DOI: 10.21917/ijct.2018.0270

SECURE TRANSMISSION OF BIO-MEDICAL DATA USING STEGANOGRAPHY

S. Thenmozhi, P. Sureka and Ramgopal Segu
Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, India

Abstract

To transmit secret data over the internet, the information should be sent in a way attacker finds it difficult to read the secret data. In this paper patient's secret information is hidden in the bio-medical signal like ECG/EEG/PPG. The transmitted information generally contains (1) biomedical-signals (2) patient data. Main concerns include privacy and authenticity of the data being transmitted. A secret key is used which is known to sender and receiver. This paper introduces a novel steganography technique that guarantees (1) protection of private data utilizing a key and (2) originality of the bio-medical-signals. To maximize embedding, Fast-Walsh-Hadamard Transform is used to convert the signals into a set of coefficients. The proposed technique can be applied on three bio-medical signals like ECG/EEG/PPG unlike any other technique which uses only one bio-medical signal. To achieve least distortion, coefficients of least significant bit is considered. The algorithm has less impact on the bio-medical signal and the signal at the transmitting side can be recovered with less distortion.

Keywords:

Steganography, Bio-Medical Signal, Arduino Uno Board, Pulse Sensor, Temperature Sensor, BP Sensor

1. INTRODUCTION

In public health-care scheme, physical presence of the patient is required to monitor, which is not appropriate for the current generation for various reasons like crowding of patients in the hospitals and shortage of expertize in rural areas. Thus, a new model so-called "Point-Of-Care" has emerged recently and monitors patient by gathering their samples for a short period of time with the help of Smart Sensor and the information is transmitted to the health authorities. The main interest is saving patient's lives and reducing the infrastructural cost in the hospitals.

In spite of distinct benefits, P-0-C has few threats related to security such as, (1) its availability in isolated areas (2) making use of public web for transmitting highly sensitive patient's data. However, few countries like US and Australia have set strict rules on clinics commanding protection of patient's data from illegal access specially while performing 0ff-site work by health authorities. However, there is few concerns from (1) patients point-of-view is protection of their private data and (2) legitimacy of the samples transmitted and result of doctor decision (whether doctors' decision is valid for specific sample transferred). Primary concern from Health-Care viewpoint is guarantying efficient and robust method that protects sensitive information of the patient.

Earlier Models which used to solve these problems where by applying classical cryptography. Even though having few convenient functionalities, they are not utilized in this domain as a result of:

- Mobile equipment used in POC are resource limited making it difficult to install classic cryptography approach due to overhanging, by performing mathematical procedures that assures high security.
- Making health authority's job difficult as the original samples are manipulated into cipher-text.

Homomorphic encryption method is used to solve these above issues. The advantage of homomorphic method over classical cryptography is cipher-text is utilized as it satisfies patients concern by guaranteeing end to end security and allowing health authorities for direct service to the web since the content is not revealed in both cases.

However, researchers are looking forward to solve threats faced by health authorities and patients: (1) ensuring end to end security for patients sensitive information that is transmitted like personal data (details, id), diagnosing data (glucose Level), biometric data (Fingerprint and Iris) along with authenticity of normal biomedical signal collected (EEG,ECG,PPG), (2) be suitable for existing POC capacity like memory, electricity consumption and bandwidth, and (3) to avoid delaying the performance of the doctors at health authorities.

Another technique called "steganography" is utilized to protect sensitive information along with secret key embedded within transmitted data and only legitimate users can access it. Advantages of steganography are (1) its performance requires lower power and memory, and (2) guaranties originality of the data without manipulating it.

2. RELATED WORK

A thorough study of several papers based on the problem statement was done in order to understand the merits and demerits of steganography in bio-medical field.

