

# Verification approach for medical data in e-healthcare system based on biometric and watermarking

Noor Fahem Sahib<sup>1</sup>, Moatasem Mohammed Saeed Najji<sup>2</sup>, Ebtehal Akeel Hamed<sup>3</sup>

<sup>1,2,3</sup> Al Qasim Green University, Babylon, Iraq

## ABSTRACT

Medical information is crucial in the healthcare system, and its manipulation can lead to misdiagnosis. Medical images also contain personal information for patients; hence, information security and privacy protection are paramount when transferring medical images over the Internet. Biometric approach and watermarking techniques are used to achieve this purpose. The focus of this paper was on a biometric watermarking system with a frequency domain in which the sender's iris code is employed as a sender authentication key. The privacy of the patient's information is preserved by encrypting it and embedding the key in the cover medical image created by the Discrete Wavelet Transform. The algorithm has shown that the proposed system has met previous requirements.

**Keywords:** E- healthcare system, biometric, Medical data, Legendre moment, Discrete wavelet transform (DWT).

### *Corresponding Author:*

Noor Fahem Sahib  
Al Qasim Green University  
Babylon, Iraq  
E-mail: noor@fosci.uoqasim.edu.iq

## 1. Introduction

Information and communication technologies (icts) have wrought dramatic changes in our lives. Also, these strategies were used in the healthcare industry. At all levels, information plays a critical role in medicine. E-health refers to computer technologies in medical practice [1]. Because medical data is crucial in the healthcare system, its alteration might lead to misdiagnosis. Because medical images contain sensitive information about a person based on their iris is one of these ways. For meeting the above security requirements, digital watermarking proved patients, information security, and privacy are critical considerations when sending medical images over the Internet [2]. As a result, to meet the security requirements of medical images during transmission, a high level of protection and authentication is required. Confidentiality, integrity, and authenticity are among the security requirements [3]. In the healthcare setting, confidentiality refers to unauthorized individuals' access to medical data.

In contrast, integrity means that data is not altered during transmission or storage. Finally, the image needs to come from the appropriate source [4]. As a result, various strategies to tackle the abovementioned issues were required. Electronic identification and verification are the optimum approaches [3].

## 2. Material and methods

This section introduces some of the state-of-the-art methods related to the healthcare system and medical image authentication and confidentiality. In [2] the authors proposed a cryptographic approach to satisfy confidentiality, authentication, and integrity to medical images. By embedding a watermark in the region of non-interest, a watermarking algorithm based on DWT and SVD has been used to satisfy authenticity. An integrity hash watermark is computed for ROI and embedding in the RONI of the image. For confidentiality, patient data is embedded in a medical image (RONI). In [3] the authors propose that two biometric techniques,

fingerprint and face recognition, were used to enforce the proposed solution effectively. These are two of the most widely used and mature biometric methods. A combined watermarking (DWT, DCT) scheme has been implemented to ensure a higher degree of security. The same watermarking algorithm was used two times, as previously stated. To figure out who he is, one must examine his characteristics and the minor details of his fingerprint. In addition, as a complement to its identification, the face ID is applied to the original photo. We were surprised by the psychological associations with securing biometric data, especially those linked to the watermarked image. They demonstrate that the device can withstand various signal processing proposal assaults.

In [4] the authors presented a DWT-based image watermarking system for masking patient data within a region of interest (ROI) to explain identification and data authenticity. Before the watermarks are placed, a quick response (QR) code image is created for the patient's data. As a result, to enhance data security. Furthermore, the peak signal-to-noise ratio (PSNR) was utilized to detect subtly, and NC was used to compare the original and extracted watermarks. In [5] the authors offered a two-layer approach to medical data security. The first layer uses the watermarking technique to mask patient information in the input image, resulting in a watermarked image.

