Applying Electrocardiogram as a CoverSignal toHide Patient's Confidential Information: A Review

Gagandeep kaur Randhawa
M.Tech Scholar,Dept of Electronic and Communication GCET
Gurdaspur India
Damandeep Kaur
Assistant Professor
Department of Electronic and Communication GCET
Gurdaspur India

Abstract : As technology grows day by day, wearable electrocardiogram monitoring devices also increases. A lot of patient confidential data is monitored and shared worldwide. There is need to protect patient's secret information. Several techniques have been developed where Electrocardiogram signals can be utilized to hide the patient secret information. The whole process is focused on a) to provide encryption to the patient data and b) to recover the original ECG signal.HIPAA (Health Insurance Portability and accountability Act), governess that patient transmitted information must be safe to any kind of threats, to protect its confidentiality and privacy.This paper review distinct methods of ECG steganography techniques to hide patient secret information

Keywords:Electrocardiogram, steganography, watermarking.

Introduction

1.1ECG Based Data Security

In modern world data can be shared worldwide anywhere through different mode of sharing. Apart from the technologies which facilitate an ease of sharing of data, security of information from any eavesdropper/ third party client is a bigger concern. In the field of healthcare, patient information is transmitted from one place to nearby hospitals for proper observation of the patient. This information is solely important for his health records and observations hence need to protect from various threats [12]. This can be done with the help of the electrocardiogram (ECG) signals[15]. ECG is one of the most useful diagnostic tests in emergency medicine. The ECG is the cornerstone for making the diagnosis of cardiac ischemia and is used for making decisions about eligibility for thrombolytic therapy [1]. ECG can be helpful in many ways as it provides evidence to support the diagnosis. It plays an important role in management of abnormal cardiac rhythms [2]. Also, Diagnose the cause of chest pain, proper use of early intervention in myocardial infraction depends upon it. Human heart generates distinct deflections on the ECG [3]. Such deflections can be recorded in the forms of waves named as P, Q, R, S and T waves. As shown in Fig.1, P wave in the upward directions represents depolarization. Q wave represents a downward deflection and depict septal depolarization [4]. Similarly, R wave depicts ventricular depolarization; S wave represents late ventricular depolarization and T wave shows repolarization of the ventricles [5]. Hence, these waves track the activates of heart.As technology grows number of portable devices are increases which record ECG activities over time span and transmit the patient data remotely. Shimmer and Alivecor iPhone are examples of these systems [6]. The data acquired from ECG signal can be stored in different formats like ecgML,XML-ECG, Philips XML, DICOM-ECG etc. [7]

As ease of data sharing and health monitoring is increases demand of providing security to the confidential data of patient is also increases. ECG steganography techniques provides solution to this problem as it protects patient confidential data during transmission from one remote location to other [8].

1.2 Steganography

As technologies grows, monitoring patients at their home instead of hospital is also increases, which fortunately suppress the number of visitors in a hospital. These Point of care (POC) techniques [9] can provide a reliable information about patient's health and can be transmitted to the expert or doctors from anywhere at any time. Internet remains the common medium oftransmitting this information which reveals this information to some threats of communication

Many techniques based on cryptography has been evolved in past to protect the data.

