Robust and highly secure technique for wireless body sensor network using sequence of ECG data

T.SANTHI VANDANNA[1], S.VENKATESHWARLU[2], K.VISWANATH[3]
[1]KLEF Deemed to be University, Vaddeswaram, Guntur (Dt), A.P, INDIA
[3]*Professor & HoD, Dept... of ECE, R.L.Jalappa Institute of Technology, Bangalore*

Abstract: - Lately, Random Binary Sequences (RBSs) are being computed using Heartbeat signals acquired from ECG and they are crucial for security purposes in wireless Body Sensor Networks (WBSNs). Presently, 128-bit RBSs in healthcare sector takes long computation time to be generated using ECG based heartbeat signals. To reduce the computation time, a novel technique for generation of RBSs using heartbeat's Interpulse Intervals (IPI) is proposed in this paper. In this paper, the technique uses generation of monotonic increasing, finite IPI sequences and encoding process using cyclic block to extract entropic bits in high numbers from each of the IPI. The dataset used for this paper were taken from Physionet Arrhythmia database. Using the proposed method, around 16 bits can randomly be extracted from each ECG heartbeat signal In order to produce RBSs of 128 bits by concatenating eight IPIs sequentially. Using the tests given in National Institute of Standards and Technology statistical (NIST) and the hamming distance function, the distinctiveness and randomness of the generated RBSs of 128 bits can be measured. The RBSs of 128 bits that are generated from the results of both patients and healthy subjects can be utilized as encryption keys or identifiers in order to protect the WBSNs. The method proposed has been observed to be better than the existing methods by being four times faster.

Key-Words: - Interpulse Intervals (IPIs), Heartbeats, Security, Wireless Body Sensor Networks (WBSNs), Random Binary Sequences (RBSs).

1 Introduction

The heart consists of four chambers, namely, left and right Atrium and left and right ventricles. The blood collected from all the organs of the body enter the right atrium from superior vena cava then the blood is pumped from the right atrium to right ventricle from where the blood is sent to the lungs through pulmonary artery for removal of CO2 from the blood stream. Later the oxygenated blood from the lungs enters the left atrium through pulmonary veins. The left atrium sends the blood to the left ventricle from where the blood is transported throughout the body through the aorta. Electrocardiogram (ECG) is a signal acquired from heart's resting and contracting state. The signal is obtained using three different electrode placement techniques wherein 12 recordings are obtained during a routine ECG technique. The ECG signal is periodic for every 0.8 seconds. It is indicative of any disorder of the heart and hence it is the most convenient form of indicator of cardiovascular functioning.

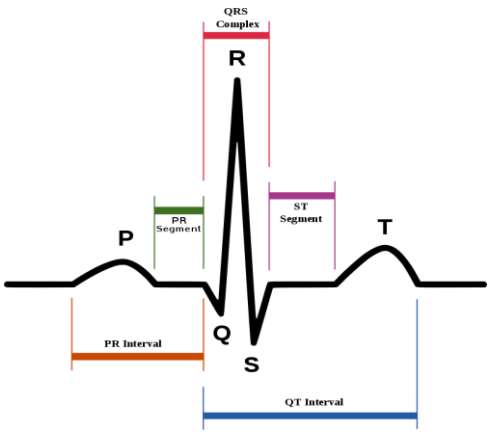

Fig.1 ECG signal components

A normal ECG rhythm consists of four waves, namely, P wave, QRS complex, T wave and U wave. Atrial depolarization is represented by the P

wave. It starts from the Sino-Atrial (SA) node till the Atrio-Ventricular Node which is from the right atrium till the left atrium. The depolarization of the left and right ventricles leads to the QRS complex in the ECG signal. The QRS complex normally has large amplitude because the ventricles are made of thick muscles because they have to withstand high pressure of blood entering through them and leaving the left ventricle. The repolarization of the ventricles leads to T wave. U wave is generally of very low amplitude and sometimes it is not considered while analyzing the ECG signal for any abnormalities in the heart. It is said to be due to the repolarization of interventricular septum.