In [1], an effort is made to use curvelet transform which allows identifying the important coefficients that store crucial data about diagnoses. To achieve less degradation, the coefficients around the value zero are modified while embedding the patient data. To avoid the overlapping of the watermark, ($n \times n$) sequence is used for embedding the patient data. Their main goal of the proposed method is to preserve the diagnosability while minimizing the signal degradation. They analyzed the effect of modifying the coefficients at three levels are: near zero, minimum, maximum of the cover bio-medical signal. Based on studying their three different levels, for better result, the coefficients around zero are modified. Authors in this paper have proposed ECG steganography where, ECG is taken as a cover medium. 1D ECG is converted into a 2D image using Discrete Curvelet transform. Discrete Curvelet transform is applied to the cover and patient data is converted into a binary format which is embedded in ECG signal using LSB embedding. Authors have evaluated on peak signal to noise ratio (PSNR) (range from 43 - 75), percentage residual difference (PRD) (range from 0.0018 - 0.0132) and Kull Back Leibler distance (KL) (range from 0.0018 - 2.94). The

proposed approach doesn't affect diagnosability which is measured using Kull Back-Leibler divergence (KL) and allows reliable steganography and the proposed algorithm can be used in case for successful bio-medical steganography.

In [2], Authors have proposed Two Reversible Data Hiding (RDH) method. First method is by applying Conventional reversible data hiding, which gives high visual quality of ECG signal, and Huffman encrypted patient data is embedded into the ECG signal using local linear predictor (LLP). First method evaluates PRD (range from 0.018 - 1.7) and (BPS) bits/sample (range from 0.05 - 0.45). And second method, a unified embedding-scrambling Reversible Data Hiding (RDH) along with local linear predictor (LLP) as predictor is used to embed patient data in ECG signal. Second method evaluates PRD (range from $1.16e^{+03}$ - 930.20) and (BPS) bits/sample (range from (7.4 - 8.3). This paper assures perfect restoration of patient data and ECG signal at the extracting side. Security of both ECG signal and patient data is guaranteed by embedding scrambling. First method using Conventional reversible data hiding guarantees distortion to be equal to 1%. And second method using unified embedding-scrambling Reversible Data Hiding (RDH) guarantees, high embedding capacity of 7.8 bits/sample where ECG signal quality is not a concern. Result shows both the methods are reversible making it suitable for real-time.

In [3], Authors have proposed DCT (discrete-cosine-transform) to achieve minimum distortion. ECG signal is decomposed using DCT (discrete-cosine-transform) and patient's data is converted in binary form. Converted patient data is embedded in ECG signal using LSB technique. To secure the information that is transmitted through the public network, the proposed technique provides an effective way to secure the data transmitted. Using matlab GUI, authors claim ECG has less distortion and it can be used for diagnoses.

In [4], authors propose encoding system that assures privacy and security to 1D bio-medical signal. The proposed 1D SPIHT (set partitioning in hierarchical trees) method compresses 1D signal, to avoid distortion the data is embedded in compressed domain. The proposed method is tested using two bio-medical signals from the standard database for ECG and EEG. SPHIT architecture can be extended to higher dimension for the bio-medical signal, as encoding relies on SPHIT algorithm. Set partitioning in hierarchical trees (SPHIT) is applied to ECG/EEG signals and AES encrypted patient data is embedded in ECG/EEG signal by hash function. This paper focuses on achieving security and efficiency. This has higher embedding capacity within the bio-medical signal (3kB-resting ECG, 200kB-stress tests, 30MB-ambulatory ECG) and encoder achieves a compression ratio of 3-real time to 5-offline operation. Results show high embedding capacity (up to 89%) and PRD (7-9).

In [5], integer to integer wavelet transform is applied to the ECG signal, for implementing an effective reversibility system, a transform is required for converting integer to integer. Since the result of the wavelet transform is a floating-point value. Patient data is encrypted using XOR cipher technique. Encrypted data is hidden in ECG using LSB technique. Experimental result shows that watermarking doesn't affect the signal quality. PRD of 0.4% is achieved which shows, PRD is low.

In [6], lifting wavelet transform is applied to the ECG signal, where the signal can be obtained in sub bands making it easy to embed in the required portion of the ECG signal. The message is encrypted using AES encryption. In this paper, LSB technique is used to embed the message bits into the ECG signal. Authors prove that the extracted signal can be used for diagnoses, since the PRD obtained is 0.5%.

In [7], here haar-wavelet-based on lifting scheme transform is applied to the ECG signal and patient data is encrypted using Arnold transform which is embedded into ECG signal using shifting operation. Using this method, high-degree of invisibility is achieved as, the watermark is embedded in high frequencies of Haar-wavelet transform which corresponds to non-QRS wave of the original signal. This paper proves originality of the ECG signal and efficiency. The result shows NRSME (0.092 - 0.192), capacity (up to 74kB).

