ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Medical signal steganography using curvelet Transform

Prasana Vadivambiga.P
Department of Computer Science and Engineering
Manonmaniam Sundaranar University
Tirunelveli, India

Murugeswari.G
Department of Computer Science and Engineering
Manonmaniam Sundaranar University
Tirunelveli, India

Abstract: Steganography is the mechanism of protecting secret data which is sent through the common communication medium. Point of Care (PoC) system is used in most of the hospitals and health care centres. PoC system, it produces patient's physiological readings like sugar level, pressure level, and medical signals like EEG, ECG and EMG etc. In order to consult with the doctors/experts those who are in some other locations, patient data and medical signals are to be sent to them. Medical steganography is the application of steganography for protecting medical data. In this work, a curvelet based medical steganography is implemented for one dimensional (1D) Medical signal like ECG, EMG and EEG. The results proved that, the curvelet based approach is best suited for 1D medical signal. We evaluate the performance of curvelet based approach using the metrics PSNR, MSE and payload. We obtained 35.89 % of average PSNR value for ECG signals, 21.47 % of average PSNR value for EMG signals and 22.57 % of average PSNR value for EEG signals.

Keywords: Medical signal processing; ECG; EMG; EEG; Steganography; Encryption; Curvelet; Watermarking.

I. INTRODUCTION

In Point of Care (PoC) applications are used by hospitals and health care centres around the world. Patient data needs to be transferred from one location to another location in PoC system.

The following two points should be examined in PoC systems.

(i) Patient Privacy

The patient personal data like name, address, phone number, medicare number and physiological readings like sugar, pressure etc. should be kept confidential. The security protocol should afford control on those who can access over the data that are confidential and who cannot access them.

(ii) Security

The embedded software should guarantee the security of the patient information within the communication channels as well as the information stored on the server or on the cloud.

Medical signal of the patients and their physiological readings such as body temperature, glucose level, blood pressure etc. are captured by Body Sensor Networks (BSNs) at home. Health Insurance Portability and Accountability Act (HIPPA) states that the information passed through the internet should be protected and secured to keep the data confidential.

A. ECG Signal

Electrocardiogram (ECG) helps to monitor the function of heart. An ECG records the heart's rhythm and activity on moving strip of paper or a line on a screen. ECG signals are of enormous sizes. A typical electrocardiogram monitoring device generates massive volumes of digital data. Depending on the application for the data, the sampling rate varies from 125 to 1024 Hz. Each data sample may be represented using 8 to 16 bit binary number. Up to 12 different streams of data may be obtained from various sensors placed on the patient's body.

B. EEG Signal

The electroencephalogram (EEG) helps to monitor the electrical activity of the brain from the scalp. The recorded waveforms reflect the cortical electrical activity. EEG signal is quite small, measured in microvolt's (mV).

C. EMG Signal

Electromyography (EMG) is an electro diagnostic medicine technique for evaluating and recording the electrical activity produced by skeletal muscles. Electromyograph instrument is used to produce a signal called an electromyogram. An electromyograph detects the electric potential generated by muscle cells when these cells are electrically or neurologically activated. The signals can be analyzed to detect medical abnormalities, activation level, or recruitment order, or to analyze the biomechanics of human or animal movement.

Steganography is the process of hiding one kind of data into another kind. The techniques used in steganography are classified into two types. They are

(i) Spatial domain technique
(ii) Frequency domain technique

- ***Spatial domain technique***

Spatial domain technique is used to operate, alter, and enhance the image by representing an object in space for given application. It is done by manipulating the pixels of an image directly. The filters used in spatial domain are smoothing filters, sharpening filters, unsharp masking and laplacian filter.

- ***Frequency domain technique***

The spectral transform of an image is modified in frequency domain technique. The transformation of the image is obtained by frequency representation. The inverse transform is computed back to spatial domain to retrieve the original signal.

In frequency domain technique, transform is applied on the original signal and the secret data is embedded on the signal. The transform technique may be wavelet, bandlet or any other frequency transforms. In this work, we used curvelet transform.

