A New Wavelet Based Steganography Method for Securing Medical Data

Aminata Ngom[1(✉)], Sidoine Djimnaibeye[1], Ndeye Fatou Ngom[2], Samba Sidibé[2], and Oumar Niang[2]

[1] Laboratoire LACGAA, Université Cheikh Anta Diop de Dakar, Dakar, Senegal
myangoma@gmail.com
[2] Laboratoire LTISI, Ecole Polytechnique de Thies, Thiés , Senegal

Abstract. The transmission of confidential information over an open communication channel is susceptible to many threats like copyright infringement, eavesdropping and hacking. In this paper, we propose a solution combining data encryption techniques and multiscale signal analysis for securing patients' confidential data. Discrete Wavelet Transform (DWT) is first applied to an ECG signal. The confidential patient information and the electrocardiogram (ECG) signal are then encrypted with the Advanced Encryption Standard (AES) method. Finally, the output of the encryption is hidden in an image to form the stego image and transferred to a medical server. While cryptography ensures the confidentiality of the data modified by the encryption process, steganography enhance the security. The evaluation of the proposed system was performed with real data and quantitative parameters such as Percent Residual Difference (PRD), Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). The experimental results show the proposed scheme has a good encryption effect and a strong ability to resist detection compared with the existing methods.

Keywords: Wavelet transform · ECG · Steganography · Cryptography · Image processing

1 Introduction

With the advent of telecare medical information systems, data exchanges over insecure support such as the internet become frequent. The security of personal information is one of the most important factors to ensure when it needs to be transmitted between two parties over an unsecured channel. Existing solutions includes cryptography and steganography [9,16]. Cryptography scrambles the information while steganography conceals the existence of the information in another medium so that the secret information is imperceptible. To address the challenges of transmitting users' personal data in the medical domain, data related to the diagnosis of the patients can be integrated in biometric supports such as electrocardiogram (ECG) signals [8,14,22]. To protect personal data, several solutions based on cryptography, watermarking and steganography have been proposed [17,20,23]. In watermarking, the secret information is hidden in the host signal by an encryption process using the confidential key and the new signal called

A. D. Mambo et al. (Eds.): InterSol 2022, LNICST 449, pp. 132–143, 2022.
https://doi.org/10.1007/978-3-031-23116-2_10

stego is sent to the receiver via the Internet. The receiver extracts the secret information from the signal by a decoding process using the same secret key. In steganography, the original information is hidden in another cover (images, video, and audio) and forms the embedded message. The embedded message is transmitted to the authorized person via the internet and the latter extracts the real information from the alternative cover. *Ibaida et al.* [14] proposed a steganography algorithm to hide patient information inside ECG signal with five-level wavelet decomposition. They used a scrambling matrix to find the correct embedding sequence with the user-defined key before determining steganography levels for each subband by experimental methods. *Priya and Suganya* [19] made a survey on various steganography methods, in which patient details and diagnosis reports are embedded into ECG signals. They observed that transform domain was mostly used since the spatial domain is prone to attacks such as noise or lossy compression attacks and it may be easily modified by the third party. Recently, several solutions with satisfying results based on information hiding and wavelets transform have been proposed [17,23]. Hybrid methods encrypt confidential information and then hide the encryption data in an image to increase the security level. Among these methods, we have the medical image steganography scheme using individual and double pixel's allocation scheme, three random function and Bit Invert System (BIS) proposed by *Hashim et al.* [10]. *Hureib and Gutup* proposed a method combining elliptic curve cryptography with Image steganography [12]. Recently, a bit mask oriented genetic algorithm based secure medical data transmission mechanism is proposed by *Hari Mohan Pandey* [16].

