Data & Metadata. 2023; 2:56
doi: 10.56294/dm202356

ORIGINAL

Secure E-healthcare System Based on Biometric Approach

Sistema sanitario electrónico seguro basado en la biometría

Amal Fadhil Mohammed[1] ✉, Hayder A Nahi[1], Akmam Majed Mosa[1], Inas Kadhim[1]

[1]Al Qasim Green University. Computer Center. Babil, Iraq

Cite as: Fadhil Mohammed A, Nahi HA, Majed Mosa A, Kadhim I. Secure E-healthcare System Based on Biometric Approach. Data & Metadata. 2023; 2:56. https://doi.org/10.56294/dm202356

Submitted: 09-04-2023 **Revised:** 24-04-2023 **Accepted:** 07-07-2023 **Published:** 08-07-2023

Editor: Prof. Dr. Javier González Argote

ABSTRACT

A secure E-health care system is satisfying by maintaining data authenticity and privacy. Authentic users only access and edit medical records, any alteration in the medical records may result in a misdiagnosis and, as a result, harm the patient's life. Biometric method and watermarking modes are utilized to satisfy goal, such as Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Least Significant Bit (LSB). In this work focused on a biometric watermarking system where the iris code of the sender programmed as a sender authentication key. The confidentiality of the patient information is safeguarded via encrypting it with an XOR algorithm and embedding the key in the DCT image. The algorithm has demonstrated which is suggested system has met earlier constraints. We used samples of original watermarked images with PSNR value, embedding time and extraction time, the lowest embedding time was 0,0709 and the PSNR value was 49,2369.

Keywords: PSNR; LSB; Watermarking; Legendre Moment; DCT.

RESUMEN

Un sistema de atención sanitaria electrónica seguro se satisface manteniendo la autenticidad y privacidad de los datos. Los usuarios auténticos sólo acceden a los historiales médicos y los editan. Cualquier alteración en los historiales médicos puede dar lugar a un diagnóstico erróneo y, en consecuencia, perjudicar la vida del paciente. Para alcanzar este objetivo se utilizan métodos biométricos y marcas de agua, como la transformada wavelet discreta (DWT), la transformada discreta de Fourier (DFT), la transformada discreta de coseno (DCT) y el bit menos significativo (LSB). En este trabajo nos centramos en un sistema biométrico de marca de agua en el que el código del iris del remitente se programa como clave de autenticación del remitente. La confidencialidad de la información del paciente se salvaguarda encriptándola con un algoritmo XOR e incrustando la clave en la imagen DCT. El algoritmo ha demostrado que el sistema propuesto cumple los requisitos anteriores. Se utilizaron muestras de imágenes originales con marca de agua con valor PSNR, tiempo de incrustación y tiempo de extracción, el tiempo de incrustación más bajo fue de 0,0709 y el valor PSNR fue de 49,2369.

Palabras clave: PSNR; LSB; Marca De Agua; Momento De Legendre; DCT.

INTRODUCTION

The dramatic changes in our lives have been caused by information and communication technologies. These methods were also used by the healthcare sector. Information plays a significant role in the practice of health at all levels. E-health means using the technologies on the computer in practice health.(1) Since medical information plays an essential role of the health system, modifying it can result in incorrect diagnoses.

Information security and privacy protection are of the utmost importance when sending medical photographs over the internet because they also contain patient personal information.[2] To meet the security needs of medical images during transmission, a high level of protection and authentication is required. There are various security needs, including authenticity, secrecy, and integrity.[3] In the health care environment, confidentiality means that unauthorized persons cannot access the medical data; integrity means not modifying data through transmission and storage. Ultimately, the image ought to come from a reliable source.[4] Therefore, it was necessary to provide some techniques to overcome the challenges outlined above. One of these techniques, iris biometric, is the electronic identification and verification of a person based on their iris. Digital watermarking proved to be the best solution for satisfying the above security requirements.[3]

Related works

This section examines some of the previously proposed techniques for medical picture authentication and secrecy in the healthcare system.

Aditi Zear et al. studied DWT, DCT, and SVD watermarking for the healthcare environment. The proposed method uses three watermarks: a doctor's signature for identity authentication, and a patient's medical information, in the form of the image. a Backpropagation neural network (BPNN) used to the extracted watermark to increase the robustness of the watermarking. The image watermark further safeguarded by using the Arnold transform technique. Note: the symptoms and verification codes are encoded using lossless arithmetic techniques and Hamming codes. Then the compressed and encoded text is applied to the cover image, locked in a watermark., the NC value is equal to 0,90883. prosody Using the proposed method.[5]

G. Cetinel and L. Cerkezi proposed a system for watermarking medical images for authentication purposes. (SVD). And (DWT) are both used in this system. The private watermark is the patient's personal information embedded in the medical image. Arnold Cat Map (ACM) applied to the watermark to improve security. As a result, the proposed watermark scheme's target is personal authentication.[6]

