MEDICAL IMAGES AUTHENTICATION IN CLOUD SYSTEM USING MODIFIED DISCRETE WAVELET TRANSFORM – (A FRAMEWORK)

OLADIMEJI Adegbola Isaac[1], Hussaini Yusuf AMANA[2]
[1,2,] Department of Computer Science, Aminu Saleh College of Education, Azare Nigeria

[1]oladimejiadeisaac@gmail.com, [2]hussainiamana@gmail.com

Keywords: medical image, cloud system, modified discrete wavelet transform, authentication

Abstract: *This study proposes a modified algorithm to secure medical images in cloud environments. In the proposed study, the medical image dataset will be obtained online from a standard medical image format called DICOM (digital imaging and communications in medicine) and will be transmitted to the system for compression. The steganography technique will be used to hide patient information in encrypted images performed using modified discrete wavelet transform (DWT-MPSO).* It *aims to demonstrate the fact that the DWT-MPSO technique can be used to improve the security, robustness, and quality of watermarked images.*

1. INTRODUCTION

In recent years, modern healthcare providers have been generating huge medical images every day thanks to recent advances in imaging tools [1]. The need to apply security techniques to medical imaging is increasing with the adoption of telecommunications technology for medical diagnosis and patient care. If the adventure sponsor and the client are disconnected due to distance, a system called telemedicine is used in such cases [2]. According to Sefer and Abdulrahman [2], telemedicine is of great importance because it provides the possibility of consulting specialists remotely, individual patient data is not lost, and is available immediately, as well as better communication between health system partners.

Cloud computing appears to be a promising network infrastructure model capable of cost-effectively deploying large-scale applications [3]. Cloud computing is an environment that delivers packaged resources over the Internet in the form of dynamic, scalable, and virtualized services that provide a variety of on-demand services to people, such as cloud computing. Cloud and telemedicine services [2]. Using the cloud and sharing medical images will help ensure patient safety and satisfaction by reducing duplicate testing, potentially saving money, and protecting people from test side effects. Repeated experiments [4]. The benefits of placing medical imaging in the cloud include data portability, flexible and incremental storage, data migration, and patient-centric connectivity [4].

A study by Botta et al. [5] notes that cloud computing has virtually unlimited storage and processing capabilities, is a much more mature technology, and at least partially solves most of the problems of cloud computing, but Qusay et al. [3] point out that there are several important cloud security challenges in cloud computing environments, including mobility issues, application security and dynamics, network service issues, and applications platform issues. [4] Stated that data integrity, confidentiality, and non-repudiation can be at risk because the cloud is a multi-tenant environment. Therefore, when transmitting user data through cloud environments, especially medical data, this type of data containing very important patient information requires a high level of protection in terms of integrity and confidentiality of the data. This data must be secured to avoid attacks they may encounter [5].

Nyeem [7] notes that the confidentiality of medical information achieved through strict ethical laws and legislation provides patients with medical ethical rights and responsibilities. The need to secure medical images and other patient data is necessary not only for privacy purposes but also to prevent possible manipulation by attackers during transmission from one medical center to another medical center. If a medical image is falsified and sent to a specialist or radiologist, it can lead to a misdiagnosis, leading to serious problems or even death [7].

2. RELATED WORK

To solve all the problems of data integrity, confidentiality, and non-repudiation in cloud medical image security, many researchers have proposed different methods, algorithms, and techniques, involving cryptography, steganography, or even a combination of both. Some of these suggestions are:

Alowolodu et al., [8], proposed to secure medical images using quantum cryptography, the design is implemented using the Shor algorithm, random secret key generation, and eavesdropping detection (factor algorithm quantum N Shor).

Smita and Vijayakumar [9], proposed encryption and watermarking of medical images, combining encryption and watermarking schemes. The proposed technique starts with extracting a region of interest (ROI) from the image using saliency detection. The protruding part of the image is then encrypted using a complex and highly secure encryption technique while the non-protruding part is watermarked and then encrypted using a simple but effective encryption technique.

Askar et al, [10], proposed lossless medical image security. This study describes current methods, previous work, security needs, and requirements for new systems, and predetermines an approach for further research in medical image security with no data loss.