In the second layer, the chaotic encryption technique is used to the watermarked image to improve confidentiality. A subjective test was used to assess the quality of the watermarked image. The proposed approach is both robust and secure. In [6] they establish a new standard for using biometric technology to produce revolutionary healthcare via the internet of things (IOT), which incorporates high data access capacity while staying simple. They also created a more secure means of connecting to the internet of things (IOT) based on biometrics and a quick identity standard, paving the path for significant breakthroughs in intelligent healthcare systems.

In [7] the authors devised a universal watermarking technology based on the DWT to secure medical data and ensure the authentication of medical images; the algorithm embeds the patient's sensitive information in the medical image as a watermark. A visual encryption approach of medical images is used to protect the watermarked image. The doctor's biometric fingerprint is also used to ensure source identification.

In [8] the authors proposed a model to enforce the security and privacy of e-healthcare systems as well as preserve and enhance the protection and confidentiality of e-healthcare systems. This approach employs agents to secure the security and privacy of e-health information transferred between users. In [9] the authors proposed two watermarks using the DWT, an approach for embedding, and the cover image was divided into the interest and non-interest regions. The iris code is utilized as a watermark from sending the physician to add the watermark. The patient information watermark the automatic segmentation approach recognized the eye iris area in the image. To strengthen security, both are included in the non-interest regions.

The non-interest regions received a double encryption watermark. Extract the watermark from the non-interest regions using the same approach (quadratic map). The proposed watermarking method would perform two critical purposes in the electronic health care system: authenticating the data source and protecting patient privacy.

### 3. Calculation theory

The proposed system as shown in Figure 1 is based on watermarking techniques and biometrics. The proposed system depends on two watermarks to protect the privacy of the patient's medical information and source authentication; the first is the sender's iris code, which is used to verify the sender's authenticity. The second watermark is encrypted patient information, which ensures patient confidentiality and data protection.

The proposed system consists of two stages stage1 pre-processing and embedding, and stage 2, an extracting process and verification. In the first stage, the features extracted from the iris of the authorized person are embedded with the patient information (second watermark) after encoding it in the XOR manner in an image after applying the DWT transformation to it.

The second stage is to send the result of the first stage to the other person, who will repeat the same procedures to produce results. These procedures will provide the features of the person's iris. Then matching these features with the features were produced from the first stage after extracting it; if the result of matching is true, that means the person is authorized and can decrypt the patient information; otherwise, they cannot access it.