Mirza et al. 2017've mixed encryption, steganography, and watermarking into a three-in-one method to create a composite security measure. It has three critical parts:[1] the original image was encrypted using a large secret key by rotating the pixel bits to the right using the XOR operation,[2] the encrypted image was altered by the cover image's least significant bits (LSBs) to create the steganography image,[3] and the resulting image was watermarked in the time and frequency domains to ensure ownership. The proposed strategy is economical, straightforward, and better protected against risks.[7]

Lamia et al. 2017 keep biometrics at a reasonable computational complexity while offering a new approach. It has successfully implemented fingerprint and face recognition, which is one of the most mature biometrics. Steps have taken to improve the quality of watermarking., the same watermarking algorithm is applied twice. It is crucial to examine who he is on the inside as well as who he leaves. Also, the face ID serves as the original photo's identification. The psychoanalytic associations were quite surprising. They demonstrate that the system can survive several signal processing attacks.[8]

In order to clarify identity and data authenticity, N. Hnoohom et al.[9] (2018) suggested a DWT-based image watermarking method for hiding patient data into a Region of Interest (ROI). Before watermarks are implanted, a Quick Response (QR) code image is generated from the patient's data to increase the security level of the data. Peak Signal-to-Noise Ratio (PSNR) and NC were used to assess imperceptibly and the degree of resemblance between the recovered watermark and the original watermark, respectively.

A two-layer strategy for protecting medical data was presented by S. Thakur et al.[10] in 2018. In order to hide patient information in the input image's first layer, the watermarking technique is applied, creating a watermarked image. To increase confidentiality, the watermarked image in the second layer is encrypted using a chaotic method. A subjective test was used to evaluate the quality of the watermarked images. The suggested approach complied with the security and robustness requirements.

A blind watermarking method based on the wavelet transform was created by S. Priya and Santhi[11] in 2019 to protect medical data and guarantee the authenticity of medical photographs. The algorithm embeds the patient's private information in the medical image as a watermark. The use of a visual medical image encryption approach next secures the existence of the watermarked medical image. To ensure source identification, a doctor's biometric fingerprint is also utilized.

In their 2020 proposal, Mohammed et al.[12] suggested two embeddings and an extraction watermark. The cover image was separated into a Region of Interest (ROI) and a Region of Non-Interest (RONI) using the DWT method. The iris code was utilized as a watermark from sending the doctor in order to add the watermark. The watermark for patient data. The eye iris region in the image was found by the automatic segmentation algorithm. Both are included in the NROI to boost security. A watermark with double encryption was sent to the NRIO. the RONI watermark from utilizing a similar technique (quadratic map). In the electronic health care system, the suggested watermarking technology will perform two crucial functions: safeguarding patient privacy and validating the data source.

https://doi.org/10.56294/dm202356

METHODS

Two watermarks are necessary for the proposed system to function; the first is the sender's iris code, which is required to confirm the sender's legitimacy. Encrypted patient data is the second watermark, used to guarantee patient confidentiality and data security. The suggested system had two stages: stage one involved preprocessing and embedding, while stage two involved retrieving and verifying data. First, after applying the DCT transformation to an image, the features taken from the authorized person's iris were encoded in the image using the XOR method and then embedded with the patient information (second watermark). The other person will complete the identical steps to create results in the second stage, which entails sending the first stage result to them. These treatments will reveal an individual's iris' characteristics. After extracting it, these attributes are compared to those that emerged from the first stage, and if the results of the check indicate that the individual is authorized and has the ability to decode patient information, access is permitted otherwise.

Two procedures make up the proposed system:

- The sending side embedding process.
- Recipient-side extraction and verification technique

Embedding Procedure

The initial watermarks are created, the second watermarks are encrypted, and then the embedding procedure is performed as part of the embedding technique on the sender side. The embedding technique's block diagram can be found in figure 1.