There has been a steady increase in the usage of wearable technology devices in the past few years. Initially, they were connected through cables and wires, but lately due to advancement in wireless communication technology, there has been a rise in the usage of wireless wearable medical devices. When multiple devices are connected and transmit different physiological signals to a network such as Wireless Body Sensor Networks (WBSNs), there can be a security issue of the signals being hacked which can violate patient confidentiality rights. There have been various techniques that were developed in order to secure the transmission of biometric data, but there were many issues with them. Moreover, WBSNs have to be secure so as to deny access to patient data by unauthorized personnel according to the rule stated by the Health Insurance Portability and Accountability Act (HIPAA). Along with the above challenge of providing security, there are resource constraints in WBSN nodes such as battery requirement, processing capability and memory requirements. Hence, it can be seen that a balance is needed between consumption of resources by the sensor nodes and security of the medical data in WBSNs.

ECG signal monitoring has additional applications currently. They are not only for heart rate monitoring, measurement of rhythm to analyse diseases and health constitutions such as arrhythmias, sleep disorders, management of stress, and so on, but also used for Autonomic Nervous System (ANS) evaluation so as to help in diagnoses of various heart related diseases. Lately, there is a new area of application, that is, in biometric security. In this area, the ECG signals are said to have characteristics that are unique compared to other biometric signals. One of the characteristics is that they are robust during attacks to acquire data forcefully.

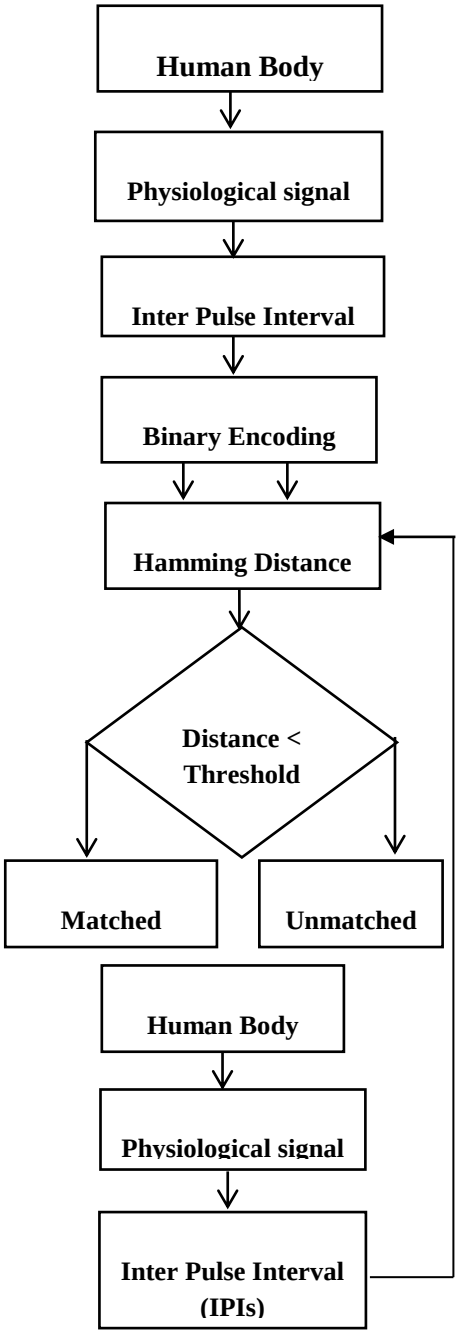

Fig.2 Block Diagram of Proposed IPI Matching Process

ECG signal can be used as the protection to deny access to the ECG data of the patient to anyone other than that person to whom the biometric signal belongs to ECG signals. Inter-Pulse Intervals (IPIs) of ECG signals are dominant choice when it comes to biometric security and efficient use of system resources because of the stringent requirements for operation of WBSNs. The intervals between two consecutive heartbeats also known as RR-intervals are given by IPIs. Synchronization of time is an important factor in order to communicate with the

nodes of sensors in WBSNs. A pulse is detected at the peripheral device after the QRS complex is constructed in the heart cycle. The IPIs in the other sensor nodes will be matched with one another after the biometric signal pattern's generation is started and it is emitted by the first sensor nodes which capture ECG signals. The communication between the sensors nodes get affected if the signal emitted from a node does not carry enough medical signal information. Hamming distance is most widely opted technique to detect errors in codes entering the receiver end, hence it is a preferred technique in the area of cryptosystems where in the binary sequences based on IPI can to test for uniqueness. This measurement is considered for the decision of applying RBSs generated to WBSNs for the purpose of security. The various security needs are, authentication of entities accessing the secure location or data, key agreement and secret keys. The system used by WBSNs using IPIs is shown in a block diagram as given in Fig.1.