In curvelet transform, a small number of coefficients are designed to handle the curves. The curvelet is used to handle the discontinuities well. A reversible curvelet transform is applied for decryption process.

Doctors can make decisions by analysing the patient data by using device at anytime. In steganography, the hidden information is embedded into cover objects and then the cover signal is decomposed into several frequency bands. In medical signal steganography, transmission of patient data is secured and the patient's medical signal is used as cover signal. In medical steganography, the process like thresholding selection, watermarking embedding, and watermarking extraction are involved. The selective numbers of coefficients are modified from ordered coefficients so that threshold is applied on that coefficients.

D. Motivation

Steganography is the successful process, due to the need of data transmission through communication medium. Medical signal steganography is the research area, which provides the solution to security issues in sending the confidential data through communication channels. Data communication is carried out efficiently if the data occupies less memory space. Motivating by above said factors, this paper is implemented to perform medical signal steganography using curvelet approach.

II. LITERATURE SURVEY

Zuo, J., et.al [12] and Deshmukh, P. V et.al [2] proposed a lifting-based wavelet transform for image encryption algorithm. The original image was fragmented into blocks. The coefficients obtained using lifting based wavelet transform are used for encrypting the user key. Wang, H. et al. [10] proposed a technique called Ibaida's wavelet-based secrecy method. This method used ECG signal for protecting the patient's secret information and to store it in a host media. But the original ECG signal cannot be completely reconstructed in this method. At the extraction side, there is a lack of elemental standpoint in both patient information and ECG signal. Embedding-scrambling method is used for securing the patient data as well as the ECG signal. Ranjeet, K., et.al [6] proposed a method using two-dimensional discrete wavelet transform (2D DWT) and Huffman coding techniques for ECG compression system. It is used to develop a 2D array of 1D ECG signal by using cut and align (CAB) technique. Forward compression rate and Huffman coding are used to control the signal quality due to its lossless nature of compression. The median compression rate of algorithm is 65% with 0.999 correlation scores. Wu, W., et.al [11] proposed a technique for protecting the patient data using reversible data hiding scheme. This technique is structured to adaptively embed the private data by using a histogram shifting and thresholding algorithm. Without any distortion, to both the private data and the original ECG signal are restored. Wahballa, O., et.al [9] proposed a watermarking scheme with defect less public key based on Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). The system is analysed by different, original and watermarking images and the robustness is proved. Ren, Y.et.al [7] developed an energy efficient architecture and the data compression of bio-potential signal is implemented by using lifting-based two-dimensional discrete wavelet transform with Z-scanning method. The authors combined two transforms together in one single processor with nearly full hardware utilization by making use of data relevance between row- and column-wise coefficients. This method outperforms many existing ones in energy efficiency, latency, area and hardware utilization, and it is claimed that the method is very suitable for data compression of electrocardiogram signal in wireless sensor system. Samima, S., et.al [8] proposed a work to hide the crucial information in some innocuous objects by using steganography technique. The approach helps to send the actual secret information and store some information of secret data in image steganography. The actual awareness of multi layered secure pass key is achieved by using the secret information. Mai, V., Khalil, I., et.al [5] proposed a stego technique in which the secret data is embedded inside another host data without changing the quality of the host data. Broda, M., et.al [1] proposed an image steganographic method which embeds the confidential information into image using Quick Response (QR) Code**.** The embedding process is conserved by Advanced Encryption Standard (AES) cipher technique so that the QR code is embedded by using Discrete Wavelet Transformation (DWT). The method provides protection by means of general characteristics of QR code with high defending level and high non-susceptibility level, the image steganographic method is implemented. This method's effectiveness is proved with peak signal- to- noise ratio.

III. METHODOLOGY

In this work, medical steganography is implemented using curvelet based approach. The issues related with medical steganography include space required to store the data and security provided to the patient information. The implemented method considers the above factors and medical 1D signals are tested using the curvelet based approach. In this work, the patient medical signal is used as the host signal that will carry the patient secret information and other physiological readings from other sensors such as temperature, glucose, position, and blood pressure. The steps involved in medical signal steganography are explained below.