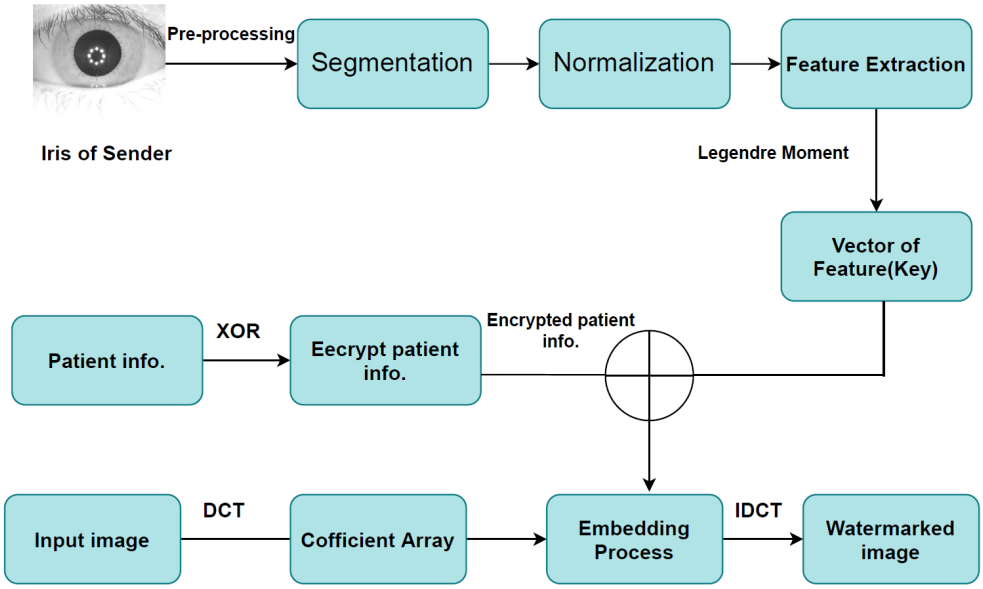


Figure 1. Block diagram of the first

The suggested approach employs two watermarks: the patient's information and the physician's Iris code. Here are some descriptions of these watermarks:

Step1: - Generating Iris code of the sender (physician)

The first watermark needs the development of an iris recognition system, which entails four steps: picture preprocessing, iris localisation, iris normalization, and feature extraction.

The following are the various phases of the iris identification technique outlined:

1. Pre-processing

Convert any image type to the gray image type before all operations. Whenever the data has undergone the prior processing, it is prepared for the following stage.

2. Iris Segmentation

The description of the pupillary and scleral boundaries is the first step in the identification method for the iris. The definition of iris biometric measurements requires the image processing system to be able to precisely pinpoint the iris region of the eye picture and distinguish eyelid regions, eyelashes, and reflection areas.[13] The pupil and outer iris boundary must be located in order to locate the iris.[14] One technique used in iris localization is the circular Hough transform (CHT), which is used to recognize any shape in the face.

With an unknown radius, the circular Hough transform can only find the circle's center. Equation provides the characteristic equation of a circle (1)

$$(x-a)2+(y-b)2=r2 \qquad (1)$$

where
$x = a + r * cos(\theta)$
$y = b + r * sin(\theta)$

Where (a, b) the circle's center, and (r) is the radius. That can describe as the parameter space will be 3-dimensional (a, b, r). All the variables that satisfy (x, y) would be available to see as a feature.[15] The inside and outside of the iris brighten differently, with the pupil expanding and the iris becoming smaller depending on the illumination. The critical stage of defining the boundaries between the sclera and the iris determines the outside iris boundary. Initially, there is no set limit around the iris area; however, there are other-centered edges. Compared to the light intensity between the sclera and the iris, points have a high light intensity. As a consequence, the edge detection system detects the iris's exterior edges. The quality of the eye image would be more critical for the localization iris[16] see in figure 2.

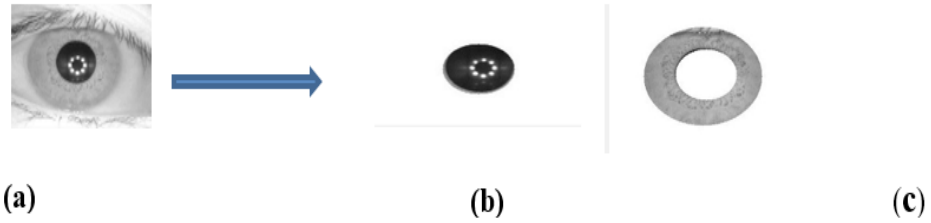


Figure 2. Steps of segmentation

3. Normalization

The segmented iris designed with Dogma's Rubber Sheet Model is flat and rectangular rather like a circular. The region of the iris is segmented and normalized by a transformation from the polar coordinate in the Cartesian coordinate after the computation of the inner and outer circles of the iris, as shown in figure 3. The polar coordinates defined by r (radial coordination) and θ, and Cartesian coordinates by x and y (equation2), so that the iris area is the matrix of data: The polar coordinates can be defined by:

$$X = r\cos\theta. \quad y = r\sin\theta \qquad (2)$$

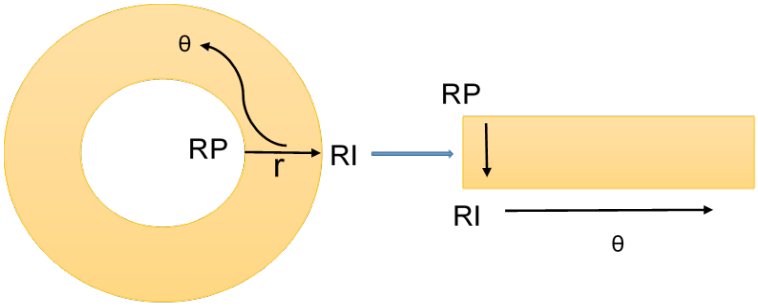


Figure 3. Daugman's rubber sheet model to conversion from Polar to Cartesian

An occlusion due to eyelids and eyelids is one of the problems in an iris recognition system. This occlusion increases the complexity of the fitting and extraction processes, as shown in figure 4.[17]