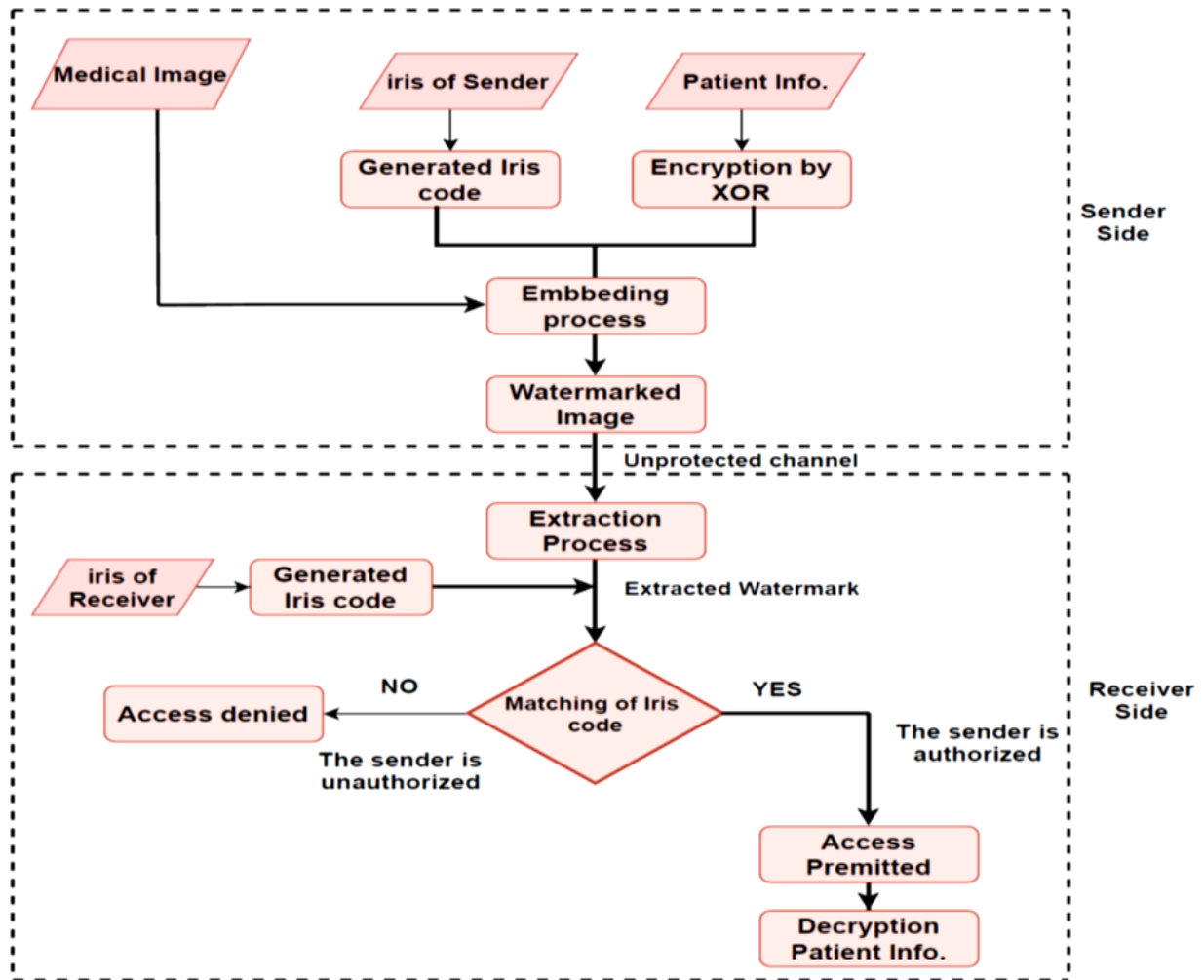


Figure 1. The proposed system

### 3.1. Embedding procedure

The embedding technique includes multiple steps on the sender side (generation of the first watermarks, encryption of the second watermarks, and embedding process). The general steps for the embedding technique are shown in Algorithm 1.

Algorithm 31: General embedding procedure
<b>Input:</b> Cov_Image // cover image. Patient_Info // patient information. Iris_image // iris of sender (physician).
<b>Output:</b> WI // Watermarked Image
Step1: Generate Iris code from Iris image by segmentation, normalization, feature extraction Step2: Encrypt patient_info by using XOR cipher. Step3: convert Cov_image to DWT transform Step4: Embed the two watermark (iris code, patient information) into a result of step3 to form the WI.
<b>End algorithm</b>

The embedding procedure consists of different steps. These steps can be listed as follows:

### 3.1.1. Generating the first watermark( iris code of the sender)

The creation of the first watermark requires building a system for iris identification; it consists of four stages: Image pre-processing, iris segmentation, iris normalization, and features extraction.

The stages of the iris identification system are explained as follows:

#### 3.1.1.1. Pre-processing

The colour image (RGB) should be converted into a grey-scale image to facilitate data processing. The colour image contains three channels, while the grayscale image contains one channel. The lightness information is kept in the most common methods while the Chroma and hue information is ignored. The mathematical equation of the conversion is[10] :

$$Gray\ image = Wr * R + Wg * G + Wb * B \quad (1)$$

Thus:

$$Wr + Wg + Wb = 1 \quad (2)$$

Where: Weight= summation of all three weights (R, G, and B), which must equal 1. After the previous processes over data, it becomes ready for the next step.