In [8], DWT helps in providing security to the patient's information, as it makes use of encryption and scrambling methods. DWT is applied to the ECG signal and RSA encrypted patient data is embedded into the ECG signal using LSB technique. This paper provides security and privacy for transferring ECG signal and patient data. Outcome of this technique improves security and performance in health-care-systems and saves elderly patients live. Experimental results show PRD (up to 2.87×10^{-4}) and WWPRD (9.026×10^{-6}).

In [9], by applying integer-wavelet transform, the host-image component is mapped to the integer-wavelet coefficient. Considering high frequency-sub-band of transformed image, the watermark data is embedded in those sub-bands. Two thresholds (T_1, T_2) are selected according to capacity required for watermarking. And two-zero points (Z_1, Z_2) are required to shift beginning and end part of histogram. Histogram region that is located between the thresholds are not changed. Authors propose a 2D wavelet transform (DWT) which is applied to the medical image and binary watermarked-data is embedded into medical image by shifting method. The proposed method allows loss-less re-construction for the watermarked and the cover image. Considering the advantage of low distortion in high-frequency sub-bands and allowing center region unchanged in the histogram. Binary watermarked-data is inserted in locations of threshold and zero-points. Experiment result shows high PSNR (up to 58dB).

In [10], to secure the transmitted data which mainly consist of bio-medical signal and patient sensitive data, this paper introduces a steganography technique that assures privacy of the patient data, by concealing within the signal employing the secrete key. Fast Walsh Hadamard Transform is used to increase hiding. In this paper Fast Walsh-Hadamard Transform is applied to the any of the three bio-medical signals like ECG/EEG/PPG. The patient data is encrypted using AES encryption algorithm employing a secret key for secure transmission. AES encrypted patient data is embedded into the bio-medical signal using discrete-wavelet-transform (DWT) - Haar wavelet Transform. To increase hiding capacity, Fast Walsh–Hadamard transform is used to convert signals into a group of coefficients. To assure minimum distortion, only less important coefficient values are selected. To enhance security, key is employed in 3D coefficients, reform to yield a 3D order used in the processing of concealing. This paper assures to have high embedding-level by using the proposed Fast Walsh-Hadamard Transform, where the signal is obtained in the frequency domain coefficient. Experimental results of this paper

work show evaluation parameters for PRD for stego image (0.21 - 0.96) and the extracted signal (0.045 - 0.77).

In [11], the patent data is encrypted using the XOR ciphering mechanism which results in binary format. ECG signal is converted into detailed and approximation values by applying DWT. Encrypted patient data in binary form is embedded into ECG signal using LSB technique. Authors in this paper have calculated PRD which calculates the diagnosability and SNR. The range of PRD achieved in this paper for normal ECG signal (0.0167 - 0.02323) and extracted PRD (0.0167 - 0.2327). From experimental results it shows watermarked ECG can be used for diagnosis.

3. MATERIALS AND METHODS

3.1 FAST WALSH HADAMARD TRANSFORM (FWHT)

FWHT is considered because of its simplicity. Matrix of this transform can be adjusted according to our required application. Advantage of FWHT is, signal reconstruction can be accomplished just by using low-series coefficients. Other main advantage is its mathematical operations as it requires only addition and subtraction making it less complicated. Making it more useful in image or signal processing when compared to already existing transform like wavelet and Fourier. This transform requires much less power, storage and computation.