In this paper, we propose a new data exchange method that combines cryptography and stenography. The proposed approach uses the frequency domain through the discrete wavelet transform (DWT) and the least significant bit based steganography method. Beyond the fact that our solution protects the signal thanks to the DWT method, we have added an AES encryption on the DWT signal and the patient's personal data to make the solution more robust. We have hidden information in an image that will be sent to the medical server. This allows us to make the message sent over the network imperceptible. While cryptography ensures the confidentiality of the data modified by the encryption process, DWT compression ensures a good reconstruction of the ECG signal and steganography ensures imperceptibility of the information sent over the network. To reinforce the security of our proposal, we assume that a mutual authentication protocol [24] between the different users of the medical system (medical staff and patients) is set up. This protocol will allow to have a session key which will be used in our architecture as AES encryption key. We evaluate the effectiveness of the proposed solution for real data and quantitative parameters such as Percent Residual Difference (PRD), Mean Squared Error (MSE), and Peak Signal to Noise Ratio (PSNR). Comparative analysis and experimental results show the proposed scheme has an efficient encryption effect and a strong ability to resist detection.

The rest of the paper is organized as follows. Section 2 presents the proposed methodology. Section 3 presents the experimental results and the performance analysis. Section 4 draw concluding remarks and future scopes.

2 Methodology

In this the section, we highlight our contribution, present the proposed framework, describe the DWT algorithm and present the encryption technique.

2.1 Contribution

Several solutions based on cryptography and stenography have been proposed for securing data [4,11,13]. Most of them propose methods that directly apply the coding of the patient's personal information on the support (signal, image, etc.). In this paper, the proposed solution is different because the signal is first compressed using discrete wavelet method before applying encryption and stenography operations. We assume that a mutual authentication protocol between the server and the personal device is set up [24]. This protocol will allow generation of a session key that will be used to encrypt patient personal data. We also take a cover image and apply AES (Advanced Encryption Standard (AES)) encryption to the original signal and the patient's personal data for added security. The steps proposed in [20] were used for preprocessing operation and wavelet coding coefficients. After applying the different steps, we obtain as output the DWT compression of the ECG signal and the patient's personal data that have not yet been transformed. At this level, we use two elements: AES encryption and a cover image. The compressed signal and the patient data are first grouped and encrypted. Then, the LSB (Least Significant Bit) method is used to hide the already encrypted signal and the patient's personal data in an image that will be sent to the medical server (Fig. 2). To obtain information on the patient, the doctor will have to retrieve the stego image (from the server), apply the LSB method to obtain the encrypted personal data of the patient and the compressed ECG signal (DWT). He will then have to decrypt the result obtained (AES) and finally decompress the ECG signal to finally gather all the elements necessary for his consultation (Fig. 3).

2.2 Proposed Framework

The proposed framework first collects the patient's ECG signals using various body sensors. The signals are then sent to the smartphone via Bluetooth, on which the patient's confidential data is stored. Then, on the smartphone, the signals are firstly decomposed using the Discrete Wavelet Transform (DWT), and the AES encryption is applied to the discrete wavelet transformed signal and to the patient's personal data. And finally the output of the AES encryption is encoded into the cover image using the LSB (Least Significant Bit) method and returns the stego image. The LSB method is applied to the stego image to obtain the encrypted information (DWT signal and the patient's personal data). The encrypted information is recovered and decrypted to get the patient's personal data and the DWT signals. Inverse of the DWT (IWT) is applied to the signals to recover the original signals.

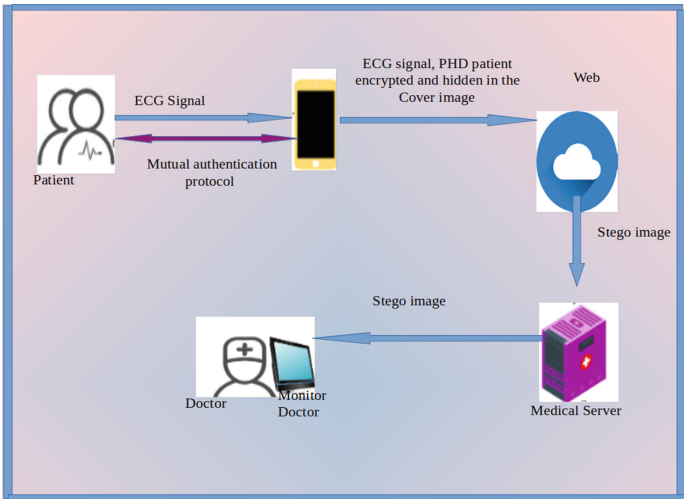


Fig. 1. Workflow

Figure 1 summarizes the different phases of data exchange on the network. The first step corresponds to the sending of the patient's data to the medical server and the second step corresponds to the exchange between the medical staff.

