RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ)
Research Paper

Review on ECG signal transmission and Hiding mechanisms

Dr. Shamsher Singh

SRPAAB College, Pathankot

Abstract:

Wearable ECG monitoring devices are becoming more prevalent as technology advances. A lot of private patient information is tracked and disseminated globally. Secret patient information must be safeguarded. Electrocardiogram signals can be used in a number of different ways to conceal the patient's confidential information. The two main goals of the entire procedure are a) to encrypt the patient data and b) to restore the original ECG signal. Health Insurance Portability and Accountability Act (HIPAA) regulations state that any dangers to the confidentiality and privacy of patient information must be avoided. This study examines various ECG steganography approaches for concealing patient-specific information.

Keywords: Electrocardiogram, steganography, watermarking.

1. Introduction

1.1 ECG Based Data Security

In the modern world, information may be disseminated in many ways with anyone, anywhere. In addition to developments that make information sharing simple, securing data from prying eyes or outside clients is of more relevance. Patient information is transmitted from one location to nearby emergency rooms in the medical profession so that the patient can be accurately perceived. This information is only important for his health records and impressions, therefore he must protect himself from other risks [12]. With the aid of the electrocardiogram (ECG) data, this ought to be doable [15]. The ECG is possibly one of the most beneficial demonstration tests in emergency care. The ECG serves as the basis for determining whether there is cardiovascular ischemia and is used to draw conclusions. These detours can be maintained in the waves known as P, Q, R, S, and T waves. P wave addresses depolarization in the vertical headings, as shown in Fig. 1. The Q wave demonstrates septal depolarization and handles a descending redirection [4]. In essence, the R wave represents ventricular depolarization, the S wave discusses late ventricular depolarization, and the T wave depicts ventricular repolarization [5]. These waves then follow the heart's actuations. A growing range of handy devices that record ECG exercises over time and transmit patient information remotely are becoming available as technology advances. Examples of these frameworks are Shine and Alivecor iPhone [6]. ECG sign data can be stored in a variety of organisations, including ecgML, XML-ECG, Philips XML, DICOM-ECG and so forth [7]

The demand for providing security to patient private information also grows as ease of information sharing and health monitoring increases. ECG steganography techniques provide a solution to this problem since they protect patient-specific information as it is transmitted between two remote locations [8].

1.2 Steganography

As innovations develops, observing patients at their home rather than emergency clinic is likewise increments, which luckily stifle the quantity of guests in a medical clinic. These Place of care (POC) procedures [9] can give a solid data about quiet's wellbeing and can be communicated to the master or specialists from anyplace whenever. Web stays the normal mechanism of sending this data which uncovers this data to certain dangers of correspondence

Numerous methods in view of cryptography have been developed in past to safeguard the information.

  ISSN: 2349-7637 (Online)

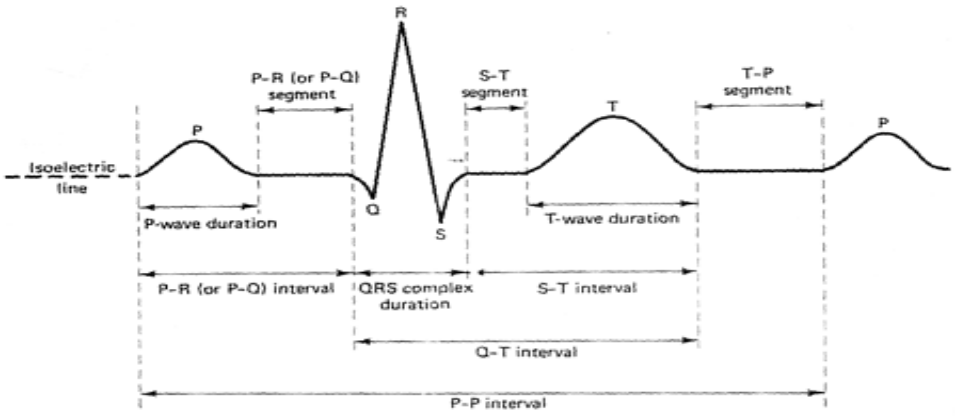

Fig.1. P, Q, R, S, and T wave of Electrocardiogram [5]