At sender side, the patient information is embedded with medical signal and encryption. At receiver end, the signals are decrypted and original medical signal and patient data are retrieved. This process is demonstrated in Figure 1.

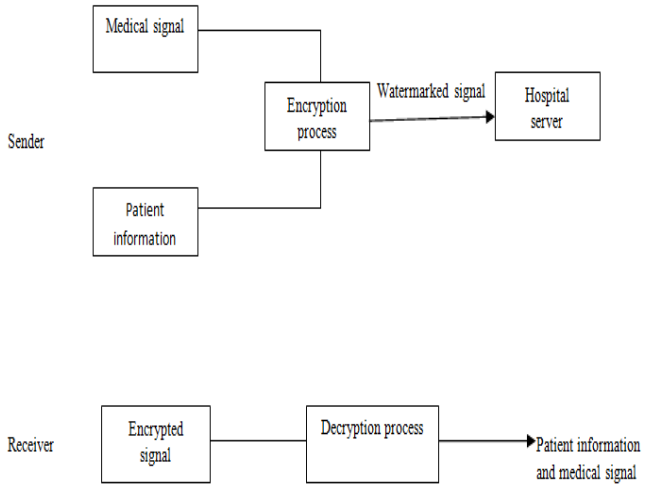

Figure.1 Point of Care system (PoC)

A. Pre-processing

In this work, curvelet transform is used for one dimensional (1D) medical signal steganography. We consider medical signals such as ECG, EMG, EEG signals. Basically these medical signals are 1D in nature. In our work, we convert these signals into 2D format for further processing. The noise present in these signals are smoothened by Savitzky-Golay filter (i.e sgolay filter).This is achieved by convolution process.

Biomedical signals are used to hide the patient data that are forwarded over the internet. The patient information is protected by using the curvelet transform technique. The patient data is converted into binary format. Then it will be stored in signal. The patient data is enclosed into coefficients of frequency sub-bands in such a way that if the value is around zero then they are kept in high frequency bands by using quantisation method otherwise they are kept in low frequency bands. The watermarking process is accomplished by hiding the patient data into cover signal using steganography.

The procedure of curvlet based 1 D medical signal steganography presented in figure 2.

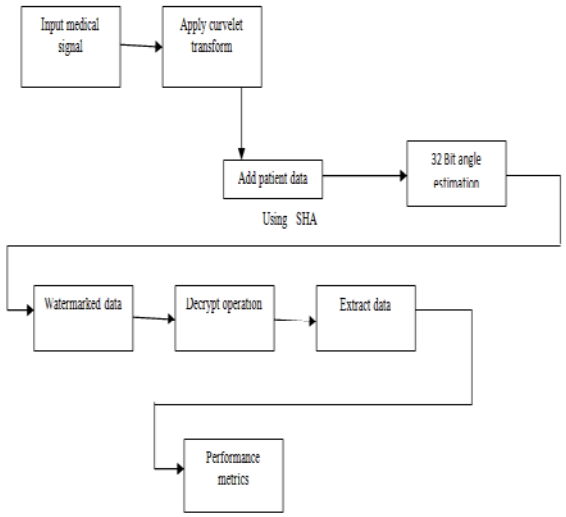

Figure.2 curvelet based medical signal steganography architecture

B. Encryption

This technique aims to prevent the patient data from unauthourized access by unknown individuals. Shamir Secret Sharing algorithm is applied for encryption and it is used with secret key which is assumed as zero.

In cryptography, secret sharing refers to a method of distributing a secret amongst a group of participants, each of which is allocated a share of the secret.The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. The following are the steps that can be involved in encryption.

- Use (k,n) threshold scheme to share the secret S where k < n.
- Choose at random (k-1) coefficients a1,a2,a3…ak-1 , and let S be the a0

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ... + a_{k-1} x^{k-1} \quad (1)$$

- Construct n points (i,f(i)) where i=1,2…..n
- Given any subset of k of these pairs, the coefficients of the polynomial can be found by interpolation, and then evaluate a0=S , which is the secret.