3.2 AES ENCRYPTION AND DECRYPTION

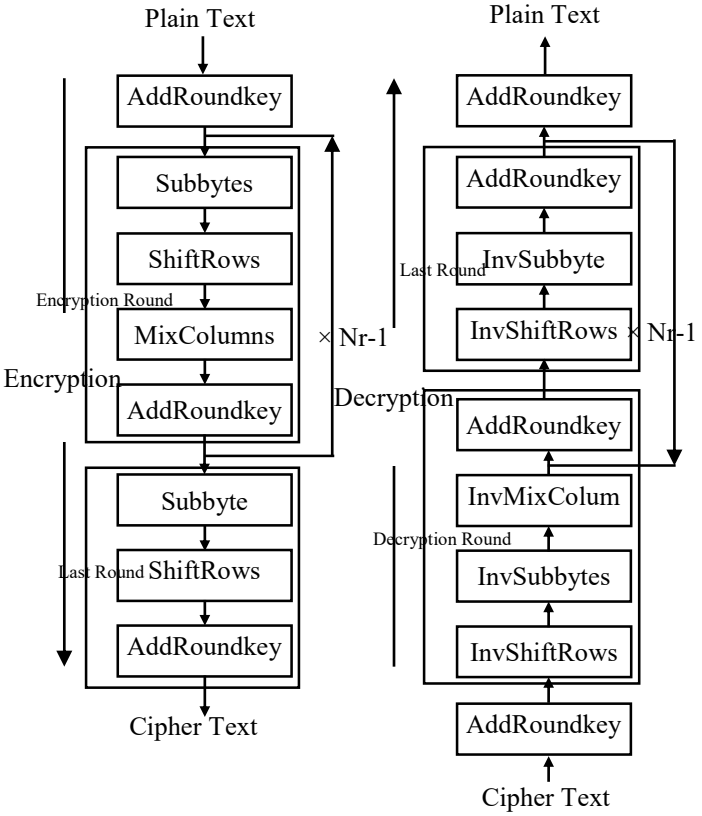

Fig.1. Overall Structure Of AES Algorithm

AES consist of the following steps:

- *Substitution bytes*: For performing a byte to byte substitution an s-box is used.
- *Shift rows*: Shift rows is a simple type of permutation.
- *Mix columns*: In mix columns the substitution uses an arithmetic of GF (8th power of 2)
- *D.ADD round key*: ADD round key is used as a XOR for the current block by using an expanded key. This structure is very simple for the process of encryption and decryption, the cipher starts by ADD round key.

3.3 EMBEDDING USING HAAR DWT

Signal is decomposed by applying 2 Level Haar DWT, first level Haar DWT gives approximation value (LL_1), and detail values (HL_1, LH_1, HH_1). 2nd level Haar DWT is applied on LL_1 (low series coefficients) which results in LL_2, HL_2, LH_2, HH_2. Embedding is done in LL_2 band. Haar transform is used to combine the inputs, passing the sum value and store the difference value.

4. PROPOSED METHODOLOGY

4.1 EMBEDDING PROCESS

The transmitted information mainly contains patient's data and the bio-medical signal. Patient data are manually entered such as name, ID, details, temperature, blood pressure, and glucose value.

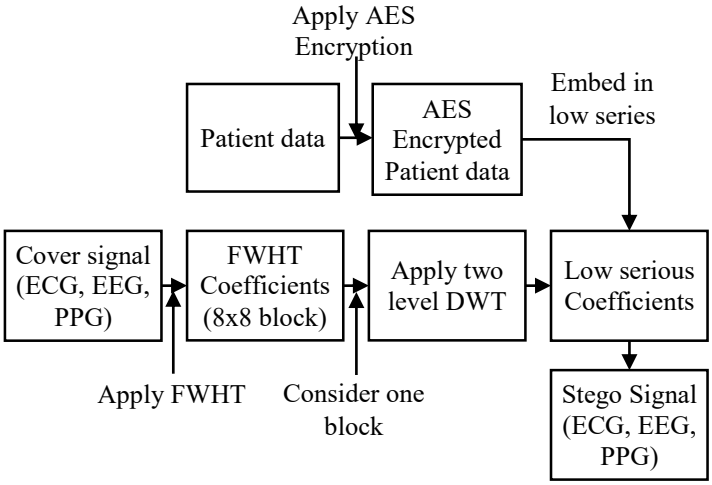

Fig.2. Embedding Block Diagram

4.1.1 AES Encryption:

Patient's data like name, ID, details along with diagnosis and biometric information is encrypted using the AES algorithm. And a secret key is used, which is known only to the authorised person such as the patient and the doctor. Here 16 byte secret key is utilised which is used in the encryption process. This secret key length will decide how many rounds to be performed in AES encryption process. Each byte is converted into its corresponding bits and these bits are again converted into its equivalent string which can be 0 or 1.

4.1.2 Applying FWHT on the Bio-Medical Signal:

The bio-medical signal can be ECG/EEG/PPG. FWHT is applied on any one of the signal, where the signal can be obtained in a set of coefficients. These coefficients can be divided into high and low series coefficients. Depending on the algorithm, any one of the coefficients can be selected to hide the patient's data. In this method, low series coefficients are used since it has a larger impact for reconstruction the bio-medical signal.

