted. Then, the decrypted iris code was compared with the iris codes saved in the database in order to find whether there was a match or not. A match meant that the access was permitted (authenticated), and the decryption process was applied to the extracted patient information, otherwise the access was denied.

The following steps were performed for the decryption process:

Step 1: Generate a random chaotic sequence using a quadratic map according to equation 7 with the same

initial parameters that were used on the sender’s side. Then convert the range of the generated sequence to the range [-1...1] using equation 8.

Step 2: Shift extracted Encrypted_template by 0.5 as in equation 16:

$$S_Encrypted_template = round(Encrypted_template - 0.5) \tag{16}$$

Step 3: Multiply the $S_Encrypted_template$ by the generated sequence (New_{seq}) in Step 1 using equation 17:

$$\begin{aligned} \text{bipolar_template} = \\ \text{New}_{Seq} * S_Encrypted_template' \end{aligned} \quad (17)$$

Step 4: Obtain the decrypted template (*Decrypted_template*) by thresholding the *bipolar_template* as in equation 18:

$$\text{Decrypted_template}(I) = \begin{cases} 1 & \text{if } (\text{bipolar_template}(I) > 0) \\ 0 & \text{otherwise} \end{cases} \quad (18)$$

For each $I=1$ to length of the *bipolar_template*.

Step 5: Apply the inverse of the scrambling and return bits into their original positions using equation 7.

After the verification procedure was performed, the patient information could be decrypted.

4. Results and discussion

The performance of the proposed watermarking system was tested in terms of security, imperceptibility and robustness. The system was simulated using MATLAB version R2016a implemented on a computer having the characteristics: Intel(R) Core i7 of 2.60GHz and RAM 8GB. A series of tests were conducted to show the effects of various parameters included in the overall system performance.

1.1 Security analysis of chaotic encryption

To increase the security and robustness of the embedding algorithm, the watermarks were encrypted using the chaotic method. According to the tests, the best values for the control parameters were $Seq0=0.15$, iteration number $n=40$ and chaotic parameter $r=0.1$ since it produced low correlation values between the original and encrypted images.

A good encryption algorithm should possess the following properties:

1. Sensitivity to the secret keys (initial values of chaotic): The Avalanche Effect (AE) metric can be used to test the efficiency of the diffusion mechanism. If the image P is encrypted using the chaotic algorithm to give C and then a single bit change can be made in key (such as the initial condition) of the chaotic algorithm. Thereafter, the same image can be encrypted to get C' . The AE metric is the percentage of different bits between C and C' as in the following equation:

$$AE = \frac{\sum_{i=1}^M \sum_{j=1}^N [(C(i,j) \oplus C'(i,j))]^2}{M*N}, \quad (19)$$

If C and C' differ from each other in half of their bits, we can say that the encryption algorithm possesses good diffusion characteristics. The AE value of the image in Figure 4 was 50.0433.

2. Information entropy: The information entropy shows the distribution of gray values in an image. It is denoted by H and is calculated follows:

$$H(S) = - \sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i), \quad (20)$$

where $p(s_i)$ is the probability of the gray scale s_i and N is the number of gray scale of the image. The ideal entropy value for an encrypted patient image should be 1 (or very close to 1) since it is a binary image. The entropy value for the patient image in Figure 4 was 0.9990.

3. Correlation computation: This was used to test the statistical properties of the original and encrypted images. The encrypted image must have a low value of correlation with the original image. The correlation coefficient (r) between A and B is computed as in follows equation:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}, \quad (21)$$

where \bar{A} is the mean of A , and \bar{B} is the mean of B .

The correlation coefficient value is measured between the original and encrypted images in Figure 4, and its value is very small (-0.0051). This means that the original image and the corresponding encrypted one are entirely uncorrelated to one another.