C. Curvelet transform

Discrete curvelet transform dissolves the given signals into frequency sub bands. The 2D format of the medical signal is obtained. During 1D to 2D conversion process, few contents will be lost. There are four scales used in curvelet transforming. Scale 1 consists of low frequency components. Scales 2 and 3 consist of the intermediate frequency components. High frequency components will be in scale 4.
The curvelet coefficients (A^D) are calculated by using Equation (2)

$$A^D(q,r,s) = \sum_{m_1, m_2 \in c_j} \dot{f}[m_1, m_2 - m_1 \tan\theta_l]\dot{U}_j[m_1, m_2] \; e^{ii2\prod(r_1 m_1 / B_{1,j} + r_2 n_2 / B_{2,j}} \quad (2)$$

Where q,r,s represents the parameters of scale, orientation and translation respectively; c_j denotes the rectangle bound of the image in the frequency space. Let f[t_1, t_2] denotes cartesian array of an image f and 2D discrete Fourier transform is given as $\dot{f}$ (m1,m2). Slope is denoted by $\tan\theta_l$. An cartesian window is denoted by $\dot{U}_j(m1, m2)$. Parabolic scaling stated that the length of $B_{1,j}$ about 2^j and width $B_{2,j}$ about $2^{j/2}$.

D. Threshold Selection Algorithm

The major components involved are (i) Threshold selection (ii) Watermark embedding and (iii) Watermark extraction. The patient data size decides the number of co-efficients to be modified. In general, the threshold is selected from ordered co-efficients. In such way that contains the number of co-efficients which is less than or greater than that of number of co-efficients to be modified. In this work, n/2 co-efficients are selected in either side of co-efficients which values near to zero.

E. Quantisation method

It is a process of representing a huge possibly countless set of values with a much less set. The quantization based watermark embedding technique alters the selected curvelet co-efficient as follows

$$A^* = \alpha \mid A \mid X \quad (3)$$

Where A^* is the modified coefficient;
A is an original coefficient;
α is the embedding strength constant.
X is +1,if the watermarked bit is 1.
X is -1, if the watermarked bit is 0.

F. Embedding Operation

Scrambling is the process of signal encoding for the prevention of unauthorized access. To ensure high data security, a scrambling is implemented. A scrambling operation is performed in this technique, where scrambling matrix is

stored inside both the transmitter and receiver. In encryption process, the host signal is given as input. In curvelet decomposition, the medical signal will be embedded with the secret data. The patient data in binary form is scrambled and embedded with signal. Data with minimal significant bit is embedded using the algorithm. For medical signal, the watermarking technique is applied and once encryption is completed, decryption occurs by reverse curvelet process.

G. Inverse Curvelet transform

At last, the rearrangement of 255 sub-bands watermark are Combination of time and requency domain is substituted with time domain by converting existing signal using reverse curvelet process. For assuring that the coefficient values are integers, transferring and scaling of coefficient matrix is done. Further, a sub-band among 255 sub-bands is selected in every row of its coefficient matrix. Till the end of the coefficient matrix the algorithm is analysed. To return the original image, coefficient matrix is transferred and rescaled and to get the watermarked medical signal, inverse curvelet transform is used.

H. Decryption

The following information is necessary for retrieving the secret data of watermarked medical signal at receiver side.

(i) Scrambling matrix
(ii) Steganography levels vector

The seven-levels of curvelet packet decomposition are applied to generate 255 sub-bands signals. By using scrambling matrix, the information is extracted, then secret bits are arranged in order and the rows of the scrambling matrix are fetched. At last decrypted process is taken using the extraction of secret bits. The watermarked extraction process resembles to watermarking embedding process.