4.1.3 Embedding Using Haar DWT:

In this step, the obtained coefficients are considered in blocks of 8. Here 2 Level DWT is applied to the signal and the result obtained after the level 2 DWT is used for embedding. In embedding, energy value and signal value is calculated. Depending on the AES result obtained which is 0 or 1, these signal value and energy value is embedded into the signal. If string value is 0, then the energy value and signal value is embedded into the signal, if the string value is 1, the same signal is retained which is the obtained FWHT Signal. The same process is repeated for each value and the energy and signal values are embedded according to the patient's string data value which is 0 or 1. The result of this process results in a signal called stego signal.

4.2 EXTARCTION PROCESS

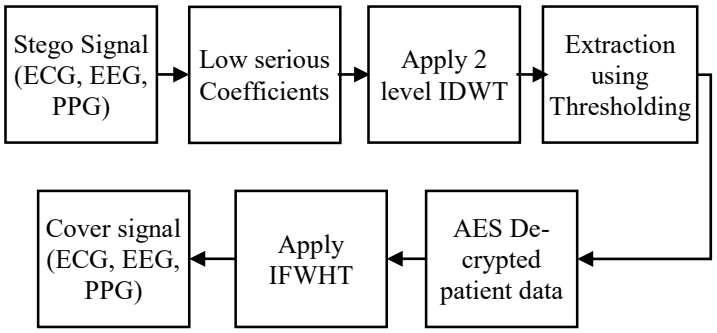

Fig.3. Extraction Block Diagram

4.2.1 Extraction Using Haar DWT:

Obtained stego signal is considered in blocks of 8. 2 Level IDWT is applied for each block which is the low series coefficient. In this stage patient data is decrypted using the threshold value. Threshold value from 0 to 10 is normally chosen. Threshold value of 5 is considered in this paper. If the obtained energy value and signal value is less than the threshold value 5, then the patient data is considered to be 1. If the energy value and signal value is greater than the threshold value 5, then the patient data is considered as 0. For each block of the signal the energy value and signal value is compared with the threshold of 5, to completely obtain the patient data.

4.2.2 Applying IFWHT:

The obtained stego signal is applied with IFWHT. To convert the signal from set of coefficients to its time domain. Hence original bio-medical signal is obtained by applying IFWHT.

4.2.3 AES Decryption:

AES decryption process will return the patient data which is name, identity, details and their diagnosis measure and biometric information. Same rounds of operation is performed as done in AES encryption which is 10 rounds in this paper.

5. PERFORMANCE ANALYSIS

5.1 ECG SIGNAL

The below Fig.4 shows original ECG signal, FWHT applied to ECG, stego ECG signal and retrieved ECG signal. It is clear from the Fig.4 that stego ECG and retrieved ECG signal is same as the original ECG signal and the signal can be reconstructed at the destination.

The quality or the reconstruction of the signal is calculated by PSNR and is found to be high. Signal can be used for diagnosis since the PRD of stego and extracted in minimum.

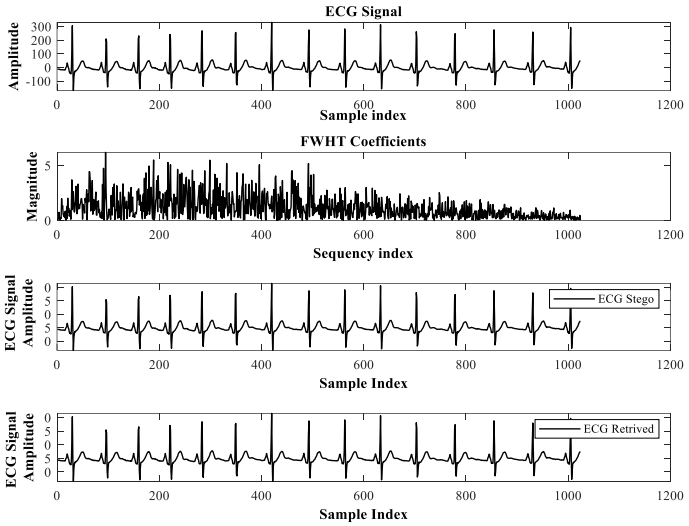

Fig.4. Simulation Result for ECG Signal

Table.1. PRD and PSNR of stego ECG signal for the proposed method

ECG sample No	PRD Stego	PSNR Stego
101	0.0569	655.13
102	0.0192	654.25
103	0.0611	657.46

From Table.1, PRD value for the proposed method is achieved to be low. PRD of stego ECG range from (0.0192 to 0.0611) and PSNR of stego ECG is found to be high.