4.2 Fidelity measuring

Peak Signal to Noise Ratio (PSNR) is applied to evaluate the fidelity of the embedding scheme. PSNR is given by equation 22 (Thakkar and Srivastava, 2016)

$$PSNR = 10 \log_{10} \frac{(2^L)^2}{MSE}, \quad (22)$$

where L is the maximum bits required to represent the pixels of the image, and MSE is the mean square which is computed using equation 23:

$$MSE = \frac{1}{N \times M} \sum_{i=1}^N \sum_{j=1}^M (I_{ij} - W_{ij})^2, \quad (23)$$

where I refers to the cover image of size $N \times M$ and W represents the watermarked image. Figure 3 shows samples of the original and watermarked images with their PSNR values.

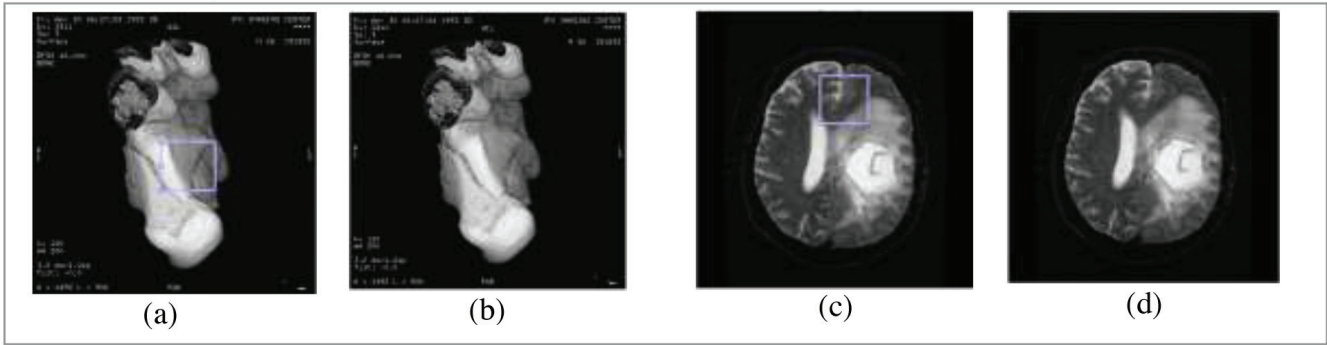

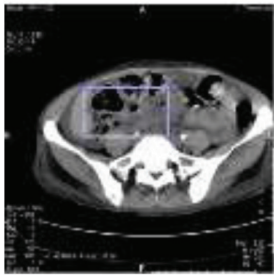


Fig. 3. Samples of original and watermarked images: (a) original CT image, (b) watermarked image (c) original MRI image, and (d) the watermarked image

PSNR values are changed according to different factors such as watermark size and scaling factor, which are used in the proposed embedding algorithm.

Table 1 shows the values of PSNR with different size watermarks using ($Q_s=4$).


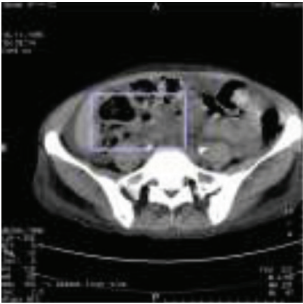
Table 1. Relation between PSNR and watermark size

Input image	Watermark size (in bits)	PSNR
CT scan, 16 bits 	20514	88.3499
	24514	87.5901
	26914	87.1971
	30514	86.6358
	340314	86.1032
	41014	85.3442
CT scan, 8 bits 	20514	41.0436
	24514	40.1939
	26914	39.8342
	30514	39.2967
	340314	38.7444
	41014	37.9732

To measure the effect of the scaling factor on the embedding process, different tests were performed. Table 2 shows the embedding with different values of

scaling factor (4, 6, 8, and 16) using a watermark size of 30,514 bits:

Table 2. Relation between PSNR and Qs

Input image	Scaling Factor			
	4	6	8	16
	PSNR value			
CT scan, 16 bits				
	86.6358	85.5630	80.6415	74.8782
CT scan, 8 bits				
	39.2967	35.7686	33.3125	27.2940

A problem may arise in the proposed method when the size of the ROI is large and the RONI is not enough for the embedding watermarks. This problem can be solved using another watermarking technique such as the reversible watermarking.