2 Problem Formulation

F. Li et.al stated in their paper that Wireless Body Area Networks (WBANs) are used for to monitor the information from health-care sector and also to create a reliable and commonly used system of health-care. The collected data of WBANs are used for the process of determining which disease or condition exists and for treatment of the disease, and only permitted users can access the data. Hence, authorization, authentication and revoking of users from accessing the WBANs become a priority. The proposed system of the authors provides a robust singncryption method without a certificate. Their method achieves coded text authenticity along with integrity, confidentiality, non-rejection, public verifiability and authentication. The authors have concluded that the method used in their paper leads to less cost of computation and less consumption of energy by the controller.

D. P. Agarwal in his paper stated that advances in communication technologies as well as information technology made Internet of Things (IoT) emerge as the sought after technology. In the present health care sector, the IoT technologies are used for convenience of patients as well as physicians, because they have applications in various areas of medical field for example, management of patient information, monitoring in real-time and so on. One of the major technologies in IoT is the body sensor network (BSN) using which monitoring patients is possible with sensor nodes that are lightweight and wireless but it's development without consideration of security concerns will lead to misuse of patient privacy. In this paper, important security concerns in using healthcare system based on BSN were highlighted. S. Pirbhulal et.al,Body Sensor Network (BSN) is made up of several sensor nodes that monitor physiological signals of human body, such as Photoplethysmography (PPG), Electrocardiogram (ECG), Electroencephalogram (EEG) e.t.c. Confidentiality of data and security of the BSN system is of vital importance. Most of the existing methods of securing BSN use the techniques of generation of complex cryptographic key that requires high resources, time of computation, energy, memory and power during transmission of the data. It is essential for having BSN that uses computationally simple authentication methods and efficient use of energy. In this paper a new algorithm based on biometric signals was proposed that used Heart Rate Variability (HRV) for generation of simple key so as to protect the security of BSN. The proposed method of algorithm was then compared with three techniques of data authentication such as Rivest Shamir Adlemait n (RSA), Data Encryption Standard (DES) and Physiological Signal based Key Agreement (PSKA). The simulation of the algorithm was done using Matlab and their results showed the efficiency of their algorithm.

X. Liuet.al,stated thatvarious medical related applications are supported by wireless body area networks (WBANs) that contain wearable computing devices. Two important applications where WBANs are used in healthcare sector are security of vital biometric data that is transmitted over wireless channels and designing efficient medical management techniques. An efficient medical information management system was proposed in this paper and it was implemented on a WBAN test system that was based on Tinos. A new zero-watermarking method which is based on modified visual secret sharing (MVSS) was contained in biometric data bounded by the electronic medical record (EMR). The EMR is used for medical management and for checking data integrity. The EMR is secured using MVSS and is also encrypted and so is the biometric data. The results and analysis of this paper showed that their system protected the privacy of EMR and biometric data and also offered authentication of patient information, and healthcare operation verification process for WBANs.

G. Zhenget. al,stated that in cryptography, generation of random binary sequences is a necessary method. Binary Sequence (BS) consists of N bits in sequence where in each bit is a 0 or 1. Electrocardiogram (ECG) is used to secure sensors in Wireless Body Area Networks (WBANs) where, BS generation is based on ECG. IPIs are used to process BSes and they are taken from each heartbeat cycle. Generation of a 128-bit BS is done using IPI methods and it usually takes half a minute for the computation. To improve the computation time, this paper proposed an ECG Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm. Detection of the arrival time of these points such as P, Q, R, S, and T peaks is done using discrete wavelet transforms (DWT). RR, RQ, RS, RP and RT intervals and other time intervals are calculated using the arrival time information and they are used as features of ECG for generation of random BS. for authentication and security key usage, the randomly generated ECG BSes are used.

3 Proposed work

In this section we discussed about three major subtopics, one is to collect the ECG data from wearable hardware with better accuracy and we will remove of unwanted data. Second one is to extract the features from ECG data which can differentiate ECG data very easily.Third one is generation of RBS(random binary sequences) using ECG data.