IV. EXPERIMENTS AND RESULTS

To evaluate the curvelet based medical signal steganography, the three performance measures are used. The peak- signal- to noise ratio (PSNR) in decibels between two signals is computed for evaluating the implemented model. The difference between the original signal and a compressed signal is measured by using Equation (4).

$$PSNR = 10\log_{10} K_{\max}^2 / MSE \text{ db} \quad (4)$$

The maximum possible pixel value of the signal is represented as . For each sample, the pixel value is represented by 8 bits. i.e. The maximum value will be 255.
The square of error between the cover signal and stego signal is noticed. The Mean Square Error (MSE) is measured by using, Equation (5).

$$MSE = \frac{1}{K*L}\sum_{i=1}^{l}\sum_{j=1}^{k}(y_{ij} - y_{ij}^{1}) \quad (5)$$

Where K is the number of rows in cover signal, where N is the number of column of cover signal, where y_{ij} is denoted as the pixel value from cover signal, where y_{ij}^{1} represents the pixel value from stego signal. Root Mean Square error (RMSE) is the measure of square root of MSE and is calculated by Equation (6).

$$\text{RMSE} = \sqrt{MSE} \quad (6)$$

A. Embedding capacity

Embedding capacity is a measure of maximum size of secret data that can be embedded. The unit for embedding capacity is Bits per pixel (BPP).

Payload

The ratio of number of bits to be embedded to the no of bits in the cover signal is referred as payload.

Payload = (No of bits to be embedded / No of bits in the cover signal)*100. (7)

The input ECG signal is given in Figure 4. And patient data is given in Figure 6. The signal at various stages is given in Figure 5, Figure 7, and Figure 8. The recovered signal is shown in Figure 9.