Table.2. PRD and PSNR of extracted ECG signal for the proposed method

ECG sample No	PRD Extracted	PSNR Extracted
1	0.0569	655.13
2	0.0574	655.33
3	0.0407	657.46

From Table.2, PRD value for the proposed method is achieved to be low. PRD of extracted ECG range from (0.0407 to 0.0574) and PSNR of extracted ECG is found to be high.

Table.3. PRD of ECG signal in [11] using different wavelets

ECG sample No.	PRD Extracted Sym20	PRD Extracted Coif5	PRD Extracted db3	PRD Extracted Bior6.8
1	0.0931	0.0996	0.0988	0.0960
2	0.0167	0.0172	0.0175	0.0170
3	0.2111	0.2151	0.2327	0.2157

From Table.3, PRD of extracted ECG signal in [11] is found to be in the range of (0.0192 to 0.0611). Proving our algorithm achieves low PRD than [11].

5.2 EEG SIGNAL

The Fig.5 shows original EEG signal, FWHT applied to EEG, stego EEG signal and retrieved EEG signal. It is clear from the Fig.5 that stego EEG and retrieved EEG signal is same as the original EEG signal and the signal can be reconstructed at the destination.

The quality or the reconstruction of the signal is calculated by PSNR and is found to be infinity. Signal can be used for diagnosis since the PRD of stego and extracted in minimum.

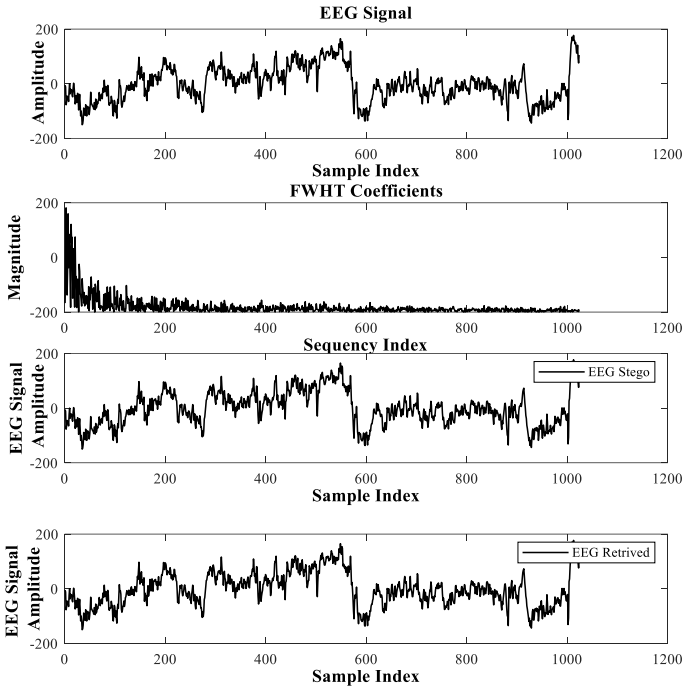

Fig.5. Simulation Result for EEG Signal

Table.4. PRD and PSNR of stego EEG signal for the proposed method

EEG Sample No.	PRD Stego	PSNR Stego
1	0.0025	Inf
2	0.0013	Inf
3	0.0021	Inf

From Table.4. PRD value for the proposed method is achieved to be low. PRD of stego EEG range from (0.0013 to 0.0025) and PSNR of stego EEG is found to be infinite.

Table.5. PRD and PSNR of extracted EEG signal for the proposed method

EEG Sample No.	PRD Extracted	PSNR Extracted
1	0.0016	Inf
2	0.0019	Inf
3	6.9456e-04	Inf

From Table.5, PRD value for the proposed method is achieved to be low. PRD of extracted EEG range from ($6.9456e^{-04}$ to 0.0016) and PSNR of extracted EEG is found to be infinite.

Table.6. PRD of EEG signal in [10]

EEG Sample No.	PRD stego	PRD Extracted
1	0.0257	0.1056
2	0.0477	0.1952
3	0.0933	0.4179

From Table.6, PRD of stego EEG in [10] is found to be in the range of (0.0257 to 0.0933) and PRD of extracted EEG range from (0.1056 to 4). Proving our algorithm achieves low PRD than [10].