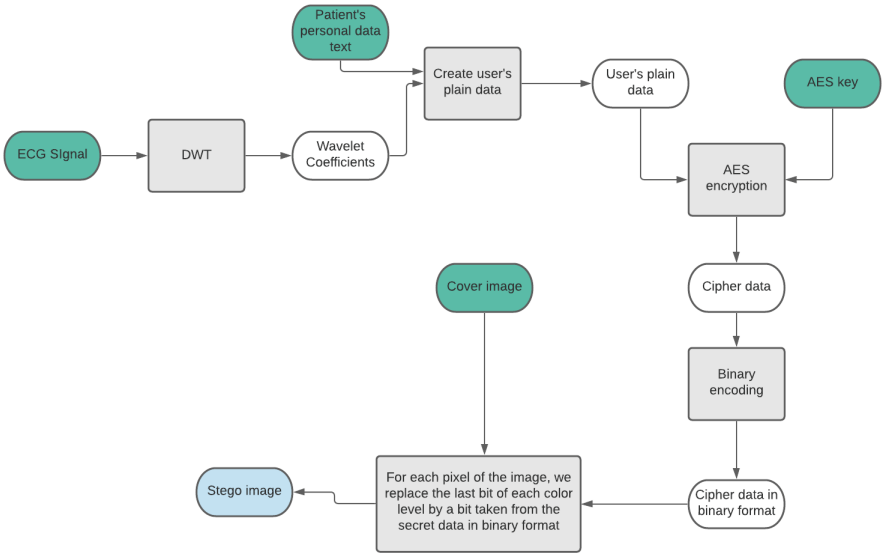


Fig. 2. Block diagram of sender stenography

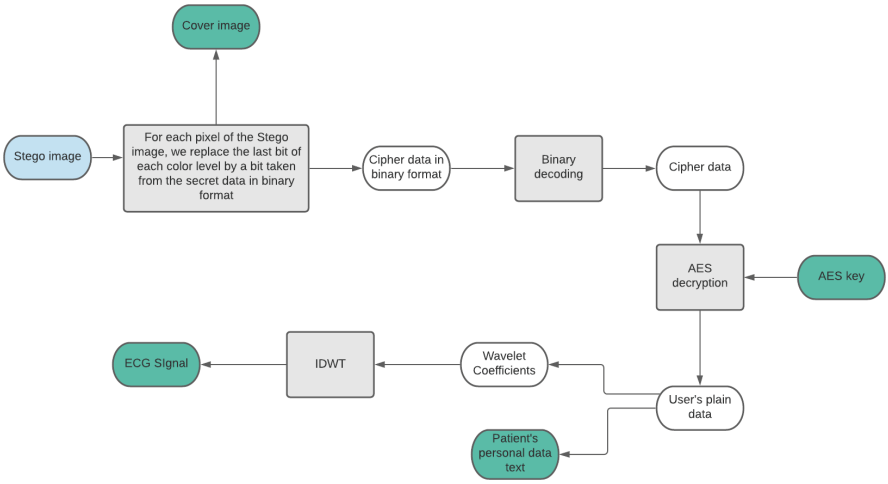


Fig. 3. Block diagram of receiver Stenography

Figure 2 summarizes transformation steps performed on the ECG signal and the patient's personal data (encryption, cover image) from a data collection (at the sensor) to storage (at the medical server). Figure 3 is the reverse process of Fig. 2. This step retrieves the initial ECG signal information and patient personal data that has been encrypted and hidden in a cover image.