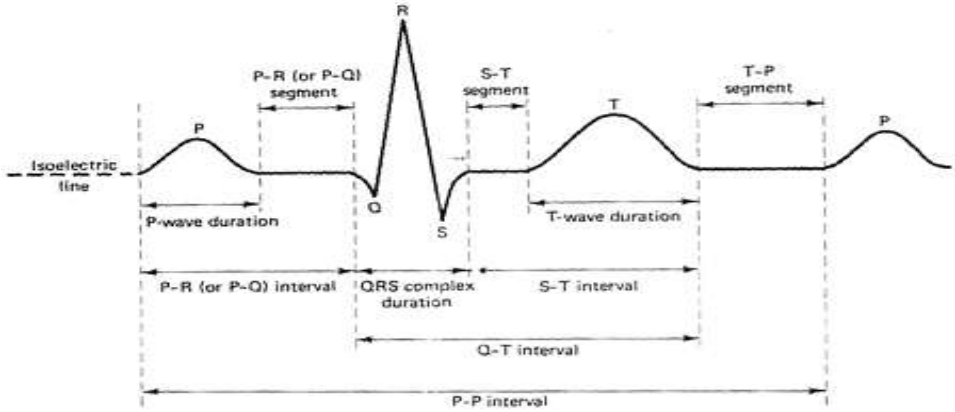

Fig.1. P, Q, R, S, and T wave of Electrocardiogram [5]

These techniques provide a desirable security to the patient information by employing some encryption. However, this lead to a complex computational data and not considered for POC techniques. Steganography i.e. hiding information (patient information in current scenario)[11] in another signal to protect it from any threats provide solution to above problem. This reduces the overall data overheads as well as original signal can be recovered from watermarked signal. There are two distinct domain of ECG steganography classified as Time domain and Frequency domain. The later one can hide large number of information but yield to lower performance. On the other hand, Time domain ECG steganography has higher rate of performance but store less amount of data [12]. Patients health data (like ECG signal, temperature etc.) can be acquired with the help of sensors.The collected data is then sent to PDA [13] via some mode of communication. Before transferring the data, a stenography technique has been applied where patient information is hide into a ECG signal (using ECG as host signal). The resultant watermarkedsignal [14] is then transferred to the hospital through the use of internet. On the receiver end (hospital) this hidden information is retrieved successfully. This reduced the overall size of size of encrypted signal and reduce overheads.

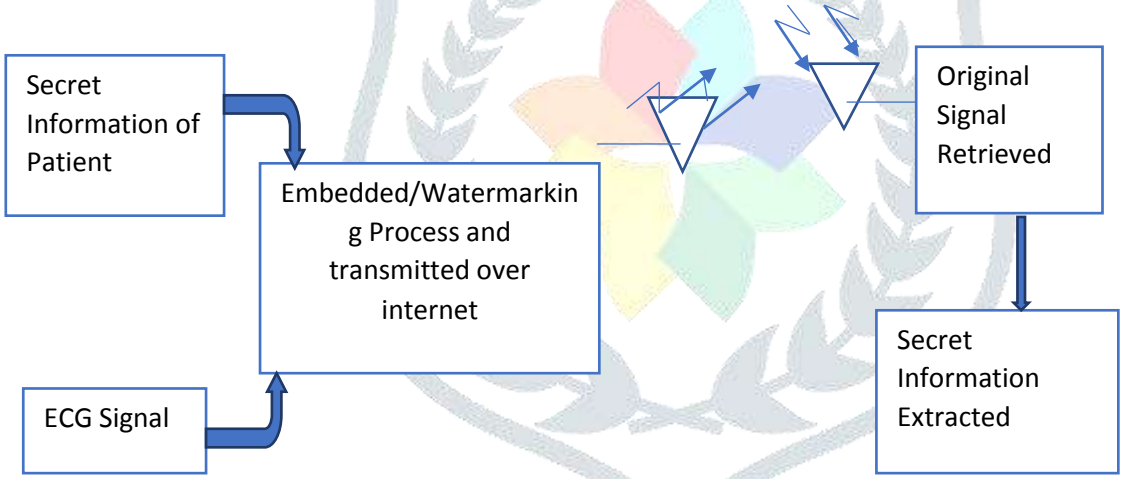

Fig.2. General Process of ECG Steganography
Ablock diagram of steganographic technique has been shown in Fig.2.

1.3ECG Data Encryption Measures

There are numerous data encryption measures which ensure secure transmission of patient data. This include key space analysis as well as key sensitivity. In key space analysis the focus is to provide large number of key spaces which reduces predictably of the key. There are chances that patient's information is vulnerable if the key is less sensitive to changes. Therefore, it must be sensitive to forefend any third party attack.