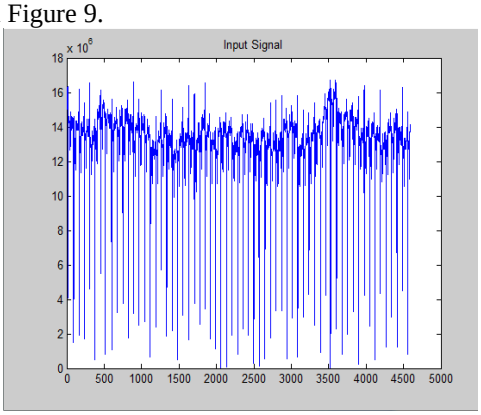

Figure.4 Input signal

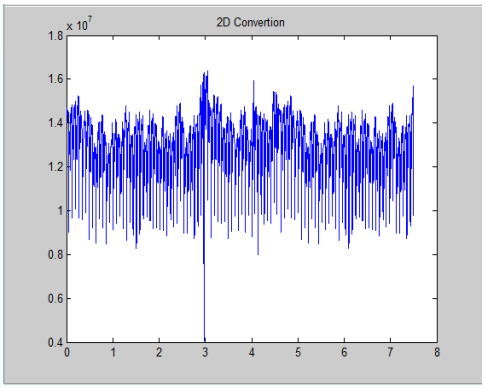

Figure.5 2D signal

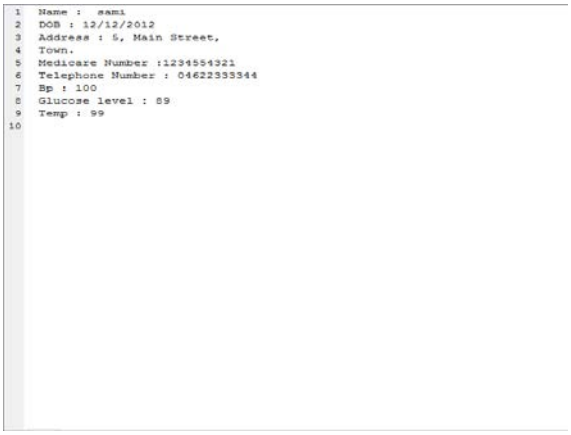

Figure.6 Patient confidential information

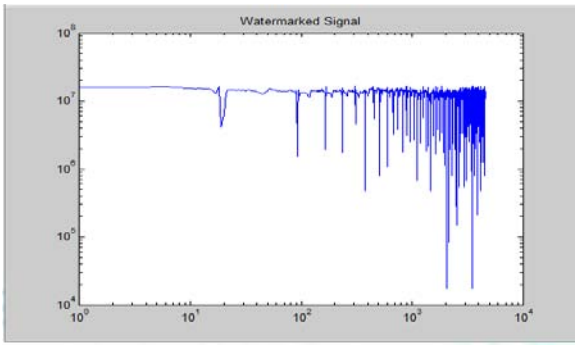

Figure.7 Curvelet signal

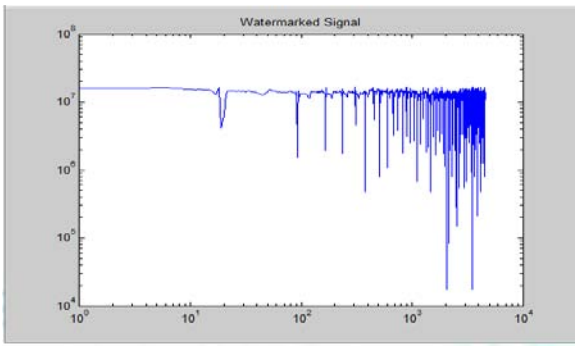

Figure.8 Watermark signal

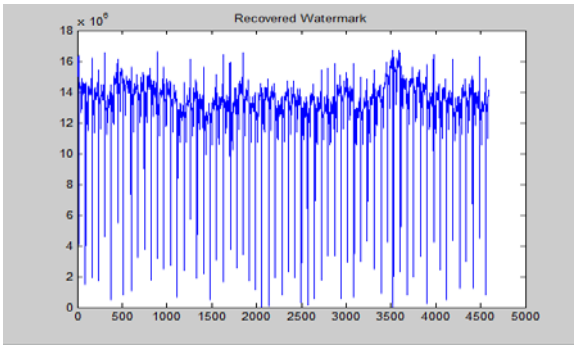

Figure.9 Recovered watermark signal

B. Performance Analysis

In order to evaluate the curvelet based steganography system, experiment was conducted by using 3 kinds of 1D medical signal namely ECG, EEG and EMG. The performance is presented in table1, table2 and table3.

ECG, EEG and EMG signals are taken from MIT-BIH dataset which is available publically in the internet. For ECG signal analysis, we used 5 patent's data and their respective ECG signals. We used same cover size and various message size data. It is found that, this approach produces 98.47 % payload and 38.43 % of PSNR. From the analysis it is found that, payload and PSNR factors are affected by message size.

Table.1. Performance analysis using various ECG signals

S.NO	ECG signal	Patient record	MSE	RMSE	PSNR	Message size	Cover size	Payload
1	100.dat	Patient1	303.5706	17.4233	35.7535	17586	1800	97.7000
2	217.dat	Patient2	320.4434	17.9009	35.6360	17810	1800	98.9444
3	219.dat	Patient3	211.2937	14.5359	36.5404	17922	1800	99.5667
4	220.dat	Patient4	564.6782	23.7630	34.4058	17698	1800	98.3222
5	221.dat	Patient5	161.8475	12.7219	37.1193	17362	1800	96.4556
		AVERAGE	**251.648**	**17.269**	**35.891**	**17675**	**1800**	**98.197**

In ECG signals analysis, 35.90 % of PSNR is obtained.

Table.2. Performance analysis using various EMG signals

S.NO	EMG signal	Patient record	MSE	RMSE	PSNR	Message size	Cover size	Payload
1	Emg-healthy .dat	Patient1	567.3467	23.8190	20.6263	6889	8640	95.6806
2	Emg-myopathy.dat	Patient2	734.9625	27.1102	19.5021	7001	8640	97.2361
3	Emg-neuropathy.dat	Patient3	243.8692	15.6163	24.2932	7113	8640	98.7917
		Average	**515.3928**	**22.1818**	**21.4739**	**7001**	**8640**	**97.2361**

In EMG signals analysis, 21.47 % of PSNR is obtained.

Table.3. Performance analysis using various EEG signals

S.NO	EEG signal	Patient record	MSE	RMSE	PSNR	Message size	Cover size	Payload
1	eeg-1.dat	Patient1	133.7513	11.5651	26.9018	6833	8640	94.9028
2	eeg-10.dat	Patient2	404.0695	20.1015	22.1002	7169	8640	99.5694
3	S001a.dat	Patient3	885.7235	29.7611	18.6918	7113	8640	98.7917
		Average	**474.5145**	**20.476**	**22.5646**	**7038**	**8640**	**97.755**

In EEG signals analysis, 22.57 % of PSNR is obtained.