Another approach was presented by Khalill [11], the study of Medical Image Quality degradation when embedding data in the frequency domain, he made use of the RC4 encryption technique, which he applied for the encryption and decryption of information, Least Significant Bit (LSB) technique in the spatial domain and discrete Fourier Transform (DFT) technique in the frequency domain are used for steganography.

Parah et al [12] used a novel high-capacity, reversible data hiding system for e-healthcare applications. The pixel-to-block (PTB) conversion technique has been used as an efficient and computationally efficient alternative for interpolation to generate cover images to ensure the reversibility of medical images.

A study by Sefer and Abdulrahman [2] proposed the use of a chaos-based medical image encryption algorithm, based on the traditional chaos-based image cryptography architecture developed by Fridrich, which includes some basic operations. The least significant bit (LSB) method is applied to the encrypted medical images, and each encryption key of the medical image as well as the medical data resulting from the separation of the DICOM file is used as the steganography data. The researchers concluded by suggesting future work implementing the hybrid model using other encryption techniques such as the Advanced Encryption Standard (AES) algorithm with the least significant bit algorithm or using a selected logistics map with a watermarking method such as a reversible watermark and evaluate the results to maximize robustness against attack attempts.

Most of the aforementioned studies have common and major drawbacks related to the types of encryption algorithms used. The disadvantages of current systems are the problem of image noise, lack of proper encoding methods, outdated watermarking systems, etc. [2]. Due to the disadvantages of user data privacy in cloud environments as well as further investigation and research into the shortcomings of existing solutions, this research aims to develop medical imaging form authentication in a cloud system using modified discrete wavelet transform (MDWT) can protect data. Privacy in cloud environments, this will help address key issues that prevent users from trusting cloud services. In other words, the research aims to give users self-control over their data files. Furthermore, the problem of time complexity required to complete the entire process will be completely resolved.

3. PURPOSE OF THE STUDY

The main implication of this study for the watermarking of patient information is that a modified approach will be developed for the watermarking technique. In this study, a secret key, based on the best-fit block criterion through the influence of particle swarm optimization, will be developed. This essentially makes the proposed watermarking method more powerful and flexible in protecting medical images. The blocking technique would be preferred to replace medical images with watermarked patient information because it results in a negligible change in the medical image. The proposed method will use discrete wavelet transform (DWT) to decompose medical images. Detail coefficients obtained using discrete wavelet transform (DWT) of the image are used to integrate patient information in a manner that produces very small variations or changes during integration. The proposed approach consists of two stages: the coating stage and the extraction stage. Details of these stages are described in the methodology.

Discrete wavelet transform (DWT) is a linear signal processing technique that transforms time domain signals into “wavelet” domains [13]. Discrete wavelet transform (DWT) is typically implemented using a finite impulse response (FIR) filter bank structure [14]. There have been a significant number of research proposals on the application of discrete wavelet transform (DWT) in digital watermarking and imaging systems due to its excellent and superior properties, but the scope is limited. Optimization in this area is significantly smaller. Discrete Wavelet Transform (DWT) optimized for digital image watermarking is capable of creating transparency and perceptual reliability between the watermarked image and the extracted image [15, 16].

4. METHODOLOGY

In this study, a modified algorithm for secure medical imaging in a cloud environment will be developed. The medical image dataset will be obtained online from a standard medical image format called DICOM (digital imaging and communications in medicine) and will be transmitted to the system for compression. The steganography technique will be used to hide patient information in encrypted images realized via modified discrete wavelet transform (DWT-MPSO).

4.1 EMBEDDING PHASE

The block diagram of the proposed embedding phase is illustrated in Figure 1. In the embedding phase, the image (I) is decomposed into four sub-frames such as approximation coefficients (I_A), horizontal detail coefficients (I_H), vertical detail coefficients (I_V), and diagonal detail coefficients (I_D) using Discrete Wavelet Transform (DWT). Similarly, the secret fingerprint (S) is decomposed into four sub-images such as approximation coefficients (S_A), horizontal detail coefficients (S_H), vertical detail coefficients (S_V), and diagonal detail coefficients (S_D) using Discrete Wavelet Transform (DWT). These sub-images are partitioned into non-overlapping blocks. The blocks of S_A will be matched with blocks of I_A using the root mean square method. The difference blocks are computed using the best-matched blocks of I_A and of S_A. The replacement of difference blocks is done with best-matched block coefficients of *I_H*, *I_V*, or *I_D*. The Inverse Discrete Wavelet Transform (IDWT) is applied on *I_A* and modified detail coefficients $(I'_H, I'_V, and\ I'_D)$ to get watermark image (I').