3.1 ECG Measurement Using Hardware Platform

In this work we measured ECG signal from the wearable devices which is nothing but frontend ADI-ECG analog frontend.We acquired good quality signal and garanted simplified version of quality signal. The collected ECG data further used for generating 128-bit RBSs.

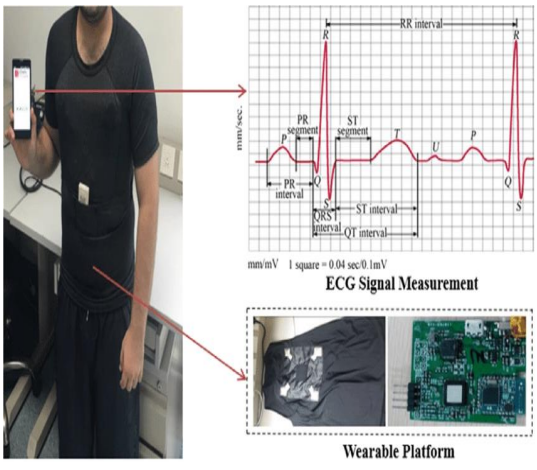

Fig.3 ECG Measurement using Hardware Platform

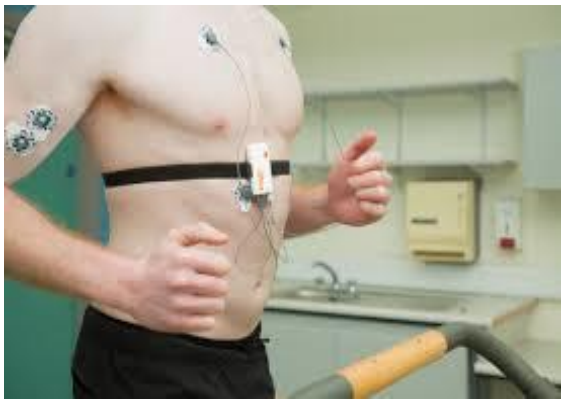

Fig.4 Sensors Directly Placed On Body for ECG Measurement

A signgle lead for ECG measurement detect rhythm and monitor it for measument of beat-to-beat heartrate as well as raspiratory rate. Various cardiac trends are analyzed using features of ECG data.

3.2 Procedure for Generation of 128 bit RBSs

There are in all 4 steps with the help of which we can generate 128 bit RBSs.

1. Exact R-Peak Calculation and Denoising
2. Sequence Generation which is Monotonic and Finite
3. Cyclic Encoding
4. Feature Extraction and its Concatenation

3.3.Exact R-Peak Calculation and Denoising

The most important and first step towards development is preprocessing and in this experiment preprocessing is the process of applying nonlinear transformation as well as filtering to remove unwanted data.

Output of the linear filters $F_L[n]$ to remove the unwanted data is given by

$$F_L[n] = \{E[n] - E[n-2]\} + \{E[n+2] - 2 * E[n] + E[n-2]\} \quad \ldots\ldots(1)$$

Where, $E[n]$ is a ECG data collected from wearable hardware.By above equation we can observe that linear filter output is combination of first and second derivative of original ECG data.Nonlinear Transformation is also the process of boosting high frequency amplitude of the ECG data by eradicting noise produced because of P and T deflections.

Squaring operator which is represented by 's[n]' gives the optimal output by $F_L[n]^2$. S[n] enhances the frequency of high frequency signals also its supresses the differenced arised due to P and T deflections. Output from the nonlinear transformation can be produced by moving window integration of s[n],

$$N_{LT}[n] = \frac{1}{N}\Big(s\big(n-(N-1)\big) + s\big(n-(N-2)\big) + \cdots \ldots + s(n)\Big) \ldots\ldots\ldots (2)$$

Where,'N' indicated the window width.

3.4.Sequence Generation which is Monotonic and Finite

First process to get inter pulse interval (IPI) from the individuals by heartrate.Once the IPI we got we can generate IPI based RBSs depending on some conditions.This algorithm thinks about to enlarge the decimal value of IPI. The IPI is monotonically increasing when the condition IPI(n+1) >=IPI(n) , gets satisfied.