2.3 Signal Transformation

In this section, we follow the steps described in [20] to perform preprocessing operations and the coding of the wavelet coefficients. Then, we use the LSB method to hide the encryption of the ECG and the user's personal data to obtain the stego image.

The prepocessing step aims to improve data quality before computing the discrete wavelet coefficient. If x_i is the ECG signal, then the signal y_i generated after normalization, mean removal and zero padding is described by the following equation:

$$yi = [zeros(1, M)(\frac{x_i}{A_m}) - m_x zeros(1, M)] \tag{1}$$

where $zeros(1, M)$ represent a row vector of M zeros, A_m is the maximum value of the original signal, and m_x is the mean of the signal which is normalized. Zero padding reduces the reconstruction error. Normalization and mean removal reduce the number of wavelet coefficients and make the magnitude of the largest coefficient less than one.

Discrete Wavelet Transform (DWT) like Fourier Transfrom (DFT) are method for converting an image from the spatial domain to the frequency domain. However, unlike the DFT which represents a signal in just frequency domain, the DWT can give simultaneous space and frequency representation. In continuous wavelet, the signal is

separated into scaled and translated versions $(\psi_{a,b}(t))$ of a single function $\psi(t)$ known as the mother wavelet [7]:

$$(\psi_{a,b}(t)) = \frac{1}{\sqrt{|a|}}\psi(\frac{t-b}{a}) \tag{2}$$

where a and b are the scale and translation parameters with $a, b \in \mathbb{R}$ and $a \neq 0$. The DWT uses a sampling with parameters a and b based on powers of two: $a = 2^j, b = k2^j$ with $j, k \in \mathbb{Z}$. DWT could be written as:

$$d_{j,k} = \int_{-\infty}^{\infty} s(t)2^{-\frac{j}{2}}\psi^*(2^{-j}t - k)d(t) = (s(t), \psi_{j,k}(t)) \tag{3}$$

The ECG signal is decomposed by DWT up to the fifth levels. The decomposition of the signal is achieved by rotating the signal with a pair of high-pass and low-pass analysis filters to form Quadrature Mirror Filters (QMFs). The output of each filter is sampled by a factor of two. The scale wavelet coefficients are calculated by recursively applying a low-pass signal sampled from the previous scale by a pair of analytical filters. The inverse transformation is obtained starting from the top layer, where the wavelet coefficients are over-sampled by a factor of two, and then filtered using a QMF composite pair. The determination of the decomposition band threshold is done by removing all coefficients lower than a threshold T. The thresholds are selected on the basis of Energy Packing Efficiency (EPE) defined as:

$$EPE_{Di} = \frac{\bar{E}_{CDI}}{E_{CDI}} \times 100 \tag{4}$$

where $\bar{E}_{CDI}$ is the total energy in the detail coefficients of level i after thresholding and E_{CDI} is the total energy in the detail coefficients of level i before threshold determination. The computation of a threshold based on a EPE, is done with the following steps:

1. compute the total energy in the wavelet coefficients X: $E = \sum X^2$,
2. compute the desired retained energy E' and the thresholded coefficients,
3. form the sequence $X_x[K]$ by sorting the magnitudes of the wavelet coefficients in descending order.

Coding the Wavelet Coefficients: The significant coefficients are grouped together in a separate file before being compressed using a variable-length code based on run-length encoding. The code uses 1 bit to identify the run type, 4 bits to represent the number of bits needed to code the run length and represents the binary equivalent of the run length. The header information consists of 64 bits. The first 20 bits are used to store the number of wavelet coefficients, the next bits are used to store the index value of the last significant coefficients, the next 12 bits are used to store the magnitude of the original signal, and the last 12 bits are used to store the mean of the normalized signal.