5.3 PPG SIGNAL

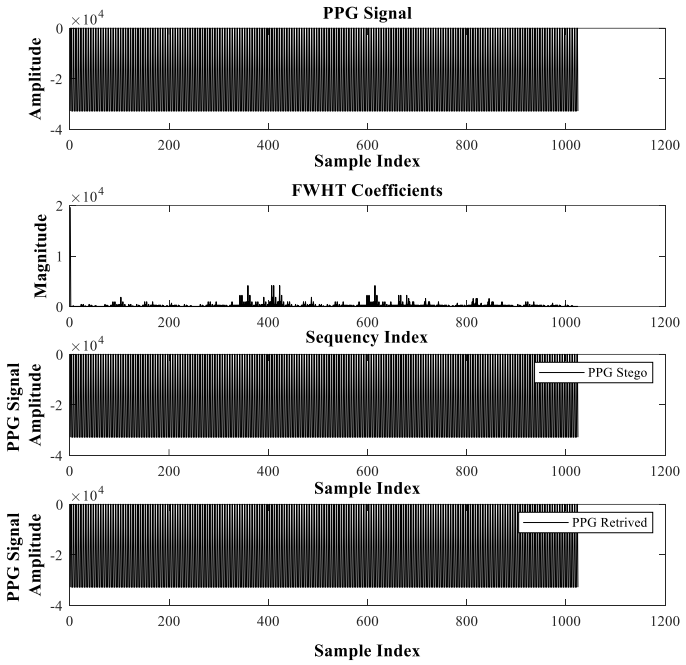

Fig.6. Simulation Result for PPG Signal

The Fig.6 shows original PPG signal, FWHT applied to PPG, stego PPG signal and retrieved PPG signal. From the Fig.6 we can say that stego PPG and retrieved PPG signal is same as the original PPG signal and the signal can be reconstructed at the destination.

The quality or the reconstruction of the signal is calculated by PSNR and is found to be infinity. Signal can be used for diagnosis since the PRD of stego and extracted in minimum.

Table.7. PRD and PSNR of stego PPG signal for the proposed method

PPG Sample No.	PRD Stego	PSNR Stego
1	8.6322e-05	Inf
2	0.0324	Inf
3	4.6735e-05	Inf

From Table.7. PRD value for the proposed method is achieved to be low. PRD of stego PPG range from ($4.6735e^{-05}$ to 0.0324) and PSNR of extracted PPG is found to be infinite.

Table.8. PRD and PSNR of extracted PPG signal for the proposed method

PPG Sample No.	PRD Extracted	PSNR Extracted
1	8.6322e-05	Inf
2	0.0218	Inf
3	1.4022e-04	Inf

From Table.8. PRD value for the proposed method is achieved to be low. PRD of extracted PPG range from ($1.4022e^{-04}$ to 0.0218) and PSNR of extracted PPG is found to be infinite.

Table.9. PRD of PPG signal in [10]

PPG Sample No.	PRD Stego	PRD Extracted
1	0.4544	0.2595
2	0.6934	0.5405
3	0.7405	0.0453

From Table.9. PRD of stego PPG in [10] is found to be in the range of (0.4544 to 0.7405) and PRD of extracted PPG range from (0.0453 to 0.5405). Proving our algorithm achieves low PRD than [10].

5.4 PATIENT DATA

Following AES encryption and decryption procedure for the patient data is same for all the three biomedical signals. One such example is considered below.

Patient data contains the following information

Name ‘sureka’

Id 27

Blood Pressure 89

Temperature 90

Glucose 78

Details ‘kolar’

Input data is converted into decimal value

Columns 1 through 20

115 117 114 101 107 97 27 89 90 78 107 111 108 97 114 0 0 0 0 0

Columns 21 through 40

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

So on….

Columns 61 through 64

0 0 0 0

AES Key (hexadecimal to decimal conversion)

43 126 21 22 40 174 210 166 171 247 21 136 9 207 79 60

AES Encrypted

Columns 1 through 20

102 160 185 44 251 217 61 172 152 4 250 139 79 122 219 93 125 247 107 12

So on….