V. CONCLUSION AND FUTURE SCOPE

Curvelet based medical steganography is implemented in this work and this approach is tested for one dimensional medical signal such as ECG, EEG, and EMG. This approach provides a security and secrecy for medical data. In Point of Care system the 7 level decomposition is applied in this work. Embedding sequence is obtained using scrambling matrix. It is found that the curvelet base medical steganography supports one dimensional medical signal analysis. We obtained appreciable values for PSNR and payload. This approach can be extended for 2D medical images like MRI, CT ultra sound images. The watermarking scheme is used in this work can be extensively used in other image processing and data communication application where data security is an important issue.

A steganography for hiding patient details and their diagnostic data using one dimensional medical signal is implemented in this paper. This method provides a secured communication and secrecy in a Point Of Care System. The 7-level curvelet decomposition is applied. Relying on a user defined key a suitable embedding sequence is found using a scrambling matrix. We analyzed the diagnoses standard mal perversion. Hence the watermarked medical signal are utilised for diagnoses and encrypted data are retrieved as a whole.

VI. REFERENCES

[1] Hajduk,V., Broda,M., Kováč,O., & Levický,D. (2016, April). Image steganography with using QR code and cryptography.InRadioelektronika(RADIOELEKTRONIKA), 2016 26th International Conference (pp. 350-353). IEEE.

[2] Deshmukh, P. V., Shahade, A. K., & Patil, G. Y. (2015, January). Data hiding mechanism based on encrypted image in a discrete wavelet zone of a carrier image. In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on (pp. 1-4). IEEE.

[3] Fridrich, J., & Kodovsky, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868-882.

[4] Lei, B., Soon, Y., Zhou, F., Li, Z., & Lei, H. (2012). A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition. Signal Processing, 92(9), 1985-2001.

[5] Mai, V., Khalil, I., & Ibaida, A. (2013, July). Steganography-based access control to medical data hidden in electrocardiogram. In Engineering in Medicine and Biology Society (EMBC), 2013 35th Annual International Conference of the IEEE (pp. 1302-1305). IEEE.

[6] Ranjeet, K., Kumar, A., & Pandey, R. K. (2013, December). An efficient compression system for ECG signal using QRS periods and CAB technique based on 2D DWT and Huffman coding. In Control, Automation, Robotics and Embedded Systems (CARE), 2013 International Conference on (pp. 1-6). IEEE.

[7] Ren, Y., Han, J., Yu, Z., Xuan, S., & Zeng, X. (2015, November). A lifting-based 2-D discrete wavelet transforms architecture for data compression of bio-potential signals. In 2015 IEEE 11th International Conference on ASIC (ASICON)(pp. 1-4). IEEE.

[8] Samima, S., Roy, R., & Changder, S. (2013, December). Secure key based image realization steganography. In Image Information Processing (ICIIP), 2013 IEEE Second International Conference on (pp. 377-382). IEEE.

[9] Wahballa, O., Abdalla, A., Hamdnaalla, K., Ramadan, M., & Xu, C. (2016, July). An efficient and secure certificateless public key watermarking scheme based on 1VD-DWT. In 2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) (pp. 183-188). IEEE.

[10] Wang, H., Zhang, W., & Yu, N. (2015). Protecting patient confidential information based on ECG reversible data hiding. Multimedia Tools and Applications, 1-15.

[11] Wu, W., Liu, B., Zhang, W., & Chen, C. (2015, May). Reversible data hiding in ECG signals based on histogram shifting and thresholding. In Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on (pp. 1-5). IEEE.

[12] Zuo, J., Cui, D., Gong, Y., & Liu, M. (2015, April). A Novel Image Encryption Algorithm Based on Lifting-Based Wavelet Transform. In Information Science and Control Engineering (ICISCE), 2015 2nd International Conference on (pp. 33-36). IEEE.