Least Significant Bit (LSB): LSB steganography is a technique in which least significant bit of pixel is replaced with secret data bits. It has the advantage to be easy to implement and give stego image that contain embedded data without major perceptible distortions. The pixels choice or the order of embedding capacity may be determined by a stego key. General operations of data hiding by using the LSB substitution method are described in [6]. Let C be the original 8-bit grayscale cover-image of $M_c \times N_c$ pixels represented as:

$$C = (x_{ij}|0 < i < M_c < j < N_c, x_{ij} \in (0, 1, ..., 255)) \tag{5}$$

Suppose that the n-bit secret message M is to be embedded into the k LSBs of the cover-image C. Firstly, the secret message M is rearranged to form a conceptually k_bit virtual image M represented as:

$$M' = (m'_i|0 < i < n', m'_i \in (0, 1, ..., 2^k - 1)), \tag{6}$$

where $n' < M_c \times N_c$. The mapping between the $n - bit$ secret message $M = m_i$ and the embedded message. $M' = m'_i$ can be defined as follows:

$$m'_i = \sum_{j=0}^{k-1} m_i \times k + j \times 2^{k-1-j} \tag{7}$$

A subset of n pixels $(x_{li1}, x_{li2}, ...x_{ln'})$ is selected from cover-image C in a predefined sequence. The embedding process is completed by replacing the k LSBs of x_{li} by m'_i. The pixel value x_{li} of the chosen pixel for storing the $k - bit$ message m'_i is modified to form the stego-pixel x'_{li} as follows:

$$x'_{li} = x_{li} - x_{li} mod 2^k + m'_i \tag{8}$$

In the extraction process, given the stego-image S, the embedded messages can be readily extracted without referring to the original cover-image. Using the same sequence as in the embedding process, the set of pixels $(x'_{li1}, x'_{li2}, ...x'_{ln'})$ storing the secret message bits are selected from the stego-image. The k LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. The embedded message bits m'_i can be recovered by:

$$m'_i = x'_{li} mod 2^k \tag{9}$$

2.4 Data Encryption

Asymmetric cryptography is an encryption algorithm that uses the concept of a key pair. Thus, in asymmetric cryptography, encryption and decryption are performed with different keys. In contrast, symmetric cryptography is an encryption algorithm in which encryption and decryption are performed with the shared key. This shared key is calculated by each party through a mutual authentication and key exchange protocol. *Abd Elminaam and al.* presents a performance evaluation of some symmetric encryption algorithms: AES, DES, 3DES, RC6, Blowfish and RC2 [2]. Following the analysis of the experimental results, they conclude that AES is faster and more resource-efficient.

AES [3] is symmetric-key block encryption with 128, 192 or even 256 bit keys. AES comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (Fig. 4). AES performs all its computations on bytes rather than bits and treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