By using some encryption, these techniques provide the patient data with useful protection. Whatever the case, this resulted in sophisticated computational information that wasn't taken into account for POC procedures. Steganography, which hides data (now, patient data) [11] in another sign to protect it from potential threats, provides a solution to the aforementioned problem. As unique sign may be recovered from watermarked signal, this reduces generic information overheads as well. ECG steganography uses two distinct areas called Time area and Recurrence area. The latter can hide a huge amount of data but respects slower execution. On the other hand, Time area ECG steganography operates at a faster rate but stores less data [12]. information about a patient's health (such as an ECG signal, temperature, and so forth) can be obtained with the assistance of sensors. The collected data is subsequently sent to PDA [13] via some kind of interaction. Patient data is stowed away into an ECG signal using a transcription technique before the data is moved (involving ECG as host signal). The resulting watermarked signal [14] is then transferred through the web to the emergency room. This confidential data is successfully recovered at the collector end (clinic). As a result, overheads and the overall size of the encoded signal were reduced.

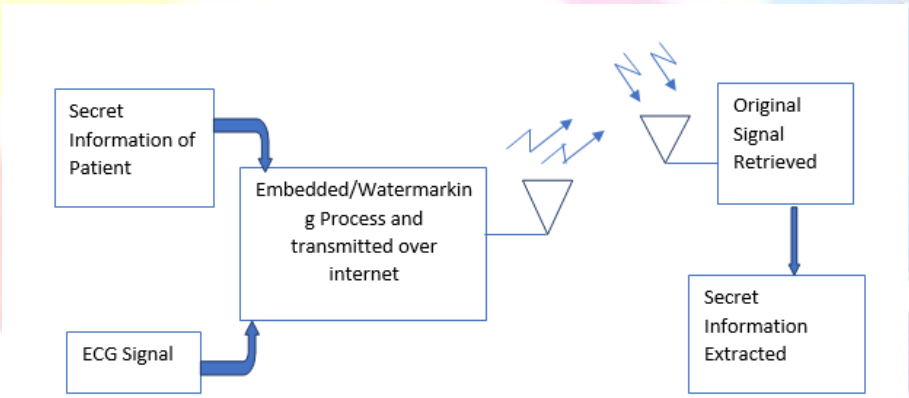

Fig.2. General Process of ECG Steganography

A block diagram of steganographic technique has been shown in Fig.2

1.3 ECG Data Encryption Measures

A secure transfer of patient information is guaranteed by a number of information encryption estimates. This includes both key responsiveness and key space examination. The goal of key space analysis is to provide a large number of key spaces that typically reduce the key. If the key is less sensitive to modifications, there is a potential that the patient's data will be helpless. As a result, it must be delicate to fend off any outside attack.

1.3.1 Limitations of ECG data hiding and encryption techniques

There are several techniques for protecting patient information from various threats. ECG signals can be used as a cover signal for similar phenomena, however there are still many areas that require concern. Following issues can in any case get to the next level:

- Choice of boundaries

- Recreation of unique ECG signal
- Contortion level in recuperated information.
- Inserting process
- Mistaken measures
- arbitrary way of behaving of mistake.
- Security Dangers
- Complex element extraction

The next section examines specific steganographic techniques where patient-restricted information is hidden with an ECG signal to send it securely from one location to another. The subsequent section clarifies the various phrasings used in steganography by using the electrocardiogram as a cover sign to conceal patient-specific classified data.