1.3Limitations of ECG data hiding and encryption techniques

There are namouras techniques which are utilized for hiding patient information from many threats. ECG signals can be used as a cover signal for the same, but there are still many areas which need a concern.Following issues can still improve:

- Selection of parameters
- Reconstruction of original ECG signal
- Distortion level in recovered data.
- Embedding process
- Inaccurate measures
- random behavior of error.

- Security Threats
- Sophisticatedfeature extraction

The next section reviews distinct steganographic techniques where patient's secret information is embedded with ECG signal to transmit it securely from one place to the other. The later section explains the various terminologies used in steganography applying Electrocardiogram as a cover Signal to Hide Patient's Confidential Information.

2. Related Work

Ibaida. A. in [15] proposed a stenographic technique to secure ECG data of the patient by enclosing it with the range of special numbers at some particular locations. The complete methodology of their technique has been depicted in Fig.3. They have utilized data from MIT-BIH Arrhythmia database [16]. Further authors validate that there are numerous ($2.1475* 10^{9)}$ combination of special range which can provide a great level of security to the data. Authors achieved very small PRD of watermarked ECG for both normal and abnormal ECGs.

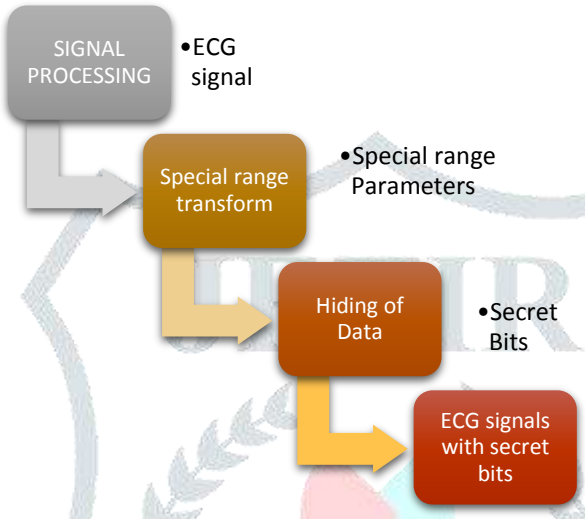

Fig.3. Process of hiding patient information with special number series

In today's world cardiac patient's health has been taken care by utilizing POC (point of care) devices which monitor the activities of an ECG patient. *Ayman Ibaida and Ibrahim Khalil* in [17] coined a novel technique to secure the patient's patient data using ECG steganography based on wavelet. Their research mainly focused on reducing the distortion level of ECG signals (during steganography) in POC [9] systems. The entire provides security to patient data according the privacy and security guidelines of HIPAA [10]. Their methodology includes encryption of patient data using technique XOR ciphering, wavelet packet decomposition (DWT) [18] and embedding operation to provide high end security with the help of a pre-shared key and scrambling matrix. Further, watermarked ECG signal is transferred (secured data using wavelets) to the receiver end. To get back the original data safely on the other end; inverse wallet decomposition and extraction process of watermark has to performed. They also performed effective analysis of their technique to evaluate author utilized the percentage residual difference and wavelet PRD[18]. Authors claimed that there is very less distortion in the received data (< 1%) and encrypted data is fully recovered.

Chen S. T. et.al in [19], proposed a scheme based on transform domain quantization to hide the confidential data of the patient. In this paper they employed a watermarking technique on ECG data to prevent the information of the patient. Quantization includes various transforms like Discrete wavelet transform (DWT), Discrete cosine transform (DCT) and Discrete Fourier transform (DFT)[18]. More precisely in this paper authors coined a technique based on quantization audio watermarking. Quantization has been done ECG signals rather than audio signals. They utilized data from MIT-BIH Arrhythmia database [15]and embed the watermarks with the ECG data. Authors asserted that the obtained data when compared with original MIT-BIH Arrhythmia database samples, results into very negligible variation, hence the proposed technique is effective.