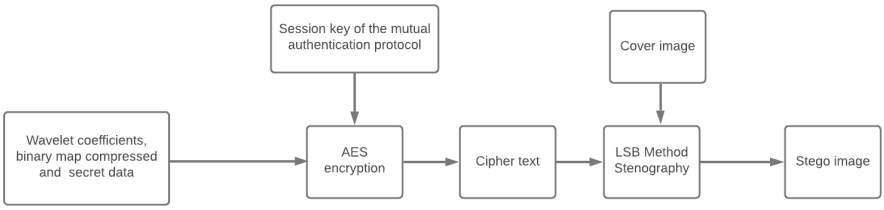


Fig. 4. AES encryption method

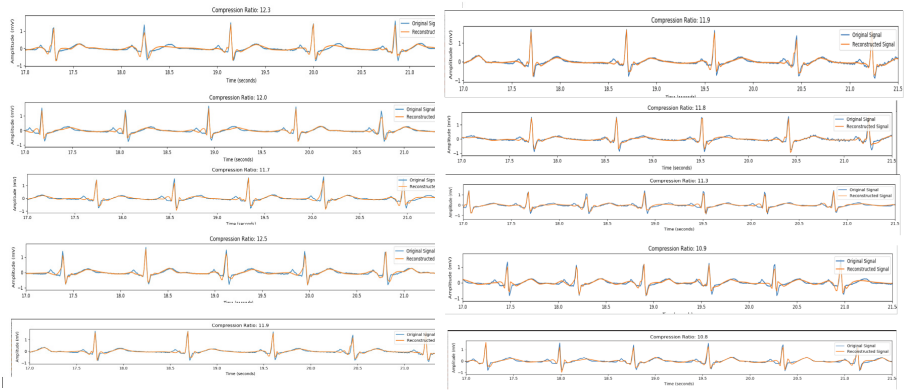
3 Performance Measure and Experimental Results

3.1 Data Considered

In this work, we used data from the physioNet apnea-ECG database [1,18]. The data consist of records varying in length from slightly less than 7 h to nearly 10 h each. The study also considers AES-128 encryption and cover image of size $384 \times 800 \times 3$.

3.2 Assessing the Multiscale Analysis Quality

The compression algorithm was tested on 10 records from the MIT-BIH arrhythmia database. The PSNR (Peak Signal to Noise Ratio), PRD (Percent Residual Difference), and (mean squared error) are used as quantitative performance measures. The results were obtained by first encoding and decoding the real signal file and the compressed signal file (DWT). Figure 5a and 5b give illustrations of the results obtained. We can observe on Fig. 5a the results of the first 5 signals obtained before and after the compression of the signal. We can notice that the PRD varies from 12.3, 12, 11.7, 12.5, 11.9. Figure 5b represents the results of the last 5 signals before and after the compression, and we can observe a variation of the PRD of 11.9, 11.8, 11.3, 10.9, 10.8. The compressed signal is recovered with the personal data of the patient to be encrypted and encoded again in an cover image to form the stego image.



(a) Original and reconstructed signal with 5 first normal ECG samples

(b) Original and reconstructed signal with 5 second normal ECG samples

Fig. 5. Original and reconstructed signal with 10 normal ECG samples

3.3 Assessing Effects of the Encryption Process

Comparing stego images with cover image results requires measuring image quality. To evaluate the proposed model, the performance of the proposed technique is measured by using Peak Signal to Noise Ratio (PSNR), Percent Residual Difference (PRD), and the Mean Squarred Error (MSE). PSNR provides information about signal and noise levels. It is a good measure to compare restoration results for the same image. If the image has a high PSNR, it means that the received signal has little interference effect and is therefore faithfully restored. PSNR value shows the peak signal to noise ratio of the original signal and stego image. PSNR is defined as:

$$PSNR = 10 \times log(\frac{P^2}{MSE}) \tag{10}$$

where $P = max(C(i,j), S(i,j))$ is the peak signal value of the cover-image. MSE is the cumulative squared error between the compressed and original image, while PSNR is a measure of the maximum error. A low MSE value corresponds to a low error. MSE is the mean pixel-by-pixel squared difference between the cover image and the hidden image. MSE is defined as:

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} [C(i,j) - S(i,j)]^2 \tag{11}$$

where x_i is the original signal obtained from the ECG record, y_i is the reconstructed signal ,and N denotes the number of bits in the input signal [5]. Where, M and N are the rows and columns of the cover image respectively, and $C(i,j)$ and $S(i,j)$ mean the pixel value at position (i,j) in the cover image and the corresponding stego-image,

respectively. The distortion between original signal and reconstructed signal is measured by the PRD. PRD is defined through Eq. 12 as follows:

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N}(x_i)^2}} \tag{12}$$

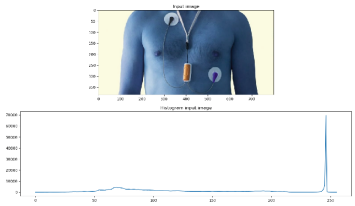
Table 1 shows the results of the performance of the system by using PRD, MSE and PSNR values for 10 normal ECG. We evaluated the quality of the signal recovered with the PRD and the quality of the image obtained with the PSNR. According to the analysis of *Nemcová et al.* [15], a PRD between [0–4.33] is an excellent result, a PRD between [4.33–7.8] is a very good result, a PRD between [7.8–11.59] is a good result. We can see in Table 1 that our PRD is between [0.11–0.13] where it was observed that the PRD value of Bashar A Rajoub proposal produced 1.06%. We can therefore conclude that we have a satisfactory result of signal compression.