2. Related Work

*Ibaida. A. The stenographic method described in [15] involves walling in the patient's ECG data with the scope of unusual numbers at a few key locations. Fig. 3 illustrates the entire process of their strategy. The MIT-BIH Arrhythmia data set was used by them [16]. More authors concur that there are several (2.1475*109) combinations of amazing reach that can provide a very high level of information security. Creators achieved a small PRD for watermarked ECGs for both common and uncommon ECGs.*

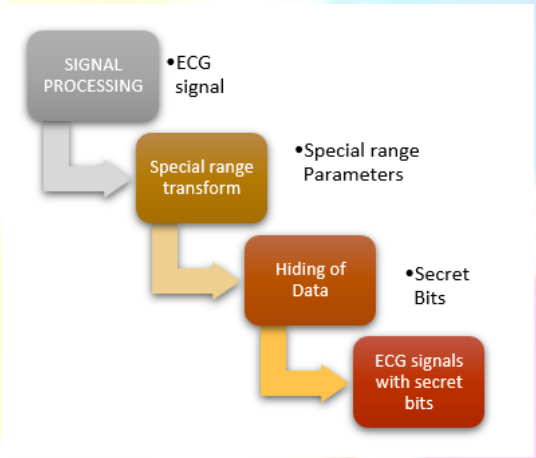

Fig.3. Process of hiding patient information with special number series

Today, POC (mark of care) devices that monitor an ECG patient's activities are used to consider the health of cardiac patients. In [17], Ayman Ibaida and Ibrahim Khalil developed a novel method to obtain the patient's information using wavelet-based ECG steganography. Their primary focus was on reducing the degree of ECG signal deformation (during steganography) in POC [9] systems. The overall agreement with the HIPAA security and protection requirements provides security for patient information [10]. Their system uses procedure XOR encoding, wavelet parcel disintegration (DWT), and implanting activity to encrypt patient information. With the help of a pre-shared key and scrambling grid, they are able to provide very good security. Additionally, watermarked ECG signal is transmitted to the receiving end (information obtained using wavelets). It is necessary to perform the inverse wallet deterioration and watermark extraction cycle in order to securely retrieve the initial information on the other end. They also conducted a convincing analysis of their method to determine how well the wavelet PRD and rate remaining contrast were utilised by the designer [18]. According to the creators, there is only 1% or less information mutilation in the data that was obtained, and scrambled data can be totally recovered.

Chen S. T. et.al in [19], offered a strategy to hide the patient's private information in light of change space quantization. In this study, the ECG data was watermarked to prevent patient data from being revealed. Different alterations, including discrete wavelet change (DWT), discrete cosine change (DCT), and discrete Fourier change (DFT), are incorporated during quantization[18]. More specifically, authors of this work developed a method considering quantization sound watermarking. Instead of sound signals, ECG flags were used for quantization. They installed the watermarks with the ECG data and used data from the MIT-BIH Arrhythmia data collection [15]. The proposed approach is successful, according to the creators, who claimed that the information obtained when compared to specific MIT-BIH Arrhythmia data set samples results in completely insignificant variety.

ISSN: 2349-7637 (Online)

Jerro S. T. et al in [20], Utilizing Quick Discrete Curvelet Change, an original ECG steganography technology was extended. Their technique includes: a) Preprocessing: In this step, 1D ECG signals are converted to 2D ECG images, and the corresponding curvelet coefficients are calculated. Additionally, a watermark in a double configuration is embedded with the image's curvelet coefficients. b) Limit determination; c) n*n grouping selection for watermarking. There is no information shortage and there is less sign twisting.

S. E. Jero et. al. [21] developed a cunning ECG steganography technique in which they use DCT to disintegrate signs and solitary worth decay to implant the patient's private information into the ECG signal (deteriorated).

They insert a 2D ECG image and watermark (using SVD) by replacing the sole benefit of the image with the benefit of the patient's data.

Using reverse DWT, it is possible to recover the privileged data. With a base error rate of 0.6%, this technology respects conceal sensitive information into ECG signals.

Chen C. Yang Wang F. W. is another In light of the coefficient arrangement, [22] presented an electrocardiogram (ECG) steganography approach. Two techniques were discussed by the creators: lossy and reversible steganography. Lossy steganography is further divided into high limit and quality categories.