Feature Extraction

The iris identification system is currently in its third level. The most important phase in the iris recognition system is extracting useful features. The iris has been transformed into a rectangle and normalized before the feature extraction stage can start. Legendre Moment has been utilized in the suggested approach for that.

https://doi.org/10.56294/dm202356

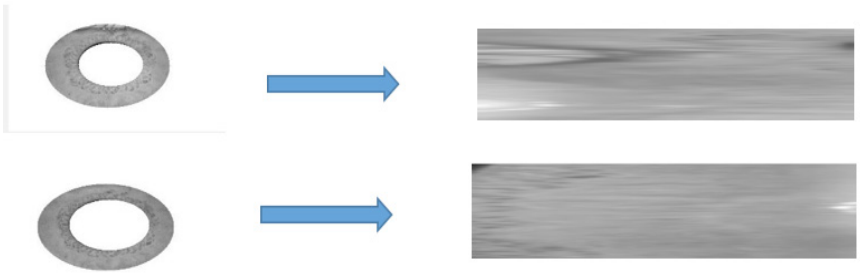


Figure 4. Sample of occlusion

Legendre Moment

The intensity function of the image is f(x,y), and Legendre's two-dimensional moments of order (p+q) are defined as follows:[18]

$$L_{pq} = \frac{(2p+1)(2q+1)}{4} \int_{-1}^{1}\int_{-1}^{1} P_p(x)P_q(y)f(x.y)\,dx\,dy \quad \text{where } x,y \in (-1.1) \tag{3}$$

beginning with Pp(x), a Legendre polynomial of rank p.

$$P_p(x) = \sum_{k=0}^{p}\left\{(-1)^{\frac{p-k}{2}}\frac{1}{2p}\frac{(p+k)!x^k}{\left(\frac{p-k}{2}\right)!\left(\frac{p+k}{2}\right)!k!}\right\}_{p-k=even} \tag{4}$$

A recurrent relationship shown following can be utilized to compute the Legendre polynomial.

$$P_p(x) = \frac{(2p-1)xP_{p-1}(x)-(p-1)P_{p-2}(x)}{p} \quad \text{for } p>1 \tag{5}$$
$$P_0(x) = 1.P_1(x) = x$$

To derive Legendre's moments from a digital image, summations must be used in place of integrations in the previous equation (3), and the image coordinates must be normalized to (-1; 1). The approximate numerical representation of Legendre moments for a discrete image of the NN pixels with f(x;y) is:

$$L_{pq=\lambda_{pq}} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} P_p(xi)P_q(yj)f(i.j) \tag{6}$$

Assuming normalization is constant:

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

(xi) and (yj) represent the normalized pixel coordinates for the (-1,1) range provided via:

$$x_i = \frac{2i}{N-1} - 1 \quad \text{and} \quad y_j = \frac{2j}{M-1} - 1 \tag{7}$$

Step2: Encrypt the second watermark

Patient data is the second watermark. This watermark is employed to maintain patient data confidentiality. Diagnoses can be aided by patient information like doctor's name, age of patient, address of patient, submission date, and diagnosis outcome. The suggested approach employed XOR encryption to protect patient data.

Step 3: embedding process

Applying the Discrete Cosine Transform (DCT) on the image and then embed the encrypted patient information with the vector produced from the Legendre Moment (key) in the image resulting from step 1.4

DCT Transform

Due to its simplicity and great energy compaction, the DCT is one of the most frequency transformations that used in image and video processing. DCT represents the image as a collection of sinusoids with varying (frequencies, magnitude). The output of the G (u, v) transform computed over an input image f (x, y). as follows:[19]

https://doi.org/10.56294/dm202356

$$G(u.v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x.y)\cdot\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cdot\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (8)$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{2}} & if\ u = 0 \\ One\ if\ u = 1.2.\cdots M-1 \end{cases}$$

$$\alpha(v) = \begin{cases} \sqrt{\frac{1}{2}} & if\ v = 0 \\ One\ if\ v = 1.2.\cdots N-1 \end{cases}$$

the image reconstructed using IDCT following equation

$$f(u.v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha(u)\alpha(v)\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} G(u.v)\cdot\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cdot\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (9)$$

The image is divided into non-overlapping 8*8 blocks. The DC coefficient is the first DCT coefficient, X (0,0). In both the vertical and horizontal axes, the DC coefficient has zero frequency. Because it refers to the average of the pixel values in the league, it indicates the brightness of the image block. The AC coefficients are the remainder coefficients.