Table 1. Performance analysis

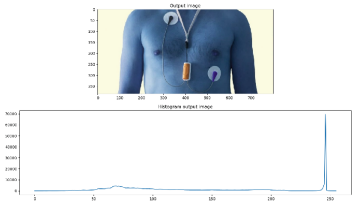
Sample No	PRD %	MSE (db)	PSNR (db)
1	0.13	0.29	53.53
2	0;12	0.30	53.51
3	0.11	0.29	53.48
4	0.12	0.29	53.45
5	0.11	0.30	53.40
6	0.12	0.30	53.40
7	0.11	0.30	53.28
8	0.11	0.30	53.33
9	0.11	0.30	53.31
10	0.12	0.30	53.40

The signal to noise ratio (PSNR) is a measure of the fidelity of a stego image. PSNR is the estimation of the degree of distortion caused in the stego image compared to the original cover image. *Ratnakirti et al.* [21] classified the visual fidelity scale into three groups. For a value of PSNR < 40, the fidelity is low. If $40 < PSNR < 60$, the fidelity is medium. And finally if $PSNR > 60$, then the fidelity is high. For our architecture we have satisfactory results since our PSNR > 50 db.

One significant requirement to certify the security of the encryption method is that a slight change in a plain image should result in a noticeable change in the cipher image. To observe the impact of the encoding on the image we displayed the histogram of the cover image before the encoding process (Fig. 6a) and the histogram of the image (stego) after the encoding process (Fig. 6b) and compared the results of the two histograms before and after the encoding. And we have satisfactory results since there is no remarkable difference between the two images and the two histograms.



(a) Input image and Histogram of input image



(b) Output image and Histogram of output image

Fig. 6. Output image before and after the encoding process

4 Conclusion

This paper proposes a transmission system based on a combination of encryption approaches (cryptography, steganography) and multiscale signal analysis techniques. The experimental results show the proposed scheme has a good encryption effect and confirmed its performance and its efficiency compared with the existing methods. Future research will focus on using machine learning techniques to choose the region of interest for embedding patients' information and network analysis as an optimization mechanism to secure image information through canal transmission. Another challenge will be using blockchain to better secure data transmission.

References

1. Apnea-ECG Database. www.physionet.org/content/apnea-ecg/1.0.0/. Accessed 9 Nov 2021
2. Abd Elminaam, D.S., Abdual-Kader, H.M., Hadhoud, M.M.: Evaluating the performance of symmetric encryption algorithms. Int. J. Netw. Secur. **10**(3), 216–222 (2010)
3. Abdullah, A.: Advanced encryption standard (AES) algorithm to encrypt and decrypt data, June 2017
4. Abdur Razzaq, M., Shaikh, R., Adnan, M., Ahmed, A.: Digital image security: fusion of encryption, steganography and watermarking. Int. J. Adv. Comput. Sci. Appl. **8** (2007). https://doi.org/10.14569/IJACSA.2017.080528
5. Bhardwaj, R., Sharma, V.: Image steganography based on complemented message and inverted bit LSB substitution. Procedia Comput. Sci. **93**, 832–838 (2016). https://doi.org/10.1016/j.procs.2016.07.245, www.sciencedirect.com/science/article/pii/S1877050916314879
6. Chan, C.K., Cheng, L.: Hiding data in images by simple LSB substitution. Pattern Recogn. **37**, 469–474 (2004). https://doi.org/10.1016/j.patcog.2003.08.007
7. jin Chen, D., Wan, S., Xiang, J., Bao, F.S.: A high-performance seizure detection algorithm based on discrete wavelet transform (DWT) and EEG. PLoS ONE **12**, e0173138 (2017)
8. Cheng, L.T., Yang, C.Y.: High performance electrocardiogram steganography based on fast discrete cosine transform. Int. J. Inf. Control Comput. Sci. **11**(7) (2018). https://doi.org/10.5281/zenodo.1317262
9. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A.: Secure medical data transmission model for IoT-based healthcare systems. IEEE Access **6**, 20596–20608 (2018). https://doi.org/10.1109/ACCESS.2018.2817615