3.5. Cyclic Encoding

To encode the obtained IPIs to a set of binary sequence there are different encoding techniques.In this work there is use of cyclic block encoding method is used to produce the set of binary sequences which are helpful to get significant randomness as well as it produces more bits extraction.

3.6.Feature Extraction and its Concatenation

This step is the major task in the development.Extraction of the binary bits from available IPIs is an imporatant task to get generate RBSs. Because of very low entropy value the Most Significant Bits (MSBs) of the IPI are not considered where as the LSB(Least Significant Bits). The extracted unique Sequence of the ECG data has the garanteed randomness.

4 Distinctiveness testing for RBS's

ECG provides distinct features which can be used for securing the data passed through WSBN(Wireless Sensor Body Network).There are different features such as peak amplitudes of P,Q,R,S ,T wavesas well as peak to peak intervals such as RR intervals are used to protect the data transmitted through WBSN.RBSs generated from RR interval in WSBN are mandatory unique and random.

4.1 Randomness Testing

Several tests are conducted to get randomness in generated IPI which are 128-bit RBS as follows,

a) Entropy Testing

The probability of generated IPI which is 128 –bit RBS can be calculated as given below,

$$H(x) = -\sum_{j=1}^{n} P(x_j) * log_2 P(x_j)$$

$P(x_j)$ indicates probability of getting jth event.

'X' is an information data present which is mutually exclusive to x1,x2,….,xn.

b) Statistical Testing

There are different types of statistical tests performed to get the randomness in the RBS generated. Some of the tests are discussed as below,

(R-Test) Run Test is the fluctuations in the zeros and ones in time series.

(F-Test) Frequency Test It provides zeros and ones ration to get satisfy the conditions.

(FFT-Test) Fast Fourier Transform Test it identifies is there any pattern adjacent to the another pattern which is periodic.

(C-Test) Cumulative Sum Test it find the random number in time series

(LC-Test) Linear Complexity Test it proves that generated random binary sequnce should be complicated enogh.

4.2 Distinctiveness Testing

The generated RBS from IPI should be distinct enough is the major condition. There is use of Hamming Distance(HD) which will give us the distinceion between any two random binary sequences.

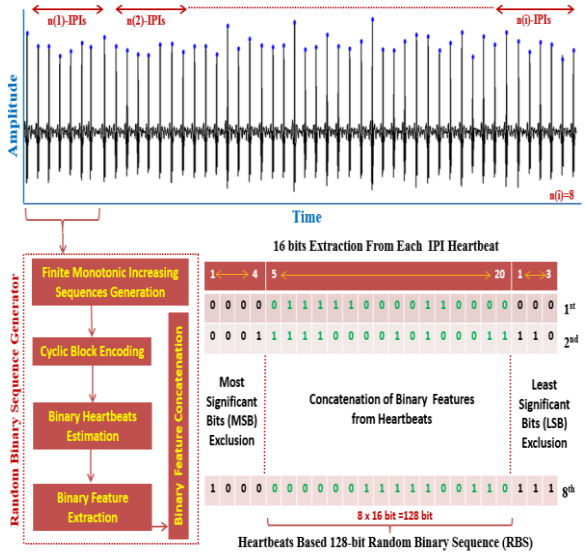

Fig.5 Procedure for Generation of 128-bit RBSs

5. Results and Discussion

The proposed design is successfully simulated for different datasets using MTALAB 2017a software platform and the simulated results are discussed in below

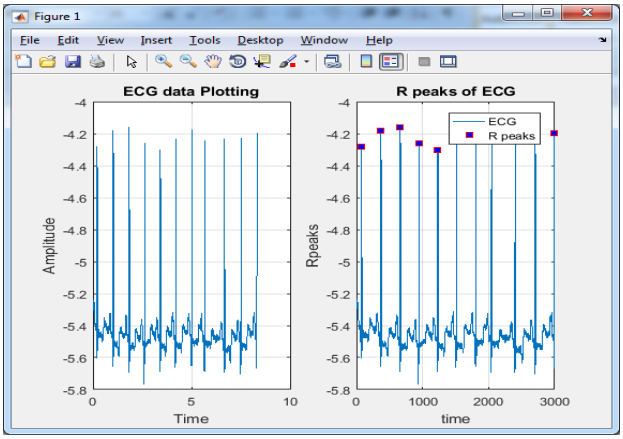

Fig.6 ECG input data and R-peaks detected

The Fig.6 to 12 represents input ECG data which is collected from physionet website (MIT-BIH database) for standard analysis. The highest positive peak in the signal is nothing but R-peak which is used for further analysis is calculated by simple Matlab coding. Blue-Red dark bounding boxes are used to plot R-peaks on ECG data.