Step 4: Extracting Process

The result of the embedding process sent to another person that is doing the flowing:

1. Create iris code for the receiver by applying the same procedure in the step1
2. Extract the **(key)** from the image generated in step1, then compare it with the result of step 4.1

The block diagram of the Extracting technique shown in figure 5.

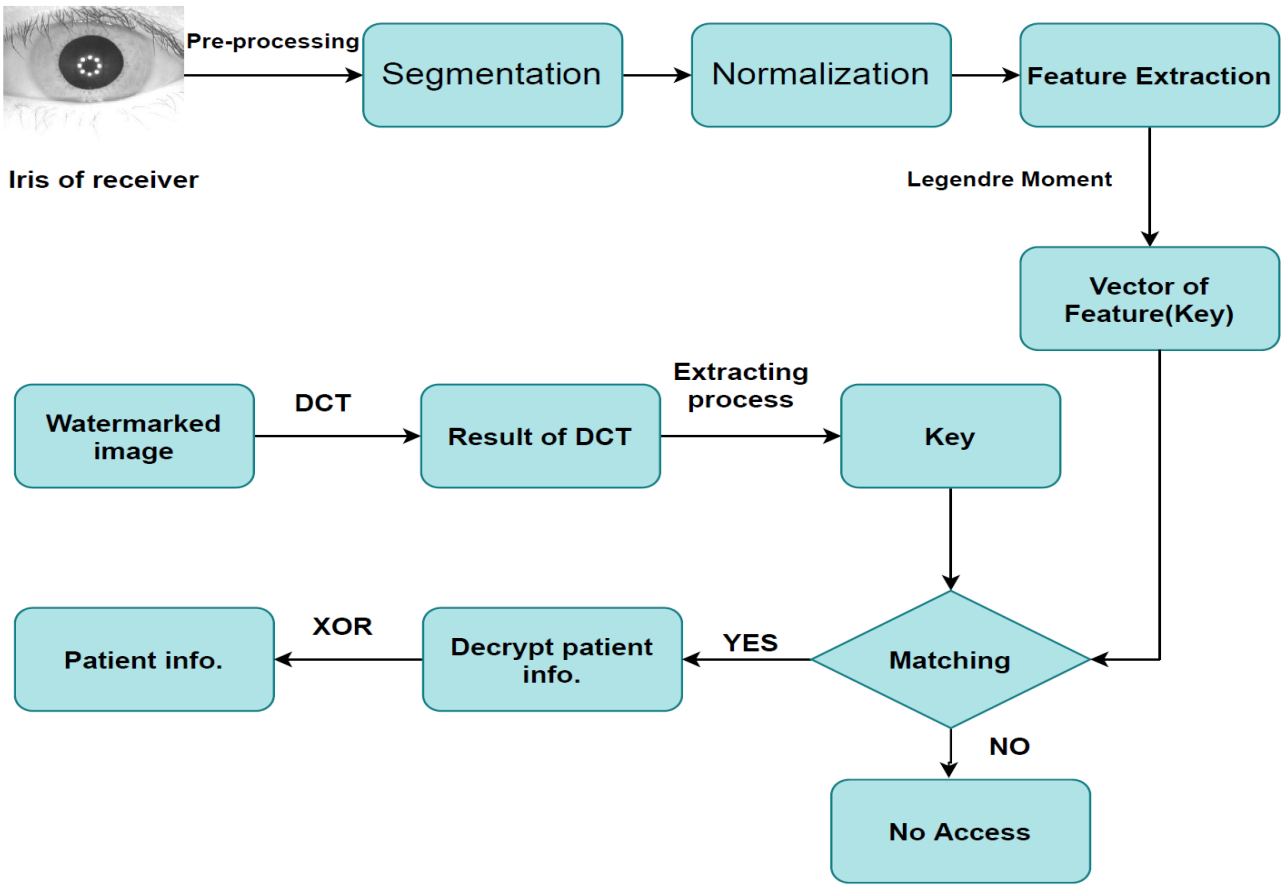


Figure 5. Block diagram of the second stage(Extracting)

https://doi.org/10.56294/dm202356

Step 5: The Matching

The person who receives it will receive a key that he employs the structural similarity index measure (SSIM) to compare to the features obtained in step 1; if the result is one, it means that the recipient is the authorized source that decodes the encrypted text and extracts the patient's data. If the result is zero, the recipient is not approved. There are three steps in the matching process:

1. The same person and the same snapshot
2. The same person and another snapshot
3. Another person

SSIM

The SSIM method compares two photos to see how similar they are. The outcomes SSIM index are a decimal value between 0 and 1, with 1 signifying perfect structural similarity between two pieces of data that are exactly the same. If the value is zero, there is no structural similarity between the two images.