10. Hashim, M., Taha, M.S., Aman, A.H.M., Hashim, A.H.A., Rahim, M.S.M., Islam, S.: Securing medical data transmission systems based on integrating algorithm of encryption and steganography. In: 2019 7th International Conference on Mechatronics Engineering (ICOM), pp. 1–6. IEEE (2019)
11. Hashim, M., Taha, M., Aman, A., Hashim, A., Rahim, M., Islam, S.: Securing medical data transmission systems based on integrating algorithm of encryption and steganography. In: 2019 7th International Conference on Mechatronics Engineering (ICOM), pp. 1–6, October 2019. https://doi.org/10.1109/ICOM47790.2019.8952061
12. Hureib, E., Gutub, A.A.: Enhancing medical data security via combining elliptic curve cryptography and image steganography. Int. J. Comput. Sci. Netw. Secur. **20**(8), 1–8 (2020)
13. Hureib, E., Gutub, A.: Enhancing medical data security via combining elliptic curve cryptography and image steganography, Vol. 20, pp. 1–8 , August 2020
14. Ibaida, A., Khalil, I.: Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE Trans. Bio-med. Eng. **60** (2013). https://doi.org/10.1109/TBME.2013.2264539
15. Nemcová, A., Smisek, R., Maršánová, L., Smital, L., Vitek, M.: A comparative analysis of methods for evaluation of ECG signal quality after compression. BioMed Res. Int. **2018** (2018). https://doi.org/10.1155/2018/1868519
16. Pandey, H.: Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Fut. Gene. Comput. Sys. **111** (2020). https://doi.org/10.1016/j.future.2020.04.034
17. Pawar, K., Naiknaware, D.: AES encrypted wavelet based ECG steganography. Int. J. Eng. Tech. **4** (2018)
18. Penzel, T., Moody, G., Mark, R., Goldberger, A., Peter, J.: The apnea-ECG database. In: Proceedings of Conference Computers in Cardiology 2000, vol. 27, pp. 255–258 (2000). https://doi.org/10.1109/CIC.2000.898505
19. Priya, J., Suganya, R.: Steganography techniques for ECG signals: a survey. In: 2016 11th International Conference on Industrial and Information Systems (ICIIS), pp. 269–273 (2016). https://doi.org/10.1109/ICIINFS.2016.8262949
20. Rajoub, B.: An efficient coding algorithm for the compression of ECG signals using the wavelet transform. IEEE Trans. Bio-med. Eng. **49**, 355–362 (2002). https://doi.org/10.1109/10.991163
21. Roy, R., Changder, S.: Quality evaluation of image steganography techniques: a heuristics based approach. Int. J. Secur. Appl. **10**, 179–196 (2016)
22. Edward Jero, S., Ramu, P., Ramakrishnan, S.: Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. J. Med. Syst. **38**(10), 1–11 (2014). https://doi.org/10.1007/s10916-014-0132-z
23. Santiago, A.M., et al.: Lightweight security hardware architecture using dwt and AES algorithms. IEICE Trans. Inf. Syst. **E101.D**(11), 2754–2761 (2018). https://doi.org/10.1587/transinf.2018EDP7174
24. Zhang, Y., Xie, K., Ruan, O.: An improved and efficient mutual authentication scheme for session initiation protocol. PLoS ONE **14**, e0213688 (2019). https://doi.org/10.1371/journal.pone.0213688