#### 3.1.1.2. Iris segmentation

The primary function of Iris segmentation is to obtain the cercal of the iris and pupil. An efficient and automatic algorithm for iris detection is proposed first. Next, define the range of pupil and iris radius. To determine the inner boundary (pupil), use canny detection, and circular Hough transforms used to find pupil centre coordinates (x, y) and pupil radius (r)[11]. The outer boundary is also determined by canny edge detection on the image and performing the circular hough transform, where finding the maximum in the hough space to obtain the iris cercal. The hough transform must be a scaling factor in the proposed system using the scaling factor (0.4) to speed up this iris localisation process. After the localization process, the separation process comes where the iris is divided by the defining dimension of the image (i, j), the centre of the pupil (x, y), the radius of the pupil (Rp), and impose radius of the iris is twice the pupil radius (Ri). The value (R) is calculated using the euclidian distance equation for each point in the eye image array. The value (R) is considered an iris point when it related to the values [Rp .. Ri] range; otherwise, it a non-iris point and labelled to one value.

Figure 1 show the steps of iris segmentation.

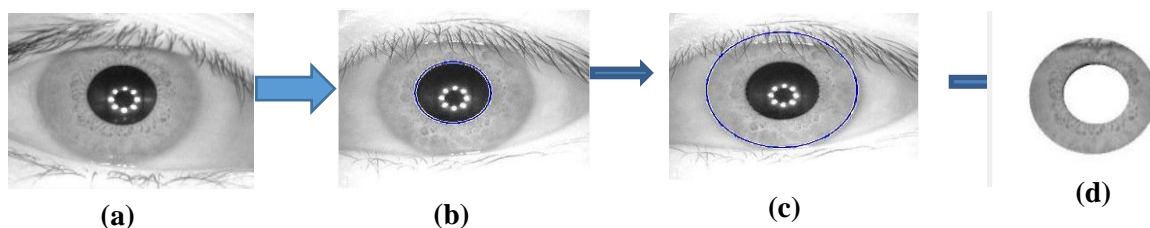


Figure 1. The iris segmentation steps.

#### 3.1.1.3. Normalization

The iris size varies from person to another, even of the same person, due to a variety of factors such as pupil size, lighting, and camera distance. These elements can have an impact on iris matching performance. As a result, in order to produce perfect results, these effects must be removed or reduced to the point that the isolated iris for all input images is the same size. To achieve this task, an iris rectangular rather than circular plotting process is performed by daugman's rubber-sheet model as shown in Figure 3. In order to complete this work, each "cartesian coordinates" (x, y) point within the iris region is converted to "polar coordinates" (r,θ) using (3) and (4) [12].

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \quad (3)$$

Such that

$$x = r \cos \theta \quad y = r \sin \theta \quad (4)$$

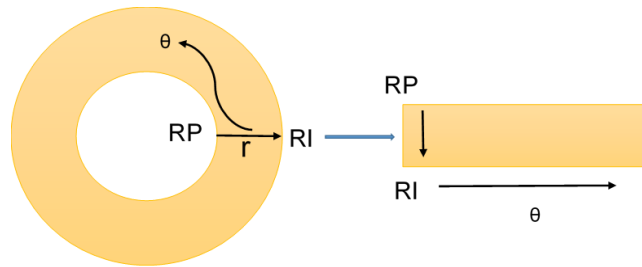


Figure 2. Daugman's rubber sheet model to conversion from polar to cartesian

### 3.1.1.4. Feature extraction

It is the third stage of the iris identification system. Extracting good features is the critical step in the iris identification system. After the iris is normalised and converted to a rectangle, the feature extraction stage begins. In the proposed method, legendre moment has been used for that.