1.1 Robustness measures

The robustness of the system is measured with several kinds of attacks (Table 6). The system is tested with a set of 8- and 16-bit DICOM gray-scale medical images.

Since the watermark consist of two parts (iris code and the image of patient information) each of them will be evaluated separately. The Hamming Distance (HD) is used to measure the similarity between the extracted iris code and iris codes saved in the database. The system checks whether the sender is authentic or

not. For an iris code of length k , HD is defined as in equation 24:

$$HD = \frac{1}{k} * (\sum_{i=1}^k Iris(i) \oplus Iris^*(i)) * 100, \quad (24)$$

where $Iris(i)$ is an original iris code at position, (i) and $Iris^*(i)$ is an extracted iris codes at position (i) , and \oplus is an exclusive-OR operator.

The iris images taken for the same individual do not matched 100% since these pictures were captured under different statuses. Thus, there is a need to determine the threshold t of acceptable difference between two iris codes in order to achieve the best values of performance parameters. With the proposed system the value of the threshold is set to 0.31. Table 3 shows values of HD under several types of attacks:

Table 3. HD values under several types of attacks

Type of attack	Density	HD	Verified
Salt & pepper	0.02	0	√
	0.03	0.0019	√
	0.05	0.0038	√
	0.1	0.0369	√
	0.2	0.0778	√
Cropping 50*50		0.0428	√
Cropping 110*110		0	√
Brightness (+110)		0	√
Compression		0	√

If the iris is verified, it means the source is authentic. Then the patient information is decrypted, and its similarity between the inserted and extracted patient information is evaluated by using calculating the Normalized Correlation (NC). NC can be defined as in equation 25 (Jamali *et al.*, 2016):

$$NC = \frac{\sum_{i=1}^x \sum_{j=1}^y w(i,j)w'(i,j)}{\sqrt{\sum_{i=1}^x \sum_{j=1}^y w(i,j)^2}} \quad (25)$$

where w and w' refer to the original and recovered watermarks, respectively. Figure 4 shows the original and extracted watermarks embedded in a 16-bit image without any attack (NC=1).

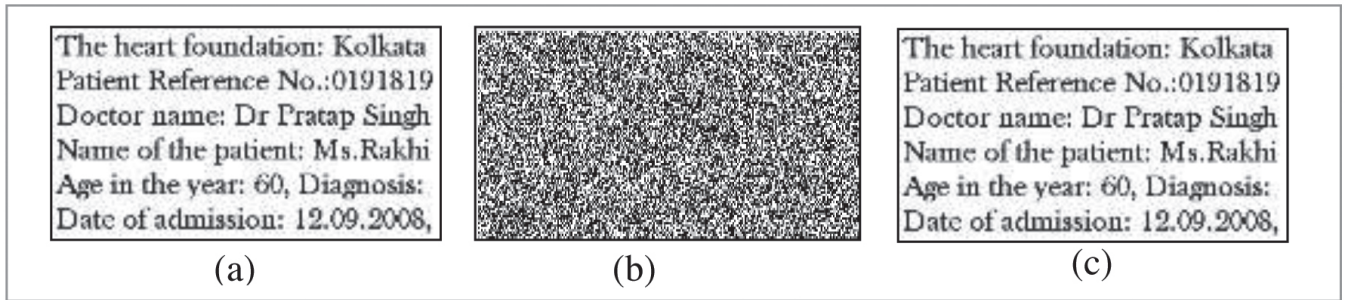


Fig. 4. Watermark extraction (a) original watermark, (b) encrypted watermark, (c) extracted watermark

Several attacks were implemented to check the performance of the proposed scheme. In addition, the time consumed for the embedding and encryption processes was 6.168158 seconds, while the time consumed for the extraction and decryption processes was 5.619777 seconds.

5. Conclusions

This paper presented a medical watermarking system for satisfying the two important requirements in e-healthcare system data management (source authentication and medical record privacy). The proposed method exploited the DWT for embedding and extracting the watermark. In addition, the proposed system used the

quadratic map to encrypt patient information in order to preserve the privacy of the patient.