ECG steganography is a reliable method for protecting patient data. Additionally, irreversible surgery can recover the initial indication while concealing something extremely similar. Additionally, creators recreated the two techniques and captured the results of several attacks on distinct watermarks. This tactic is effective in a variety of ways since it requires less time and respects more obvious computational speeds.

Wang H. et. al [23] described a method of protecting patient data that relies on reversible ECG storage. They also contradict the method employed because it is unable to completely replicate the original ECG data. In this study, the authors developed a method for implanting that maintains a high-quality image and another method to obtain the patients data in view of inserting scrambling.

Creators claimed to have higher installation limits and a 1% bending between watermarked and distinctive ECG signals. The two tactics can generally be reversed.

Yuan S. Additionally, et. al introduced an information concealing technique that relies on pixel value differencing in [24]. The fact that their technique is undetectable by RS attack and histogram assault raises the security level in a favourable way [25]. In their method, a picture (cover) is matched into a 1D pixel grouping by using Hilbert filling bend. This technique lessens the obvious antiquities and requires no memory to store implanted knowledge. Additionally, the provided embedded image has less editing.

3. Performance Evaluation Parameters

3.1 Mean Square Value

The proportion of similitude or the degree of offeror/mutilation between two signals is known as the Mean Square Error (MSE). MSE may also be regarded as a percentage of sign quality. Y is a special indicator of M forecasts and Y's considered signal. [26]

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

3.2 Peak Signal to Noise Ratio

The top sign to-commotion proportion (PSNR) is the ratio of the loudest possible pixel value to the loudest possible signal. It is primarily determined using a logarithmic scale, and its value is always expressed in db. MAX denotes the highest sign value.[26]

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

3.4 Percentage Residual Difference

The PRD (rate lingering contrast) gadget is used to measure the difference between an ECG signal that is authentic and one that has been watermarked. [25]

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

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

3.5 Bit Error Rate (BER)

BER can be measured as the number of errors that occurred relative to the quantity of pieces sent by a transmission system.

3.6 Wavelet Based Weighted Percentage Residual Difference (WWPD)

WWPRD depends on organic wavelet decay [25]. Numerically, it characterized as:

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

where Nm is the total number of subgroups, w' is the weight value related to subband j, and WPRD' is a representation of the wavelet-based rate lingering difference.

3.7 Root mean Square Error (RMS)

To identify the mutilation or error between the replicated signal and the actual sign, the Root Mean Square Error is used. It is described in mathematics as:

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

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

3.8 Quality Score

This boundary measure pressure according to the remaking mistakes. It is characterized as the proportion of Pressure proportion and PRD.

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

The presentation of pressure strategy is overwhelming on the off chance that it has better score [25].

4. Conclusion

Restricted patient information is stored and obtained when ECG impulses are implanted into it. To achieve two important aims, specific time and recurrence space ECG stenographic algorithms have been developed: (1) providing encryption to patient-restricted data; and (2) recovering unique sign after watermarking. The approaches connected to it were recovered in this work. The kind of Table.1 has finally come to an end. They depict the key elements of a few ECG strategies.

Table.1. Features of distinct approaches [15]

S.No	Reference	Features
1	[1]	• Compelling procedure for concealing patient information • Different combinations of extreme ferocity numbers that can protect patient information during transmission. • Modest amount of PRD
2	[2]	• Novel methodology of concealing patient information in view of wavelets. • Zeroed in on decreasing the bending level of ECG signals (during steganography) in POC frameworks.