Legendre's two-dimensional moments of order (p+q), the intensity function of the image is f(x,y) are defined as below[13] :

$$L_{pq} = \frac{(2p+1)(2q+1)}{4} \int_{-1}^1 \int_{-1}^1 P_p(x)P_q(y)f(x,y)dx dy \quad \text{where } x,y \in [-1.1] \quad (5)$$

Where, Pp(x) (Legendre polynomial), of order p, is begin

$$P_p(x) = \sum_{k=0}^p \left\{ (-1)^{\frac{p-k}{2}} \frac{1}{2^p} \frac{(p+k)!x^k}{\left(\frac{p-k}{2}\right)!\left(\frac{p+k}{2}\right)!k!} \right\}_{p-k=even} \quad (6)$$

The legendre polynomial can calculate using a recurrent relationship below:

$$P_p(x) = \frac{(2p-1)xP_{p-1}(x)-(p-1)P_{p-2}(x)}{p} \quad \text{for } p > 1 \quad (7)$$

$$P_0(x) = 1. P_1(x) = x$$

Summations replace the integrations in previous (5) to calculate legendre's moments from a digital image, and the image coordinates have to normalize to

[-1; 1]. For a discrete image of the N×N pixels with f(x;y), the approximate numerical form of legendre moments is:

$$L_{pq}=\lambda_{pq} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} P_p(xi)P_q(yj)f(i,j) \quad (8)$$

Where the constant of normalizing is:

$$\lambda_{pq} = \frac{(2p+1)(2q+1)}{N^2}$$

(xi) and (yj) indicate pixel coordinates of normalization within the range of [-1,1] that are provided by:

$$x_i = \frac{2i}{N-1} - 1 \quad \text{and} \quad y_j = \frac{2j}{M-1} - 1 \quad (9)$$

### 3.1.2. Encrypt the second watermark

The second watermark is patient information. This watermark is used to provide confidentiality and for protecting patient data. The patient information can assist in diagnoses, such as patient name, physician's name, patient's age, patient address, date of submission, and diagnosis result. In the proposed system, the patient information was encrypted b using the XOR manner.

### 3.1.3. Cover image processing

The proposed system will convert the cover image to a DWT transform. In this system, the haar filter will splitting the image into four non-overlapping sub-bands: LL, LH, HL, and HH. LL related to coarse-scale

DWT coefficients, whereas LH, HL, and HH have fine-scale DWT coefficients[14]. Because the information expected to be included in low-frequency coefficient of the original image, embedding a watermark in this position is more robust. Watermarks must be resistant to compression, and as such, it is necessary to embed them with a low frequency of DWT.

**3.1.4. Embed the watermarks**

Applying DWT on the covered image to get four parts (LL, LH, HL, HH). LL will be chosen to embed the two watermarks (iris code of the physician sender and patient information) in the proposed system part because the compression or scaling operations may cause in losing the high frequencies. After embedding the bit in LL, the final watermarked image resulted from applying the inverse of DWT on the image.

**3.2. Extracting procedure**

This procedure is divided into four phases: generated iris receiver code, extraction operation, verification process, and decryption process. Algorithm (2) illustrates the overall steps of the extraction operation.

<b>Algorithm 3.2: Extraction process</b>
<b>Input:</b> Watermarked image WI
<b>Output:</b> The encrypted patient information // <i>encrypted_info</i> The iris code as a binary vector // <i>cod_iris</i>
<b>Step1:</b> Generate iris code by applying the same procedure on the sender side
<b>Step2:</b> Apply DWT on WI to produce LL, HH, HL, and LH.
<b>Step3:</b> Extract each bit of watermark from the sun band (LL) until the length of the watermark
<b>Step 4:</b> Compare the result of the step3 with the iris code resulting from step1. If the matching is valid, go to step5
<b>Step 5:</b> Decrypt the patient information
<b>End algorithm</b>