Future research into this subject should include the possible implementation of the proposed system with other types of watermarking techniques such as reversible watermarking. An investigation into the ability of applying the proposed system for medical video applications would be of value as well.

ACKNOWLEDGEMENTS

This work was supported by Department of Computer Science, College of Science for Women, Babylon University, Babylon, Iraq.

References

- Abdallah, E.E., Ben Hamza, A. & Bhattacharya, P. (2007).** MPEG video watermarking using tensor singular value decomposition. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 772-783.
- Abdallah, E.E., Hamza, A. Ben & Bhattacharya, P. (2010).** Video watermarking using wavelet transform and tensor algebra. *Signal, Image and Video Processing*, **4**(2): 233-245.
- Aparna, P. & Kishore, P.V.V. (2018a).** An efficient medical image watermarking technique in e-healthcare application using hybridization of compression and cryptography algorithm. *Journal of Intelligent Systems*, **27**(1): 115–133.
- Aparna, P. & Kishore, P.V.V. (2018b).** Biometric-based efficient medical image watermarking in E-healthcare application. *IET Image Processing*, **13**(3): 421–428.
- Avci, D. (2016).** A novel meaningful secret image sharing method based on Arabic letters. *Kuwait Journal of Science*, **43**(4): 114-124.
- Balamurugan, G. & Senthil, M. (2016).** A fingerprint based reversible watermarking system for the security of medical information, *IEEE Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave 2016)*. Coimbatore, India, 29 Feb-1 Mar.
- Jamali, M. et al. (2016).** Robust watermarking in non-ROI of medical images based on DCT-DWT, 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS), Orlando, FL, 2016: 1200-1203.
- Sharma, A., Singh, A.K. & Ghrera, S.P. (2015).** Secure Hybrid Robust Watermarking Technique for Medical Images. *Procedia Computer Science*, **70**: 778–784.
- Singh, A.K., Dave, M. & Mohan, A. (2015).** Robust and secure multiple watermarking in wavelet domain. *Journal of Medical Imaging and Health Informatics*, **5**(2): 406-414.
- Thakkar, F.N. & Srivastava, V.K. (2016).** A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, **76**(3): 3669-3697.
- Thakur, S. et al. (2018).** Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia Tools and Applications*. Springer Verlag: 1-14.
- Zhang, R. & Liu, L. (2010).** Security models and requirements for healthcare application clouds. *CLOUD '10: Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing*, USA: 268-275.

Submitted: 05/09/2018**Revised:** 21/11/2019**Accepted:** 13/02/2020

نظام العلامة المائية الطبية المعتمدة على البصمات للتحقق من موثوقية المصدر والخصوصية

ندى فاضل محمد*، ماجد جبار جواد، سهاد احمد علي
قسم علوم الحاسوب - كلية العلوم للبنات - جامعة بابل - العراق
Nfm.computers@gmail.com*

ملخص

يناقش هذا البحث اثنين من أهم متطلبات نظام الرعاية الصحية الالكترونية لضمان موثوقية مصدر البيانات المرسله وكذلك ضمان خصوصية السجل الطبي للمريض. يجب التعامل مع السجل الطبي وتعديله من قبل مصدر موثوق به. حيث قد يؤدي أي تعديل في السجل الطبي إلى خطأ في التشخيص مما يؤثر على حياة المريض. ومن ثم يجب الالتزام بالحفاظ على خصوصية السجل الطبي وموثوقية المصدر المرسل. يدرس هذا البحث قدرة تقنية العلامة المائية على استيفاء الشرطين السابقين، وتوضح هذه الورقة البحثية أن نظام العلامة المائية يعتمد على نظام البصمة المتمثل في توكيد قزحية العين الخاصة بمُرسل البيانات لاستخدامها كوسيلة للمصادقة على تفويض المصدر المرسل للبيانات، وعلاوة على ذلك يتم حفظ خصوصية سجل المريض وكود قزحية العين عن طريقة التشفير واستخدام أسلوب التشفير العشوائي، كما أظهرت النتائج التجريبية ان النظام المقترح قد استوفى شرطي الأمان اللازمين.