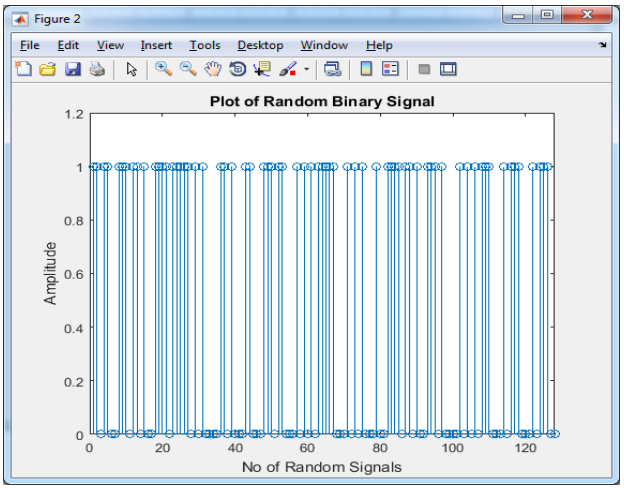

Fig.7 Simulated results of first sequence from Random Binary Sequence

It is the first sequence obtained from the RBS (random binary sequence) using 128bit RBS model.

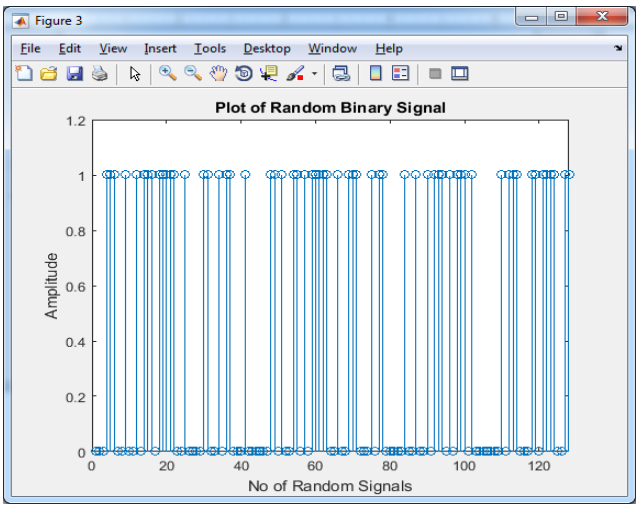

Fig.8 Simulated results of second sequence from Random Binary Sequence

It is the second sequence obtained from the RBS (random binary sequence) using 128bit RBS model.

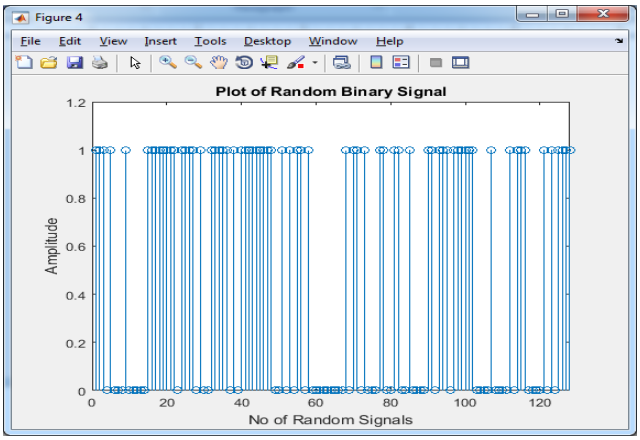

Fig.9 Simulated results of third sequence from Random Binary Sequence

It is the third sequence obtained from the RBS (random binary sequence) using 128bit RBS model.