**3.3. The matching process**

The embedding process results are sent to the receiver person who gets the iris code (key) by the extraction process. At the same time, this individual generates iris code(key) by applying segmentation, normalization, and feature extraction on iris image and then compare this key with the key resulting from the extraction process by using structural similarity index measure (SSIM); if the result is zero, this means the individual is not approved, and if one the meaning is this authorized person who decodes the encrypted text and extracts the patient's information where SSIM is a technique for determining the similarity of two images. The resulting SSIM index is a decimal value between 0 and 1. In the proposed system, we will choose the value (0.6) as a threshold to determine access to the system. The SSIM is defined as[15] :

$$SSIM(I, W) = l(I, W) c(I, W) s(I, W)$$

$$\begin{cases} l(I, W) = \frac{2\mu_I\mu_W+C_1}{\mu_I^2\mu_W^2+C_1} \\ c(I, W) = \frac{2\sigma_I\sigma_W+C_2}{\sigma_I^2\sigma_W^2+C_2} \\ s(I, W) = \frac{\sigma_{IW}+C_3}{\sigma_I\sigma_W+C_3} \end{cases} \quad (10)$$

The three terms in (10) represent luminance, contrast, and the structure comparisons functions, respectively.

## 4. Results

### 4.1. Environments

The proposed method is implemented on an image from a (CASIA-V4-interval) database. The developed system simulated using (MATLAB version R2018a) programming language. The programs work under the (Windows7) operating system and (HP (z book)) laptop.

### 4.2. System performance

The information of patient and iris code are included in the watermark. The extracted iris code is compared to the sender's iris code using the (SSIM). As a result, the system confirms the sender's identity. However, the iris photos taken for the same person do not match 100 per cent because they were taken under different situations. A threshold  $t$  of allowable difference between two iris codes must be determined to attain the optimal performance characteristics. The suggested approach provides a 0.6 threshold; if the SSIM result is more significant than the threshold, the source is authentic, and the patient information is decrypted.

#### Accuracy measuring

Peak signal to noise ratio (PSNR) is applied to evaluate the accuracy of the embedding scheme. PSNR is given by the (11) below [15]

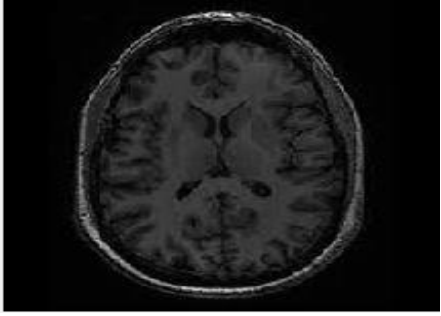
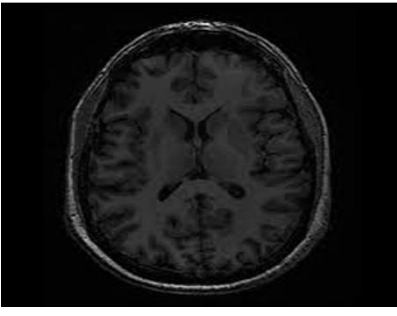


$$PSNR = 10 \log \frac{(2^L)^2}{MSE} \quad (11)$$

where  $L$  is the maximum bits required to represent the pixels of the image, and MSE is the mean square which is computed using the following (12) [15]

$$MSE = \frac{1}{N \times M} \sum_{i=1}^N \sum_{j=1}^M (I_{ij} - W_{ij})^2 \quad (12)$$

Where  $I$  refer to the cover image of size  $N \times M$  and  $W$  represents the watermarked image. Table 2 shows the original and their corresponding watermarked images versions with PSNR. Figure 4 shows the flowchart of PSNR for five images.