Jerro S. T. et al in [20], projected a novel approach of ECG steganography utilizing Fast Discrete Curvelet Transform . Their methodology includes a) Preprocessing: In this ECG signals (1D) is converted into ECG image (2D) and corresponding curvelet coefficients has been calculated. In addition, watermark in binary format is embedder with curvelet coefficients of image. b) selection for threshold,c) selection of n*n sequence for watermarking. The distortion of signal is less and no loss of data.

Jero S. E. et.al[21] coined a novel ECG approach of steganography in which they utilize DCT to decompose signals and singular value decomposition for embedding the secret data of the patient into ECG signal (decomposed).

They embed ECG image (2D) and watermark (utilizing SVD) by replacing the singular values of image with the values of patient data.

The secret information can be reobtained with the help of inverse DWT. This method yields to hide secret data into ECG signals with a minimum error rate of 0.6%.

Yang C. C. and Wang F. W. in [22] proposed steganography technique for electrocardiogram (ECG) based on coefficient alignment.Authors, represented two techniques; lossy steganography and reversible steganography. Lossy steganographyis further classified into high capacity and quality

ECG steganography, which are efficient technique to conceal the information of the patient. Further, irreversible technique can retrieve the original signal along with concealing of the same. In addition to this, authors performed simulation of both techniques and listed the results of

various attacks on extracted watermarks. This method is effective in many ways as it has lesser time complexity and yield to more prominent computational speeds.

Wang H. et.al [23] depicted an approach of protecting patient's information which is based on reversible hiding of ECG. They also oppose the technique utilized by as that is not able to reconstruct the original ECG data fully. In this paper authors proposed a method of embedding which maintain image of high visual quality and another method to secure the patients information based on embedding-scrambling.

Authors claimed to have distortion of 1% between the watermarked and original ECG signals and higher embedding capacity. Overall both methods are reversible.

Yuan S. and et.al presented a data hiding technique in [24] which is based upon pixel value differencing. It enhances the security level to a greater extent as their technique is not traceable by RS attack and histogram attack [25]. In their methodology by employing Hilbert filling curve, an image (cover) is matched into a 1D pixels sequence. This technique reduces the detectable artifacts as well as require no memory for storing embedded data. Also, the embedded image produced has less distortion.

3. Performance Evaluation Parameters

3.1 Mean Square Value

Mean Square error (MSE) is defined as the measure of degree of similarity or it's the extent offeror/distortion between two signals. MSE could also be thought of a measure of signal quality. Y is original signal of M predictions and Y' compared signal. [26]

$$MSE(Y, Y') = \frac{1}{M} \sum \frac{M}{i=1} (Y - Y')^2$$

3.2 Peak Signal to Noise Ratio

Peak signal-to-noise ratio (PSNR) is the ratio of the maximum possible power of pixel value to the power of noise. It is generally calculated in logarithmic scale and its valueis always represented in db. MAX stands for maximum value of signal. [26]

$$PSNR = 20 * log10\ (MAX) - 10 * log10\ (MSE)$$

3.4 Percentage Residual Difference

PRD (percentage residualdifference) is tool used to measure the difference between the actual ECG host signal and the watermarked ECGsignal. [25]

$$\text{PRD} = \sqrt{\sum_{I=1}^{N}((Y - Y')^2} \Big/ \sum_{i=1}^{N}(Y')^2$$

*Y*represents the original ECG signal and *Y'i*s the watermarked signal.

3.5 Bit Error Rate (BER)

BER can be evaluated as the ratio of number of errors occurred to the number of bits sent in a transmission system.