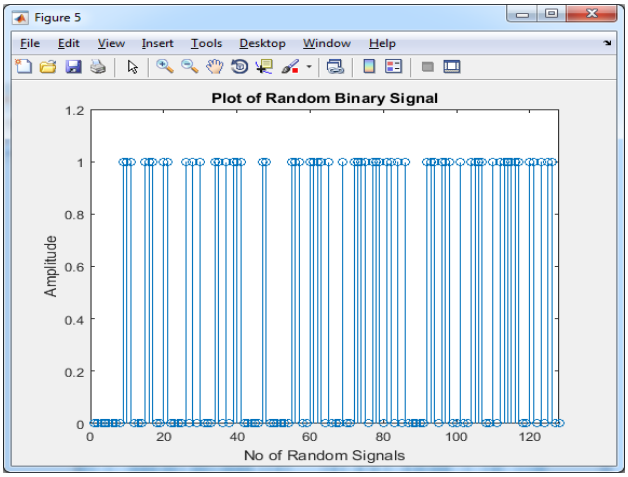

Fig.10 Plot of Random Binary Sequence

It is the fourth sequence obtained from the RBS (random binary sequence) using 128bit RBS model.

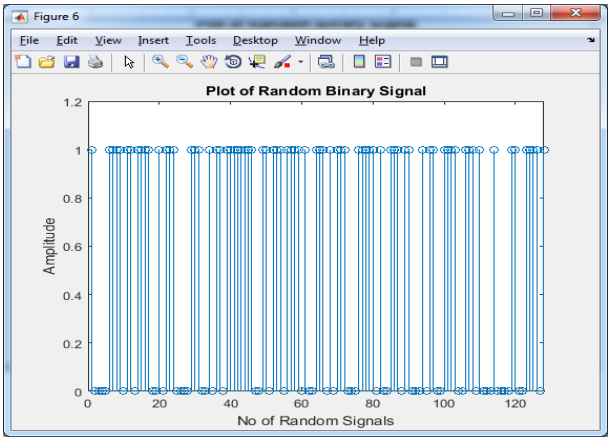

Fig.11 Plot of final Random Binary Sequence obtained from generated sequences.

It is the sum of all sequence obtained from the RBS (random binary sequence) generated using 128bit RBS model.

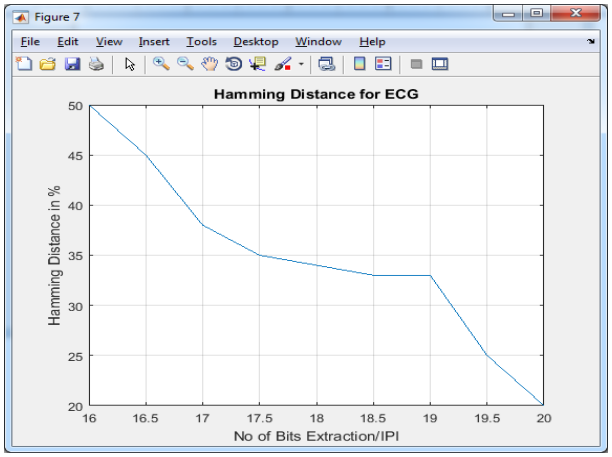

Fig.12 No of Bits Extracted/IPI vs. Hamming Distance (in %)

Above figure represents graph of no of bits extracted per IPI vs. hamming distance. As number of bits extracted increased from a limit of 16 bits per IPI, the hamming distance also decreases gradually.

5.1 Time consumption Comparison

Time taken to generate improved the random binary sequence with 128 bit takes very negligible time compared to the state of art techniques. So compared with state of art technique proposed work is having very low time complexity.

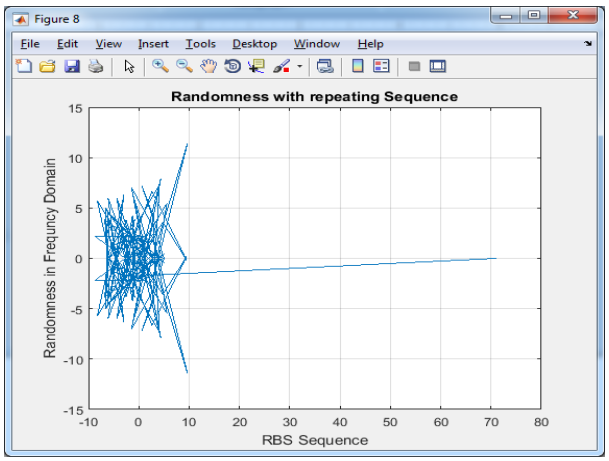

Fig.13 Randomness with repeating sequence

Randomness in the image shows that the data encrypted is very difficult to extract.