Columns 61 through 64

185 27 84 111

Parameter analysis of cover_ECG and stego_signal

PSNR =655.1383

PRD = 0.0569

AES Decrypted

Columns 1 through 20

115 117 114 101 107 97 27 89 90 78 107 111 108 97 114 0 0 0 0 0

So on….

Columns 61 through 64

0 0 0 0

AES - Ciphertext errors: 0, plaintext errors:

Given name is =sureka

Given ID is =27

blood Pressure =89

Temperature =90

Glucose =78

Given Details is = kolar

Parameter analysis of cover_ECG and retrieved_signal

PSNR =655.1383

PRD = 0.0380

6. CONCLUSIONS AND FUTURE WORK

This paper aims to hide patient data along with diagnostic data inside the bio-medical signal. Proposed technique assures high quality of the cover signal which is calculated by PSNR and the same can be used for diagnosis as the PRD achieved in the proposed method is low or almost equal to zero. Comparison of proposed method with the existing state of art papers cited as [10] [11], the value of PRD is observed to be higher than our proposed algorithm, leading to a secure and imperceptible steganographic method to hide and transmit medical data for telemedicine. From Table.1, Table.2, Table.4, Table.5, Table.6 and Table.7, it is clear that the proposed system achieved minimum PRD and high PSNR for all the three bio-medical signals. The security of the proposed algorithm is accomplished with the method of AES encryption which ensures anybody involved in the communication system can receive the message, but only the authorized or intended recipient can decrypt and know the patient’s data.

The proposed method can be used in point-of-care (POC) system to diagnose the patients at the bed side and for emergency purpose POC is considered as the main source.

REFERENCES

[1] S. Edward Jero, Palaniappan Ramu and Ramakrishnan, "ECG Steganography using Curvelet Transform", *Biomedical Signal Processing and Control*, Vol. 22, pp. 161-169, 2015.

[2] Hui Wang, Weiming Zhang and Nenghai Yu, "Protecting Patient Confidential Information based on ECG Reversible Data Hiding", *Multimedia Tools and Applications*, Vol. 75, No. 21, pp. 13733-13747, 2015.

[3] K.V. Padmaja, O.P. Ankitha, Anshu Singhania, M.R. Preethi and Rashmi R Nayak, "DCT based ECG Steganography for Protecting Patient's Confidential Data in Point-of-Care Systems", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 5, No. 7, pp. 6474-6479, 2016.

[4] Oscar J. Rubio, Alvaro Alesanco and Jose Garcia, "Secure Information Embedding into 1D Biomedical Signals based on SPIHT", *Journal of Biomedical Informatics*, Vol. 46, No. 4, pp. 653-664, 2013.

[5] C.A. Liji, K.P. Indiradevi and Anish Babu, "Integer to Integer Wavelet Transform based ECG Steganography for Securing Patient Confidential Information", *Procedia Technology*, Vol. 24, pp. 1039-1047, 2016

[6] L. Keerthana and B.Venkataramanaiah, "ECG Steganography based Privacy Protection of Medical Data for Telemedicine Application", *IOSR Journal of Dental and Medical Sciences*, Vol. 4, No. 2, pp. 46-51, 2014.

[7] Kai-Mei Zheng and Xu Qian, "Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms", *Proceedings of International Conference on Computational Intelligence and Security*, pp. 13-17, 2008.

[8] Ankita G Shirodkar, "Secure Steganography, Compression and Transmission of ECG in Point of Care System", *International Journal of Advances in Science Engineering and Technology*, Vol. 4, No. 7, pp. 94-99, 2015.

[9] Hemin Golpira and Habibollah Danyali, "Reversible Blind Watermarking for Medical Images Based on Wavelet Histogram Shifting", *Proceedings of IEEE International Symposium on Signal Processing and Information Technology*, pp. 31-36, 2009.

[10] Alsharif Abuadbba, Khalil, "Walsh-Hadamard based 3D Steganography for Protecting Sensitive Information in Point-of-Care", *IEEE Transactions on Biomedical Engineering*, Vol. 64, No. 9, pp. 2186-2195, 2016.

[11] Deepali Awasthi and Swathi Madhe, "Evaluation of Wavelet based ECG Steganography System by using Percentage Residual Difference (PRD) Measurements", *Proceedings of International Conference on Communications and Signal Processing*, pp. 1-4, 2015.