3.6 Wavelet Based Weighted Percentage Residual Difference(WWPD)

WWPRD is based on biological wavelet decomposition [25]. Mathematically, it defined as:

$$\text{WWPRD} = \sum_{j=0}^{Nm} w'WPRD'$$

where Nm is total number of sub bands, w' represents the weight value related to sub band j and WPRD' depicts the wavelet-basedpercentage residual difference.

3.7 Root mean Square Error (RMS)

Root mean square Error is utilized to find out the distortion/error between the reconstructed signal with respect to the actual signal. Mathematically it is defined as:

$$\text{RMS} = \sqrt{\sum_{n=1}^{N} \left(\frac{(Y-Y')2}{N-1}\right)}$$

Y is original signal, Y' is the reconstructed signal[25].

3.8 Quality Score

This parameter measure compression in relation to the reconstruction errors. It is defined as the ratio of Compression ratio and PRD.

$$\text{QS} = \frac{CR}{PRD}$$

The performance of compression method is dominating if it has higher Quality score [25].

4. Conclusion

Patient secret information is kept hidden and secured when it is embedded with ECG signals. Distinct time and frequency domain ECG stenographic techniques has been developed to achieve two major objectives a) providing encryption to patient secret information and b) recovering original signal after watermarking. This paper revived several techniques related with it.Finally, conclusion has been made in form of Table.1. which delineate the features of several ECG techniqu

Table.1.Features of distinct approaches [15]

S.No	Authors	Features
1	Ayman Ibaida and Ibrahim Khalil [15]	• Effective technique for hiding patient data • Numerous combination of special rage numbers which can protect patient confidential data over transmission. • Small amount of PRD
2	Ayman Ibaida and Ibrahim Khalil [17]	• Novel approach of hiding patient data based on wavelets. • Focused on reducing the distortion level of ECG signals (during steganography) in POC systems. • Very less distortion in the received data (< 1%) and encrypted data is fully recovered
3	S. Chen, T. Guo, Y. Huang, H. Kung, W. Tseng and S. Tu [19]	• Approach based on transform domain quantization to hide the confidential data of the patient. • technique based on quantization audio watermarking • very negligible variation in recovered data.
4	J. Edward, P. Ramu, and R. Swaminathan [20]	• Effective approach based on DCT • Embed ECG image (2D) and watermark (utilizing SVD) by replacing the singular values of image with the values of patient data. • minimum error rate
5	Yang C. C. and Wang F. W. [22]	• steganography technique for electrocardiogram (ECG) based on coefficient alignment. • lossy steganography and reversible steganography. • Less complex and prominent computational speeds
6	C.Y Yang, and W.F. Wang[23]	• Proposed approach reversible hiding of ECG maintain image of high visual quality of patient data • distortion of only 1% between the watermarked and original ECG signals • higher embedding capacity
7	J. Edward, P. Ramu, and R. Swaminathan [21]	• Inverse DWT • Minimum error rate in hiding secret data of 0.6%
8	S.Y. Shen, and L.H. Huang [24]	• Proposed approach pixel value differencing technique which is not traceable by RS attack and histogram attack. • Utilized employing Hilbert filling curve, an image (cover) is matched into a 1D pixels sequence reduces the detectable artifacts • no memory requirement for storing embedded data
9.	M. Al Ameen &J. Liu and K. Kwak[27]	• Illustrated about Wireless body area network • Listed various medical health care devices like Health Gear, Mobi Health, Ubimon and CodeBlue e.t.c. • Main focus on the security and privacy issues related to medical BAN and general wireless sensor networks.
10.	P. Kumar and H. J.Lee [28]	• Reviewed various healthcare technologies based on wireless medical sensor networks(WMSNs). • Compared distinct techniques of health monitoring and threats to it in a network. • Discussed about threats to patient information in CodeBlue [7], Alarm-Net [13], UbiMon [14], MobiCare [16,53] and STAIRE [55]. • Draws attention to the problems related to symmetric cryptography, secure routing, security and Quality of service.
11.	M. S. Nambakhsh et.al [29]	• Proposed a watermarking approach using EZW algorithm on medical images. • Novel approach of control watermarking as images are extracted from low to high resolution. • PSNR obtained is of 35dB (b/w the original and watermarked