RESULTS AND DISCUSSION

Environments

1. An image from a (CASIA-V4-Interval) database using the suggested method.
2. The generated system was simulated using the programming language (MATLAB version R2018a). Both the HP (z book) laptop and the Windows 7 operating system are compatible with the programs.

System performance

The iris code and the image of the patient's information make up the watermark's two components. The iris extracted corresponds to the sender iris code utilizing the structural similarity index measure (SSIM). The system checks the sender's legitimacy. The iris images obtained for the exact person do not correspond completely to the reason that they were assumed underneath different situations. A threshold t of allowable variation between two iris codes must be established to get the optimal performance characteristics. The suggested approach sets a threshold of 0,5; if the SSIM outcome is better considerable compared with a threshold, it indicates that the original is authentic, and the patient data is subsequently decrypted.

Accuracy measuring

Signal to Noise Ratio (SNR) and Peak Signal to Noise Ratio (PSNR) is used to assess the accuracy of the scheme of embedding. And PSNR is computed via equation.[10]

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

And SNR is given by equation (11)

$$SNR = 10\log\frac{P_{signal}}{P_{noise}} \quad (11)$$

in which MSE is the mean square, that calculated utilizing equation (12), and L is the number of bits at the most that may be used to represent an image's pixels.

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

in which W stands for the watermarked image and N is the size of the cover image.

Table 1 shows samples of the original and watermarked images

https://doi.org/10.56294/dm202356

Table 1. Samples of the original and watermarked images

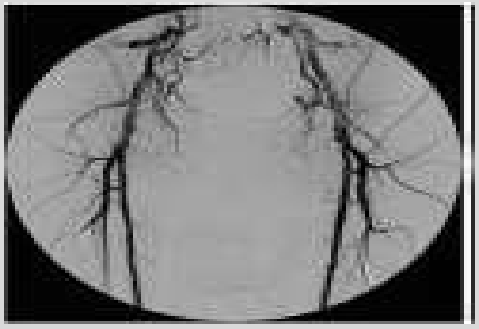
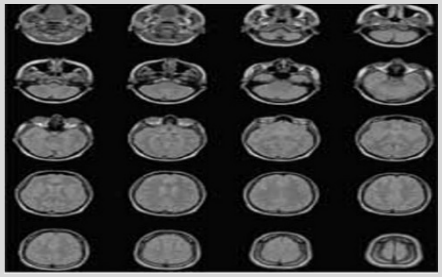
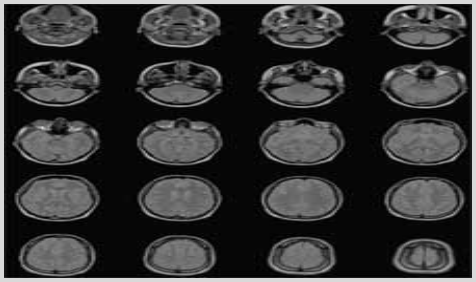
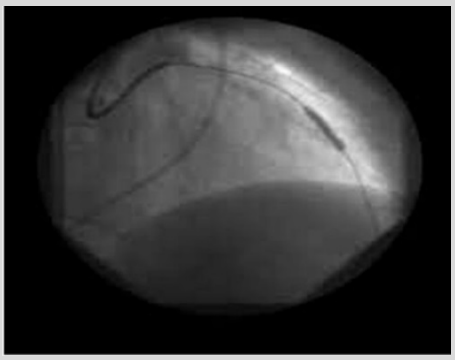
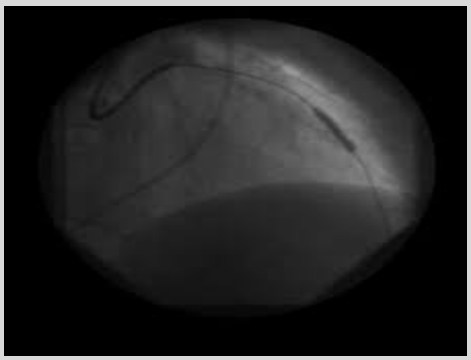
SSIM	Watermarked image	Original image
0,9999		
0,9987		
0,9899		

Table 2 indicates samples of the original and watermarked images with their PSNR val*ue*, time of Embedding and time of Extraction

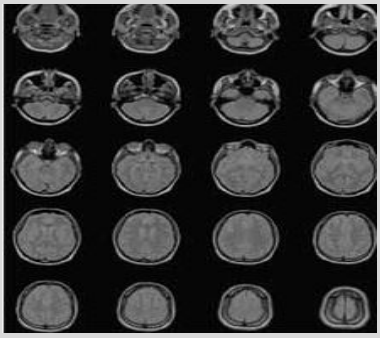
Table 2. Samples of the original and watermarked images with their PSNR value