The steps of the embedding procedure are described in detail as follows:

Step 1: Decompose the image (*I*) and the secret data medical image (*S*) into four sub-images (I_A, I_H, I_V, I_D) and (S_A, S_H, S_V, S_D) respectively using DWT.

Step 2. Each of S_A, I_A, I_H, I_V, and I_D are divided into blocks of 4 × 4 pixels and can be represented as:

$$\begin{gathered} S_A = \{B_{SA_i}, 1 \le i \le S_{A_n}\} \\ I_A = \left\{B_{IA_j}, 1 \le j \le I_{A_n}\right\} \\ I_H = \{B_{IH_k}, 1 \le k \le I_{H_n}\} \\ I_V = \{B_{IV_l}, 1 \le l \le I_{V_n}\} \\ I_D = \left\{B_{ID_p}, 1 \le p \le I_{D_n}\right\} \end{gathered} \tag{1}$$

where B_{SA_i} represents *i*th block in S_A. B_{IA_j} designates *j*th block in I_A. B_{IH_k}, B_{FV_l}, and B_{ID_p} represent *k*th block in I_H, *l*th block in I_V and *p*th block in I_D. S_{A_n}, I_{A_n}, I_{H_n}, I_{V_n}, and I_{D_n} denote a total number of 4 × 4 blocks in each of S_A, I_A, I_H, I_V, and I_D respectively.

Step 3: For each block, B_{SA_i} in S_A, the best matched block B_{IA_j} of minimum error in I_A is explored using Particle Swarm Optimization. The first secret key K_1 contains the addresses *j* of the best matched blocks in I_A.

Step 4: Compute the difference block DB_i between B_{SA_i} and the best-matched block of B_{IA_j} as follows:

$$DB_i = B_{SA_i} - \left(\min_{1 \le j \le I_{A_n}} B_{IA_j}\right) \tag{2}$$

Step 5: For each difference block DB_i, the best-matched block B_{IH_k} in I_H, (that is, FIT_{ik}) is explored using PSO. Similarly, the best-matched block B_{IV_l} in I_V (that is, FIT_{ik}) and B_{ID_p} in I_D, that is, FIT_{ik}) is also explored using PSO.

Step a: Generate random population of N, Set parameter ω_{min}, ω_{max}, c_1 and c_2 of PSO

Step b: Initialize population of particles having positions x_n and velocities v_n

Step c: Set iteration k = 1

Step d: Calculate the fitness of particles $F_{ik}(t) = f\left(FIT_{ik}(t)\right)$ and find the index of the best particle b

The feature is generated by calculating the fitness function.

$$FIT_{ik}(t) = \min_{1 \le k \le N} \sqrt{\frac{\sum_{k=1}^{N}(DB_k - B_k)}{N}} \tag{3}$$

Step e: Select $G_{best_n}(t) = FIT_{bk}(t)$ and $P_{best_{mn}}(t) = FIT_{ik}(t)$

Step f: $\omega = \omega_{max} - k \times \frac{\omega_{max} - \omega_{min}}{Max_{no}}$ (4)

Step g: Update the velocity and position of particles

$$v_{ik}(t+1) = \omega\bar{v}_{ik}(t) + c_1 r_1\left(P_b - FIT_{ik}(t)\right) + c_2 r_2\left(G_b - FIT_{ik}(t)\right) \tag{5}$$

$$FIT_{ik}(t+1) = FIT_{ik}(t) + v_{ik}(t+1) \tag{6}$$

Step h: Evaluate fitness $I_{ik}(t+1) = f\left(FIT_{ik}(t+1)\right)$ and find the index of the best particle b_1