		image) 512 to 8192 bytes of the mark signal. • This approach utilize 15% of the host image which is improved than previous works.
12.	Guo Yina and Zhou Dawei [30]	• Watermarking based on single channel electromyography blind recognition model. • Reduce the complex circuit requirements. • Reduces the noise levels in surface Electromyography(sEMG). • Problem of blind source separation disorder is removed by utilizing embedded watermarking technique.
13.	A. Pandy, B. Singh Saini, B. Singh and N. Sood [31]	• Proposed an approach for data compression of 2D electrocardiogram (ECG) based on effectual sample entropy (SampEn). • Able to compress the quasi-periodic ECG signal by intercepting the intra and inter-beat correlations. • Utilized MIT-BIH arrhythmia database. • higher compression • low reconstruction error
14.	R. Ramli and N. Zakaria [32]	• Studied distinct approaches and privacy issues • Outlines following pints as conclusion: o Video monitoring can have watched by any third party. o Spam based on location of the patient and economicdamages o Unknowingness of patient family regarding privacy of information.

References

[1]. Prieto, C. Mailhes, "Multichannel ECG data compression method based on a new modeling method," IEEE. *Computers in cardiology*, pp.261–264, 2001.

[2]. P.E. McSharry, G.D. Cliffor, and L. Tarassenko "Adynamical model for generating synthetic electrocardiogram signals," *IEEE. Trans. Biomedecial Engg*., pp. 289–294, 2003.

[3]. Z. Cheng, Y. Zhang, "Design and Implementation of Real-time Telecardiology Monitor Terminal," *Journal ofComputer Engineering*, vol. 33, pp. 264-266, Jun. 2007.

[4]. W. Xie, "Principle of ECG," *Modern Medical Science Apparatus and Application*, Vol. 3, pp. 74-75, Mar. 2007.

[5]. J. McNames, and M. Aboy, "Rekiability and accuracy of heart rate variability metrics versus ECG segment during,"*Journal of Medical Bio. Eng. Computer*, Vol:44, pp.747-756, 2006.

[6]. Available from https://www.alivecor.com/press/press_release/alivecor-expands-mobile-ecg-device-offering-to-include-iphone-5/ accessed on 24-02-2018.

[7]. Raymond R. Bond, Dewar D. Finlay, Chris D. Nugent, George Moore, "A review of ECG storage formats", *International journal of medical informatics*, pp. 681–697, 2011.

[8]. P. C. Su, M. T. Lu, "A practical design of high volume steganography in digital video files", *Journal of Information Hiding and Multimedia Signal Processing*, pp.247–266, 2013.

[9]. Er. L. Nelson, M. G. Ericksen, and Sarah E. Frasure, "Point-Of-Care Ultrasound Diagnosis of a Catheter-Associated Atrial Thrombus", *The Journal of Emergency Medicine*, Vol. 50, No. 2, pp. e75–e77, 2016.

[10]. X. Kong, and R. Feng, "Watermarking Medical Signals for Telemedicine". *IEEE Transactions on Information Technology in Biomedicine* pp.195–201, 2001.

[11]. J.S. Pan, W. Li, C.S. Yang, and L. Yan, "Image steganography based on subsampling and compressive sensing", *Multimedia Tools and Applications*, DOI 10.10071/s11042-014-2070-1.

[12]. A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in Proc. 5th *Int. ConferenceIntelligence Sensor Networkand Information*, pp. 207–212, 2010.

[13]. J. M. García, E. Parada, V. Collantes and E. Casilari-Pérez, "A PDA-based portable wireless ECG monitorfor medical personal area networks", *IEEE MELECON Benalmádena Málaga*, pp. 713-716, 2006.