Time of Extraction	Time of Embedding	PSNR	Watermarked image	Orginal Image
0,0401	0,1373	47,2503	Image1	Image1
0,0288	0,0812	47,8381	Image2	Image2
0,0250	0,0976	48,9027	Image3	Image3
0,0233	0,0761	47,2503	Image4	Image4
0,0284	0,0889	48,3027	Image5	Image5
0,0246	0,0718	49,2369	Image6	Image6
0,0211	0,0709	47,2503	Image7	Image7

PSNR values are affected by a variety of factors, including the size of the watermark and the image. Table 3 displays the PSNR values for watermark of various sizes.

https://doi.org/10.56294/dm202356

Table 3. Comparison between PSNR value and watermark size

Input image	Size of watermark (in bits)	PSNR value
	1672	48,3118
	2120	48,1924
	3048	47,8615
	3920	47,5952
	6000	47,0292
	1672	49,2712
	2120	48,8750
	3048	48,4408
	3920	48,2363
	6000	47,4211

Another element that affects the PSNR value is the size of the covered image. Table (4) displays the PSNR values for photos of various sizes.

Table 4. Comparison between PSNR value and image size

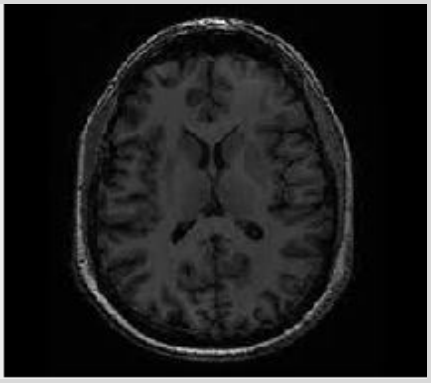
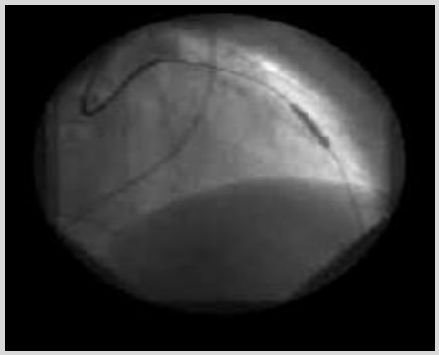
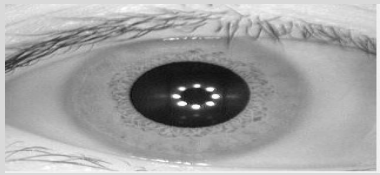
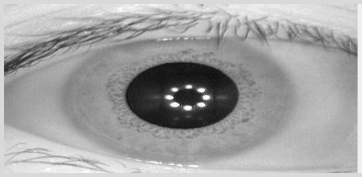
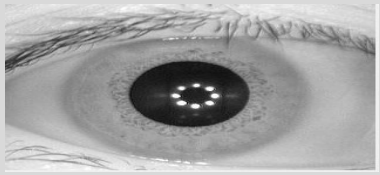
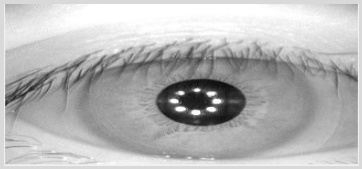
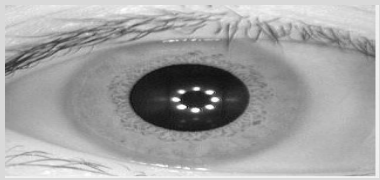
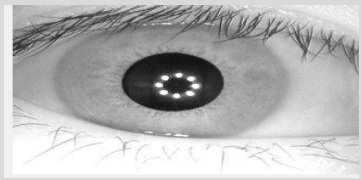
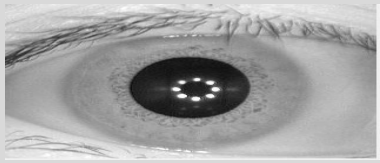
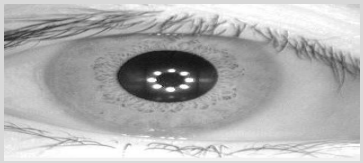
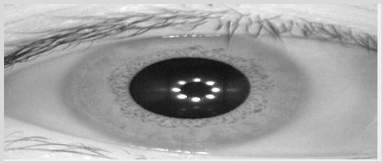
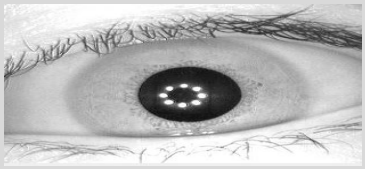
Input image	Size of image	PSNR value
	512*512	49,5876
	1024*1024	50,2975
	2048*2048	51,1544
	3072*3072	52,2332
	4096*4096	52,9932
	512*512	50,4685
	1024*1024	51,3761
	2048*2048	53,7960
	3072*3072	54,9389
	4096*4096	57,1920

Table 5 comparison iris code for sender and receiver with access state for the system.