Step i: Update $Pbest$ of population

If $I_{ik}(t+1) < I_{ik}(t)$ then $P_{best_{ik}} = FIT_{ik}(t+1)$ else

$$P_{best_{ik}}(t+1) = P_{best_{ik}}(t+1) \tag{7}$$

Step j: Update $Gbest$ of population

If $I_{bk}(t+1) < I_{ik}(t)$ then $G_{best_k}(t+1) = P_{best_{bk}}(t+1)$ and set $b = b_1$ else

$$G_{best_k}(t+1) = G_{best_k}(t) \tag{8}$$

Step k: If $k < Max_{no}$ then $k = k + 1$ and goto *step f* else goto *step l*

Step l: Output optimum solution as $G_{best_k}(t)$.

$$B_{bestmatched} = G_{best_k}(t) \tag{9}$$

Step 6: Replace DB_i with best best-matched block of either FIT_{CH}, *FIT*CV, or *FIT*CD. The secret data keys K_2, K_3, and K_4 contain the addresses *k, l,* and *p* for the best-matched block of FIT_{CH}, FIT_{CV} and FIT_{CD} respectively

$$DB_i = \min\{Bt_{CH}, Bt_{CV}, Bt_{CD}) \tag{10}$$

Step 7: Repeat **Steps 3 to 6** until all the produced difference blocks are embedded in I_H, I_V, and I_D.

Step 8: Apply the inverse DWT to the I_A and the modified sub-images $I'_H, I'_V, and\ I'_D$ to obtain the watermarked image I'.

4.2 EXTRACTION PHASE

The block diagram of the proposed extraction phase is illustrated in Figure 2. In the extraction phase, the watermark image (I') is decomposed into four sub-images using Discrete Wavelet Transform (DWT). The sub-images are partitioned into non-overlapping blocks. The best-matched blocks are extracted from I'_A. The difference blocks are extracted from detail coefficients blocks. The secret medical image will be generated from different and best-matched blocks of I'_A.

The steps of the extracting procedure are as follows:

Step 1: Decompose watermark-image I' into four sub-images $I'_A, I'_H, I'_V, and\ I'_D$ using Discrete Wavelet Transform (DWT).

Step 2: Each of $I'_A, I'_H, I'_V, and\ I'_D$ are divided into blocks of 4 × 4 pixels and can be represented as:

$$I'_A = \left\{B_{IA_j}, 1 \le j \le I_{A_n}\right\}$$

$$I'_H = \left\{B_{IH_k}, 1 \le k \le I_{H_n}\right\}$$

$$I'_V = \left\{B_{IV_l}, 1 \le l \le I_{V_n}\right\}$$

$$I'_D = \left\{B_{ID_p}, 1 \le p \le I_{D_n}\right\} \tag{11}$$

Step 3: Extract the best-matched block B_{IA_j} from sub-image I'_A using the first secret key K_1.

Step 4: Extract the difference blocks DB'_I from sub-images $I'_H, I'_V, and\ I'_D$ using secret keys K_2, K_3, and K_4 respectively.

Step 5: The secret blocks B_{SA_i} are computed as:

$$B_{SA_i} = B_{IA'_j} - DB'_i \qquad \forall i = 1, \dots, S_{A_n} and\ j = 1, \dots, I'_{A_n} \tag{12}$$

Step 6: The blocks of approximation coefficients of the secret fingerprint (S'_A) are rearranged using secret key K_1.

Step 7: Allocate each of the sub-images $S'_H, S'_V, and\ S'_D$ as zeros and apply Inverse Discrete Wavelet Transform (IDWT) on both approximation (S'_A) and detail coefficients $I'_H, I'_V, and\ I'_D$ to obtain the embedded secret medical image.

5. IMPLEMENTATION VIEW OF THE PROPOSED FRAMEWORK

The implementation of the developed technique in medical images using enhanced Discrete Wavelet Transform (DWT) involves: loading of the medical images, image pre-processing, image watermarking. The test dataset will be used to test the developed system and its evaluation will be done using the performance metrics for both Discrete Wavelet Transform (DWT) and modified Discrete Wavelet Transform (DWT). An interactive Graphic User Interface (GUI) will be developed with an online database. The implementation tool to be used is MATLAB R2020a version on Windows 10 Enterprise 64-bit operating system, Intel®Pentium® CPU T4500@2.30GHZ Central Processing Unit, 4GB RAM and 500 Gigabytes hard disk drive.