[14]. J.T. Sørensen, P. Clemmensen, and M. Sejersten, "Past, present and future",*Rev. Española Cardiol*. 66:212–218, 2013.

[15]. A. Ibaida, I. Khalil, and D. Al-Shammary, "Embedding patients confidential data in ECG signal for healthcare information systems", *In the proceeding ofIEEE EMBC*. pp 3891–3894, 2010.

[16]. Physionet https://www.physionet.org/physiobank/database/mitdb/ accessed on 21-2-2018.

[17]. A. Ibaida, I. Khalil, and D. Al-Shammary, "Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems", *IEEE Trans. Biomed. Eng.*vol. 60, pp. 3322–3330, 2013.

[18]. Ma. weizhen, "Anovel systolic array implementationof: DCT, DWT and DFT", *IEEE Conference on Computer and Communication Systems*, 1990.

[19]. S. Chen, T. Guo, Y. Huang, H. Kung, W. Tsengand S. Tu, "Hiding patients confidential datainthe ECG signal via transform-domain quantization scheme". *Journal of Medical System*, pp.38:54, 2014.
[20]. J. Edward, P. Ramu, and R. Swaminathan, "Imperceptibility-robustness tradeoff studies for ECG steganography using continuous ant colony optimization". *Expert System and Application*, Vol. 49: pp.123–135, 2016.
[21]. J. Edward, P. Ramu, and R. Swaminathan, "Discrete wavelet transform and singular value decomposition-based ECG steganography for secured patient information transmission". *Journal of Medical System*, Vol. 38: pp.1–11, 2014.
[22]. C.Y Yang, andW.F. Wang, "Effective electrocardiogram steganography based on coefficient alignment", *Journal of Medical System*, vol. 40: pp. 1–15, 2016.
[23]. H. Wang, W. Zhang and N. Yu, "Protecting patient confidential information based on ECG reversible data hiding", *Multimedia Tools and Applications*,Vol. 75: pp. 13733–13747, 2016.
[24]. S.Y. Shen, and L.H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions", *ComputerSecurity*, Vol. 48: pp. 131–141, 2015.
[25]. B. Norouzi, S. Mirzakuchaki, "A Fast Color Image Encryption Algorithm Based on Hyper-Chaotic Systems", *Nonlinear Dynamics*, Vol. 78, no. 2, pp. 995-1015, 2014.
[26]. Kainth. K and Singh G., "A potent approach to enhance security extent of an image during image encryption", *International Conference on Computing, Communication & Automation*, pp. 1104-1109, 2015.
[27]. M. Al Ameen & J. Liu and K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications", *Journal of Medical System*, pp.36:93, 2012.
[28]. Kumar. P. and Lee. H. J., "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", *MDPI Sensors open access*, pp. 55-91, 2012.
[29]. Nambakhsh.M. S., Ahmadian A., Ghavami. M., Dilmaghani. R. and Fard. S, "A Novel Blind Watermarking of ECG Signals on Medical Images Using EZW Algorithm", *Proceedings of the 28th IEEE EMBS Annual International Conference*, pp.3274-3278, 2006.
[30].Yina. G. and Dawei Z., "Single channel surface electromyography blind recognition model based on watermarking", *Journal of Vibration and Control*, pp. 42-48,2012.
[31]. Pandey. A, Singh B. S, Singh. B. and Sood. N., "A 2D electrocardiogram data compression method using a sample entropy-based complexity sorting approach", *Journal of Computers and Electrical Engineering* Vol. 56, pp.30–45, 2016.
[32]. Rusyaizila. R. N. Zakaria and Sumari. P., "Privacy Issues in Pervasive HealthcareMonitoring System: A Review", *World Academy of Science, Engineering and TechnologyInternational Journal of Health and Medical Engineering*Vol:4, No:12, pp. 1913-1920, 2010.