https://doi.org/10.56294/dm202356

Table 5. Comparison iris code

Iris sender	Iris receiver	SSIM	Access state
		1	YES
		0,723	YES
		0,121	NO
		0,647	YES
		0,253	NO

CONCLUSION

The suggested system embeds the feature (key) generated by the Legendre Moment utilizing the DCT. In order to preserve the patient's privacy, the proposed solution also encrypted the patient's data using the XOR method. This technology seeks to respect patient privacy and source authentication. New results were obtained for different images, and the maximum PSNR was 57,1920 compared to another image of the same size, which reached 52,9932. These were the results of the relationship between the PSNR value and the image size. As for the relationship between the PSNR value and the size of the watermark, the results were somewhat close by obtaining the highest value of 49,2712 for the first image, while the second was very slightly less than 48,3118.

REFERENCES

1. Khalil M, Jones R. Electronic Health Services: An Introduction to Theory and Application. Libyan J Med. 2007;2(4):202–210. doi: 10.4176/071117.

2. Liao X, Yin J, Guo S, Li X, Sangaiah AK. Medical JPEG image steganography based on preserving inter-block dependencies. Comput Electr Eng. 2018;67:320–329. doi: 10.1016/j.compeleceng.2017.08.020.

3. Hazzaa HM, Ahmed SK. Watermarking Algorithm for Medical Images Authentication. Proc - 2015 4th Int Conf Adv Comput Sci Appl Technol ACSAT 2015. 2016;239–244. doi: 10.1109/ACSAT.2015.48.

4. Aparna P, Kishore PVV. An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm. J Intell Syst. 2018;27(1):115–133. doi: 10.1515/jisys-2017-0266.

5. Zear A, Singh AK, Kumar P. A proposed secure multiple watermarking techniques based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl. 2016; doi: 10.1007/s11042-016-3862-8.

6. Çetinel G, Çerkezi L. Wavelet-Based Medical Image Watermarking Scheme for Patient Information

Authenticity. Int J Appl Math Electron Comput. 2016;4(Special Issue-1):220. doi: 10.18100/ijamec.270334.

7. AzzRaq MA, Shaikh RA. Digital Image Security: Fusion of Encryption, Steganography and Watermarking. 2017;8(5):224–228.

8. Haddada LR, Dorizzi B, Essoukri N, Amara B. A combined watermarking approach for securing biometric data. Signal Process Image Commun. 2017; doi: 10.1016/j.image.2017.03.008.

9. Hnoohom N, Sriyapai C, Ketcham M. Robust watermarking for medical image authentication based on DWT with QR codes in telemedicine. Springer International Publishing; 2018.

10. Thakur S, Singh AK, Ghrera SP, Elhoseny M. Multi-layer security of medical data through watermarking and chaotic encryption for telehealth applications. Multimed Tools Appl. 2019;78(3):3457–3470. doi: 10.1007/s11042-018-6263-3.

11. Santhi SPB. A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images. 2019.

12. Mohammed NF, Jawad MJ, Ali SA. Biometric-based medical watermarking system for verifying privacy and source authentication. 2020;47(3):2–13.

13. Turker M, Koc-san D. Building extraction from high-resolution optical spaceborne images using the integration of support vector machine (SVM) classification, Hough transformation and perceptual grouping. Int J Appl Earth Obs Geoinf. 2015;34:58–69. doi: 10.1016/j.jag.2014.06.016.

14. Proenc H, Alexandre A. Iris Recognition: An Analysis of the Aliasing Problem in the Iris Normalization Stage. 2006;1771–1774.

15. Cherabit N, Chelali FZ, Djeradi A. Circular Hough Transform for Iris localization. Sci Technol. 2012;2(5):114-121. doi: 10.5923/j.scit.20120205.02.

16. Arvacheh E. A study of segmentation and normalization for iris recognition systems. Masters Dissertation. Univ. Waterloo; 2006. Available from: http://www.collectionscanada.gc.ca/obj/s4/f2/dsk3/OWTU/TC-OWTU-1045.pdf.

17. Daugman J. BY THEIR 5 RECOGNIZING PERSONS IRIS PATTERNS.

18. Chong CW, Raveendran P, Mukundan R. Translation and scale invariants of Legendre moments. Pattern Recognit. 2004;37(1):119–129. doi: 10.1016/j.patcog.2003.06.003.

19. Ben Halima N, Khan MA, Kumar R. A novel approach of digital image watermarking using HDWT-DCT. GSCIT 2015 - Glob Summit Comput Inf Technol - Proc. 2015; doi: 10.1109/GSCIT.2015.7353317.

FINANCING

No financing.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Amal Fadhil Mohammed, Akmam Majed Mosa, Inas Kadhim.
Research: Amal Fadhil Mohammed, Akmam Majed Mosa, Inas Kadhim.
Writing - proofreading and editing: Amal Fadhil Mohammed, Akmam Majed Mosa, Inas Kadhim.