		• Extremely less mutilation in the got information (< 1%) and encoded information is completely recuperated
3	[3]	• Approach in view of change area quantization to conceal the secret information of the patient. • procedure in view of quantization sound watermarking • truly unimportant variety in recuperated information.
4	[4]	• Successful methodology in light of DCT • Insert ECG picture (2D) and watermark (using SVD) by supplanting the solitary upsides of picture with the upsides of patient information. • least blunder rate
5	[5]	• steganography method for electrocardiogram (ECG) in view of coefficient arrangement. reversible steganography and lossy steganography. less baffling and recognisable computational speeds
6	[6]	• Reversible ECG stowing away method proposed observe the high visual nature of the patient information. 1% is all that separates the watermarked and distinct ECG signal increased insertion limit
7	[7]	• Opposite DWT • Least mistake rate in concealing privileged information of 0.6%
8	[8]	• Proposed approach pixel esteem differencing method which isn't detectable by RS assault and histogram assault. • Used utilizing Hilbert filling bend, a picture (cover) is matched into a 1D pixels grouping diminishes the perceptible relics • no memory necessity for putting away implanted information
9.	[9]	• Delineated about Remote body region organization • Recorded different clinical medical care gadgets like Wellbeing Stuff, Mobi Wellbeing, Ubimon and CodeBlue e.t.c. • Principal center around the security and protection issues connected with clinical Boycott and general remote sensor organizations.
10.	[10]	• compared new developments in medical care with those of remote clinical sensor groups (WMSNs). • developed clear-cut methods for assessing wellbeing and the risks to it in a company. • CodeBlue [7], Alert Net [13], UbiMon [14], MobiCare [16, 53], and STAIRE [55] were investigated for potential risks to patient data. • Reasons to be aware of the problems with symmetric cryptography, secure steering, security, and administrative style.
11.	[11]	• proposed a method for watermarking clinical images using the EZW computation. A novel way of watermark control is used as images move from low to high aim. 512 to 8192 bytes of the imprint signal were received with a PSNR of 35dB (between the original and watermarked image). This method uses 15% of the host image, which is an improvement over earlier research.
12.	[12]	• In light of the single channel electromyography blind acknowledgment model, watermarking • Reduce the need for complex circuitry. • reduces the quantity of noise in surface electromyography (sEMG). • The use of embedded watermarking eliminates the problem of source division

ISSN: 2349-7637 (Online)

		confusion for visually challenged people
13.	[13]	• proposed a strategy for 2D electrocardiogram (ECG) information pressure in light of a solid example entropy (SampEn). • Prepared to capture the semi-rare ECG data by identifying the relationships inside and between beats. • using the MIT-BIH arrhythmia data base. • increased pressure • minimal remake
14.	[14]	• focused on distinctive approaches and security challenges • frames after pints as conclusion: • Any third party may watch the video monitoring. • Given the patient's location and potential financial consequences, spam • Patient family's carelessness with regard to data security.

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 of Computer 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]. Ari S, Das MK, Chacko A. ECG signal enhancement using S-Transform. Comput Biol Med. 2013 Jul;43(6):649-60. doi: 10.1016/j.compbiomed.2013.02.015. Epub 2013 Apr 15. PMID: 23668340..
[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. Conference Intelligence Sensor Network and Information*, pp. 207–212, 2010.
[13]. J. M. García, E. Parada, V. Collantes and E. Casilari-Pérez, "A PDA-based portable wireless ECG monitor for 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 of IEEE EMBC*. pp 3891–3894, 2010.
[16]. Gupta, R., Mitra, M., Bera, J. (2014). ECG Transmission. In: ECG Acquisition and Automated Remote Processing. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1557-8_4
[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, "A novel systolic array implementation of: DCT, DWT and DFT", *IEEE Conference on Computer and Communication Systems*, 1990.
[19]. S. Chen, T. Guo, Y. Huang, H. Kung, W. Tseng and S. Tu, "Hiding patients confidential data in the 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.

  ISSN: 2349-7637 (Online)

[22]. C.Y Yang, and W.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", *Computer Security*, 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 Healthcare Monitoring System: A Review", *World Academy of Science, Engineering and Technology International Journal of Health and Medical Engineering* Vol:4, No:12, pp. 1913-1920, 2010.

  ISSN: 2349-7637 (Online)