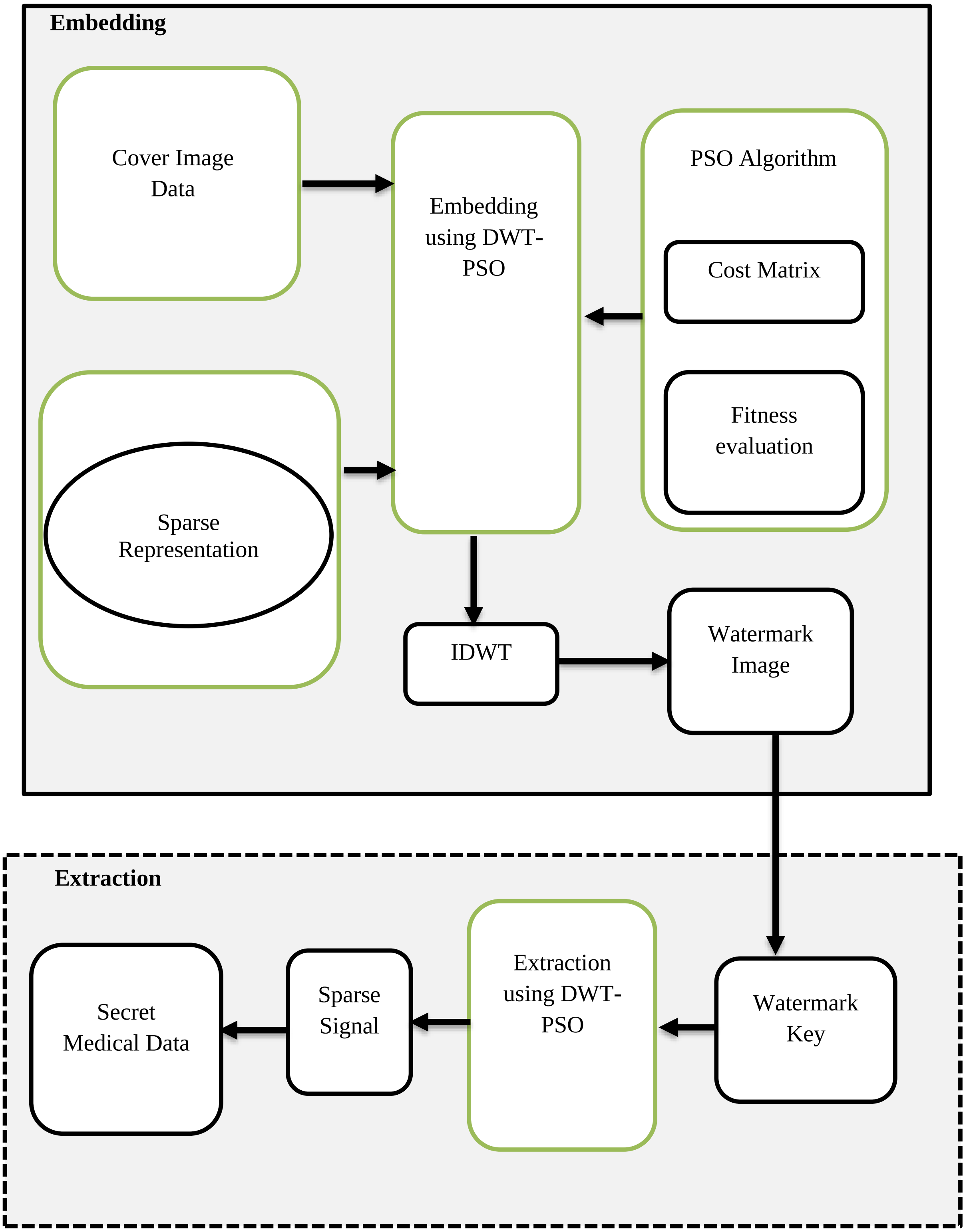

Figure 1: Block Diagram of the Developed DWT-MPSO

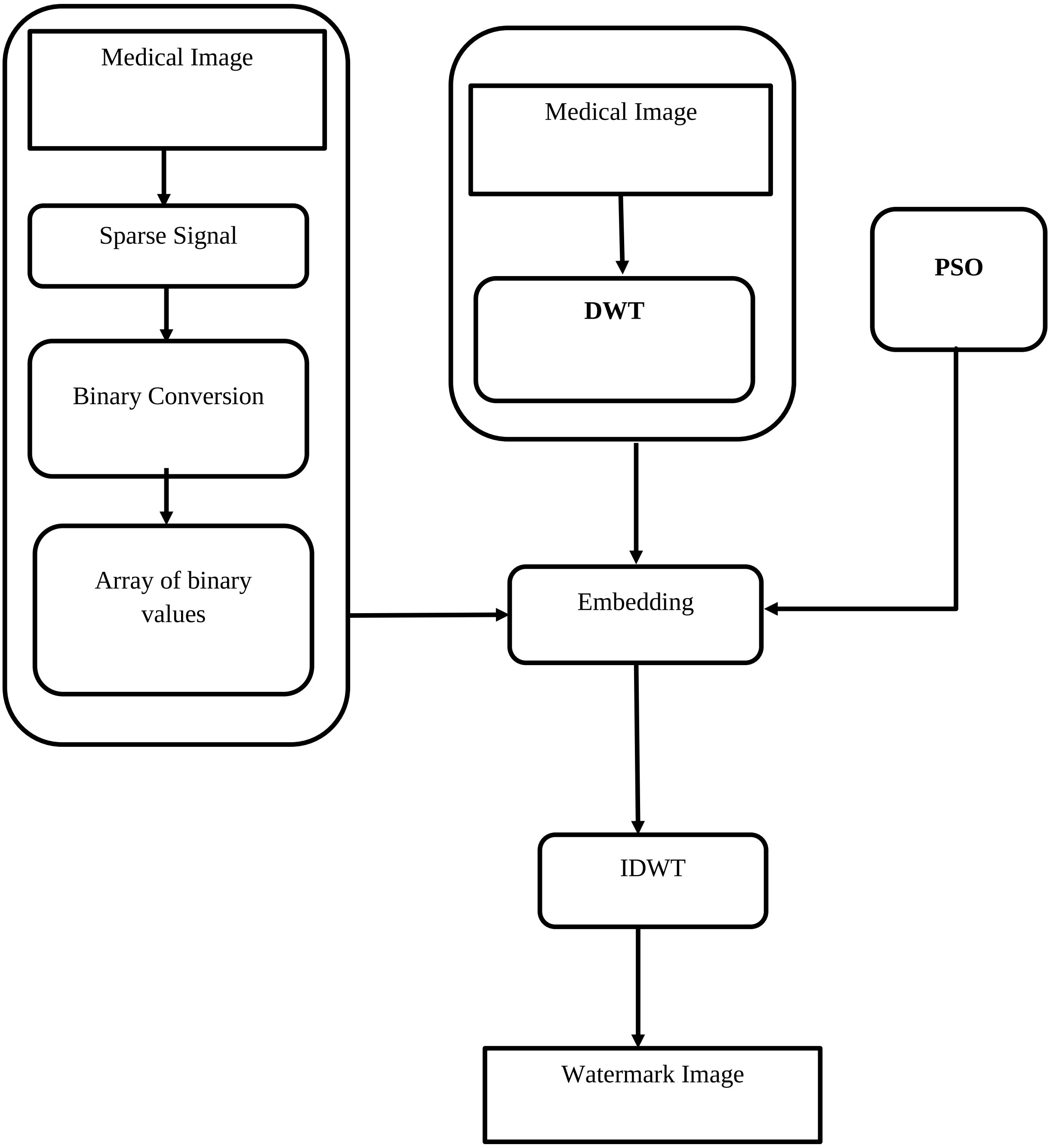

Figure 2: Block Diagram of the Embedding Process

The performance measures to be employed in this study are, peak signal-to-noise-ratio (PSNR) and mean square error (MSE). The peak signal-to-noise ratio (PSNR) is used as a measurement to test the quality of the medical image. The higher the medical image PSNR value is, the better the medical image quality is. It is an objective measurement for the medical image encryption effect. Generally speaking, if the PSNR is less than a set dB value, then the confidentiality of the medical image is preserved. The mean squared error for two streams, stored in vectors A and B, is computed as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(A[i] - B[i])^{\,2} \tag{13}$$