6 Conclusion

An improvement of the existing RBSs generation based on heartbeat has been proposed in this paper. The technique of using eight consecutive heartbeats to generate RBSs of 128 bits by application of IPIs has been analyzed. The time taken to encode and process of generating heartbeat based RBSs have been improved in order to apply it for healthcare applications based on WBSN. By utilizing NIST tests and Hamming Distance based distribution, the distinctiveness and randomness of the RBSs have been examined. By extracting 16bits from IPIs, better RBSs have been. Moreover, the proposed method performs better than previous attempts when more than 16 bits are extracted from each biometric signal.

References

[1] "TinyRNG: A cryptographic sporadic wide mix generator for faraway sensors plan center centers" Provided by strategies for A. Francillon and C. Castelluccia. Ceaselessly 2007.

[2] " Key based EKG totally information body in sensor structures" Implemented by Venkatasubramanian K , Banerjee. An, and Gupta. S Continually 2008.

[3] "Heart-to-coronary heart (H2H): support for inserted accommodating contraptions" Published by utilizing Rostami. M, Juels. An, and Koushanfar. F In the year 2013.

[4] , "Using the engineering estimations as beats of a substance to identifier sensor check chart orchestrate" Implemented by. Poon. C, Persistently 2008.

[5] "IMDGuard: Securing implantable medicinal contraptions with the out of entrances wearable gatekeeper" Produced by utilizing Qin. Z In this yr 2011.

[6] "A story biometrics methodology to confirm remote body a sensor the domain structures and telemedicine for m flourishing" Implemented by procedure for Bao. D Relentlessly 2006.

[7] "Biometric underwriting using uproarious electrocardiograms got by accommodating sensors" Published with the guide of H. Choi S. besides, Lee. B, Yoon. S Constantly 2016.

[8] "Definite ECG Studies of Multiple Point Fiducial Based Sequence Binary in Generation Algorithm E-Health Sensor Platform" Produced by Saleem. K, Abbas. By this a year 2016.

[9] "Plan of loose up based ECG biometric validation as body sensor zone structures" Implemented by procedure for S. Die down, Prata. B Reddy, Momtaz. F In this a year 2016.

[10] " Biometrics as Electrocardiogram in flag attesting Wireless Body Area Network. Dissipated through S. N. Ramli, Ahmad. R, . In the hour of 2013.

[11] "Diverse ECG Fiducial Points-Based Random Binary Sequence Generation for Securing Wireless Body Area Networks" Implemented by G. Zheng, G. Tooth, R. Shankaran. In this yr 2017.

[12] "Assessment make self-determined twofold game-plans for confirming remote body sensor structures" Produced with the guide of C. Poon. C and. Persistently 2012.

[13] "A cryptographic key association answer for HIPAA confirmation/thriving suggestion" Implemented with the guide of W.- B. Lee, and C.- D. Lee. In the yr 2008.

[14] "A comparable research of cushioned vault commonly based thriving systems for blocked off body sensor structures" Implemented by techniques for Pirbhulal. S, Zhang. H, W. Wu et al By the year 2016.

[15] "A Secure Medical Information Management System for Wireless Body Area Networks" Published by technique for Liu. X, . Ge. In the yr 2016.

[16] " A talented biometric-based figuring using beat change for asserting body sensor" Produced by system for Pirbhulal,. S. Zhang. H, By the year 2015.

[17] "BSN-Care: A Secure IOT-Based Modern Healthcare System Using Body Sensor Network" Implemented by P. Gope and T. Hwang. In the 2016.

[18] " VLSI Implementation of a Cost-Efficient Micro Control Unit With an Asymmetric Encryption for Wireless Body Sensor Network", Provided with the guide of S.L. Chen, M.C. Tuan. Reliably 2017.

[19] " Network area Personal and Applications. Social protection " Produced by D.P. Agrawal. Inside the yr 2017.

[20] "Valuable Control for underwriting less Wireless Access Networks Area Networks" wrapped up by methodologies for J. Hong and F. Li in a year 2016.