Table 1. Samples of the original and watermarked images

Original Image	Watermarked Image	PSNR
		65.5779
		65.5779

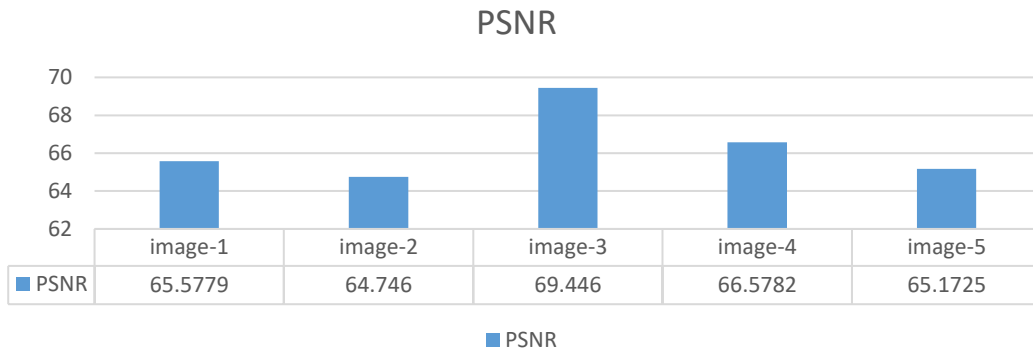


Figure 4. Flowchart of PSNR for five image

PSNR values changed according to different factors such as (watermark size). The size of the first watermark (iris code) is fixed, but patient information is changeable. Figure 5 show the relation between the size of the watermark and PSNR, where each increase in the size of the watermark leads to a decrease in PSNR.

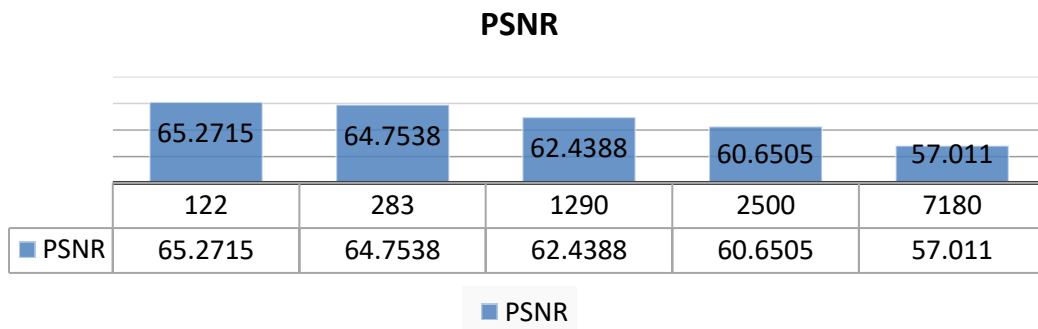


Figure 5. The relation between the size of watermark and PSNR

The size of the covered image is another factor affecting the PSNR value; Figure 6 shows the relation between the size of the cover image and PSNR, where each increase in the size of the image leads to an increase in PSNR.



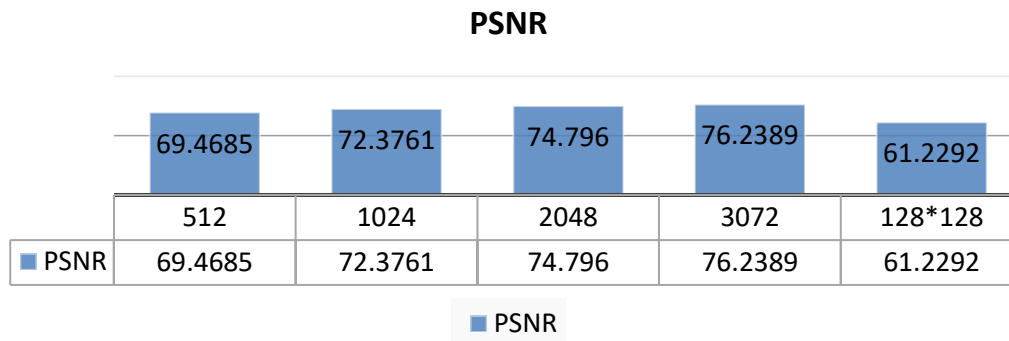


Figure 6. The relation between the size of image and PSNR

The robustness of the system is measured with several kinds of attacks. The SSIM is used to calculate the difference between extracted watermark of iris code for sender and iris code for receiver to check whether the sender is authentic or not. The threshold value equal to 0.6 will be used as a threshold of acceptable difference between iris codes. Table 2 Shows values of SSIM under various kinds of attacks:

Table 2. SSIM value after applying different attacks on the watermarked image

Type of attack	SSIM	Verify
NO attack	1	√
Salt & pepper with noise density = 0.001	1	√
Salt & pepper with noise density = 0.01	0.984	√
Speckle with variance = 0.001	0.997	√
Speckle with variance = 0.01	0.998	√
Gaussian with variance=0.0001	0.887	√
Gaussian with variance=0.0002	0.895	√
Poisson	0.999	√

## 5. Conclusions

The proposed system uses the DWT for embedding the patient information and feature (key) produced from Legendre moment. Embedding in the LL sub-band has an excellent result compared with another sub-band. In addition, the proposed method used the XOR manner to encrypt the patient's data to protect the patient's privacy. This system aims to satisfy source authentication and patient privacy. Future work into this topic should combine the proposed method with other watermarking techniques, including DFT and the system uses a media file (video) for embedding the patient's information.

## Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

## References

- [1] M. M. Khalil and R. Jones, "Electronic Health Services an Introduction to Theory and Application," *Libyan Journal of Medicine*, vol. 2, no. 4, pp. 202-210, 2007.
- [2] A. Al-Haj, A. Mohammad and A. Amer, "Crypto-Watermarking of Transmitted Medical Images," *Journal of Digital Imaging*, vol. 30, no. 1, pp. 26-38, 2017.
- [3] L. R. Haddada, B. Dorizzi and N. E. Ben Amara, "A combined watermarking approach for securing biometric data," *Signal Processing: Image Communication*, vol. 55, pp. 23-31, 2017.

- [4] N. Hnoohom, C. Sriyapai, M. Ketcham, T. Theeramunkong, R. Kongkachandra and T. Supnithi, "Robust Watermarking for Medical Image Authentication Based on DWT with QR Codes in Telemedicine," in *Advances in Natural Language Processing, Intelligent Informatics and Smart Technology*, 2018.
- [5] S. Thakur, A. K. Singh, S. P. Ghrera and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3457-3470, 2019.
- [6] H. Hamidi, "An approach to develop the smart health using Internet of Things and authentication based on biometric technology," *Future Generation Computer Systems*, vol. 91, pp. 434-449, 2019.
- [7] S. Priya and B. Santhi, "A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images," *Mobile Networks and Applications*, vol. 26, no. 6, pp. 2501-2508, 2021.
- [8] F. Khan and O. Reyad, "Application of Intelligent Multi Agent Based Systems For E-Healthcare Security," *Information Sciences Letters*, vol. 8, no. 2, p. 67-72, 2019.
- [9] N. F. Mohammed, M. J. Jawad and S. A. Ali, "Biometric-based medical watermarking system for verifying privacy and source," *Kuwait Journal of Science*, vol. 47, no. 3, p. 2-13, 2020.
- [10] S. A. H. Alrubaie and A. H. Hameed, "Dynamic Weights Equations for Converting Grayscale Image to RGB Image," *Journal of University of Babylon for Pure and Applied Sciences*, vol. 26, no. 8, p. 122-129, 2018.
- [11] N. Cherabit, F. Z. Chelali and A. Djeradi, "Circular Hough Transform for Iris localization," *Science and Technology*, vol. 2, no. 5, pp. 114-121, 2012.
- [12] J. Daugman, "How Iris Recognition Works," in *The Essential Guide to Image Processing (Second Edition)*, Academic Press, 2009, p. 715-739.
- [13] C.-W. Chong, P. Raveendran and R. Mukundan, "Translation and scale invariants of Legendre moments," *Pattern Recognition*, vol. 37, no. 1, pp. 119-129, 2004.
- [14] P. Raviraj and M. Y. Sanavullah, "The Modified 2D-Haar Wavelet Transformation in Image Compression," *Middle-East Journal of Scientific Research*, vol. 2, no. 2, p. 73-78, 2007.
- [15] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *Pattern Recognition (ICPR), 2010 20th International*, Istanbul, 2010.