If streams A and B above represent the original medical image file and its encryption, then PSNR is computed as:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{14}$$

where MAX is the maximum value in the stream. A lower PSNR value is desired for encrypted files since it indicates more resistance to attacks.

6. CONCLUSION

This study proposed a modified algorithm for secured medical images in a cloud environment using medical image dataset that will be acquired online from medical images standard form called DICOM (digital imaging and communications in medicine) and will be passed into the system for compression. It is expected to establish the fact that DWT-MPSO technique can be used to achieve improve security, robustness, and quality of the watermarked images.

7. REFERENCES

[1] M. Mbarek, K. Ali, O. Hassan (2018). A Framework to Secure Medical Image Storage in Cloud Computing Environment. Journal of Electronic Commerce in Organizations Volume 16 Issue 1. DOI: 10.4018/JECO.2018010101.

[2] K. Sefer, A.J. Abdulrahman (2018). Cloud System for Encryption and Authentication Medical Images. IOSR Journal of Computer Engineering (IOSR-JCE) Volume 20, Issue 1, Ver. II , pp.65-75.

[3] K.K. Qusay, Y. Robiah, S.M. Hamid, S. A. Sayed, R.S. Siti (2017). A Review Study on Cloud Computing Issues. IOP Conf. Series: Journal of Physics: Conf. Series 1018 (2018) 012006

[4] S.G. Shini, T.Tony, K.Chithraranjan (2012). Cloud Based Medical Image Exchange-Security Challenges. Procedia Engineering vol. 38, PP 3454 – 3461.

[5] W. Botta, W Donato, V. Persico, A. Pescapé (2016). Integration of cloud computing and internet of things: a survey. Futur. Gener. Comput. Syst., vol. 56, pp. 684–700.

[6] U. Mustafa (2011). "Medical image security and EPR hiding using Shamir's secret sharing scheme," The Journal of Systems and Software, 84(3) pp.341-353.

[7] C.B. Nyeem, (2013). Review of medical image watermarking requirements for teleradiology. Journal of Digital Imaging, vol. 26, pp 326 – 343.

[8] O.D. Alowolodu, G.K Adelaja, B.K. Alese, O.C. Olayemi, (2018). Medical image security using quantum cryptography. Issues in Informing Science and Information Technology, vol. 15, pp. 57-67.

[9] K. Smita, V. Bellamkonda, Rajasthan (2018). Selective medical image watermarking and encryption for image security, International Journal of Pure and Applied Mathematics Volume 118 No. 14.

[10] S. S. Askar, A.A. Karawia, A. Al-Khedhairi, F. S. Al-Ammar (2019). An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps. Entropy, VOL. 21, 44

[11] M.I.Khalil (2017). Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain. I. J. Computer Network and Information Security, vol. 2, pp. 22- 28

[12] S.A Parah, J.A.Sheikh, F. Ahad, (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl vol. 76, pp. 10599–1

[13] S. Mallat (2008). *A Wavelet Tour of Signal Processing, Third Edition: The Sparse Way*, 3rd edn. (Academic Press, Philadelphia, PA, USA, 2008).

[14] M. Vetterli, C. Herley (1992). Wavelets and filter banks: theory and design. *IEEE Trans. Signal Process.* 40(9): 2207–2232.

[15] P. Surekha, S. Sumathi (2012) Performance comparison of optimization techniques on robust digital-image watermarking, Against Attacks, *Applied Artificial Intelligence: An International Journal.* 26(7): 615-644.

[16] P. Agrawal, A . Khurshid (2014). DWT and GA-PSO based novel watermarking for videos using audio watermark. In *International Conference in Swarm Intelligence* (pp. 212-220). Springer, Cham.