International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

An Inter-Pulse Interval Based Security Mechanism for Wireless Body Area Networks (WBANs)

Yash Mundra[1], Anil Kumar[2]
[1]Research Scholar, [2]Assistant Professor
[1,2]Department of Computer Science and Engineering, Oriental University, Indore (M.P.)

Date of Submission: 25-12-2020 Date of Acceptance: 31-12-2020

ABSTRACT: Wireless Sensor Networks and its different categories are being extensively used for widespread applications such as large scale industries, automation, weather monitoring, disaster management, defence etc. More lately, wireless body area networks (WBANs) or Wireless Body Sensor Networks (WBSNs) have come up as a category of WSNs which are a category of WSNs which are WSNs in the periphery of the human body. It is again being extensively explored for bio-medical and defence applications [1]. However, one serious challenge which the WBANs face is the fact that due to limited memory and processing power, WBANs face a limitation of not being able to support complex encryption techniques for securing the data exchange among the WBAN. Off late, biometric security has been explored for securing the WBAN data transfer. Again limitations of limited hardware availability and compatibility, choices are very limited for the biometric approach [2]-[3]. In this paper, an IPI based WBAN architecture is designed which utilizes the MIT-BIH database (MIT-BIHdb) [1]. A Discrete Time Markov Chain (DTMC) model has been implemented with multiple transitional states. The evaluation has been carried out by evaluating the entropy and hamming distance. It has been shown that the proposed technique attains better results both in terms of hamming distance and entropy compared to previously existing techniques.

Keywords: Body Sensor Networks, Inter Pulse Interval (IPI), Random Bit Stream (RBS), Markov Process, Hamming Distance, Entropy.

I. INTRODUCTION

Off late, wireless body area networks (WBANs) are being extensively used for varied applications primarily which are disaster management, bio-medical and defence. Some typical applications along with their implementation modes are shown below.

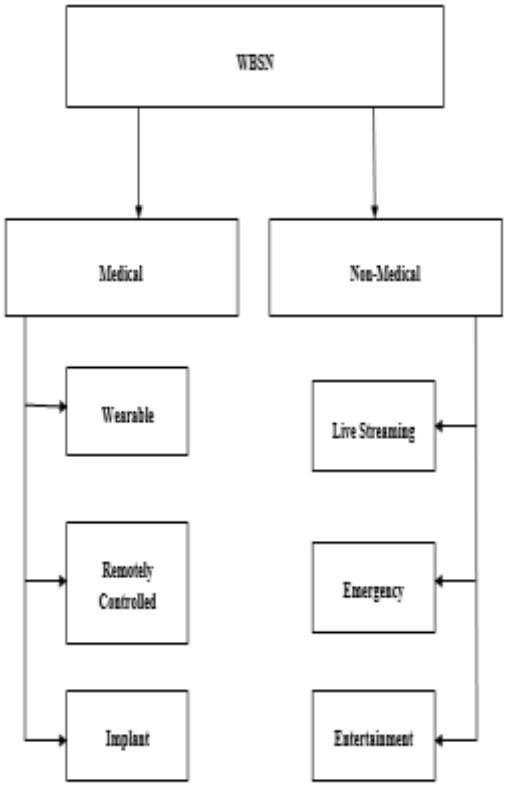

Fig.1 WBSN Categorization

The basic categorization has been done based on medical and non-medical applications. The major challenge however lies in the fact that WBANs have low or limited memory and computational resources [4]. This is majorly done to reduce the bulkiness and cost of a wide spread WBSN. Hence, sophisticated encryption mechanisms are summarily ruled out form being used for securing data transmission [5]-[6]. The other facet of securing networks is the use of biomedical features which are becoming popular. Off the, the ones which have least complexity and bulkiness need to be considered [7]. The other

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

aspect is the need for reliability. Using the electrocardiogram (ECG) of humans and using it's inter pulse interval (IPI) for securing WBAN data transfer is a promising avenue. The following figure depicts the concept.

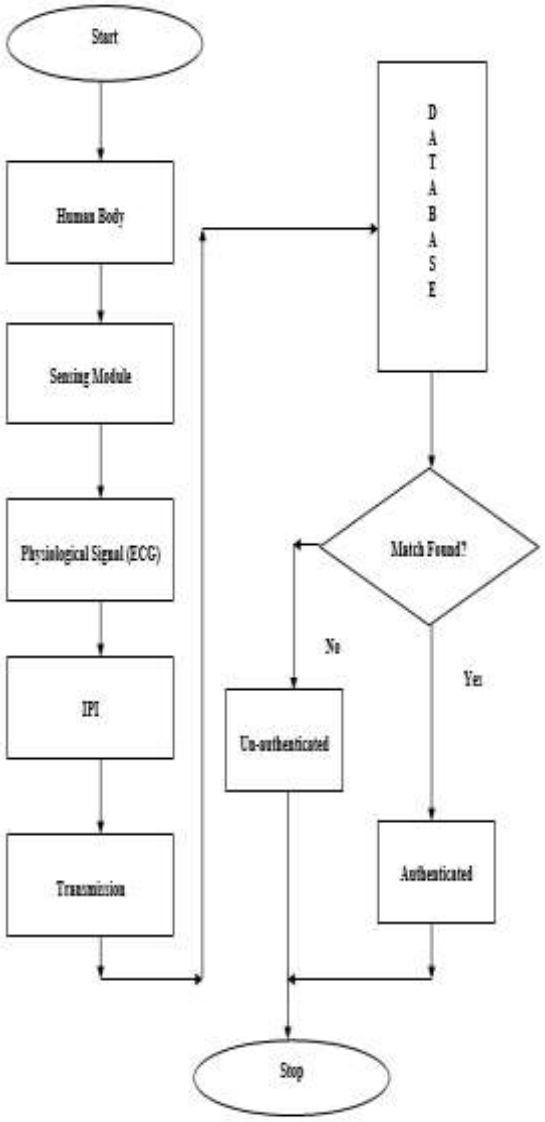

Fig.2 The IPI based security architecture for WBANs

The salient features of the IPI based security architecture are discussed in the subsequent sections. The physiological signal from the human body is the electrocardiogram (ECG) [8]-[9]. The electrocardiogram is the regular signal generated by the human heart which is depicted in figure 3.

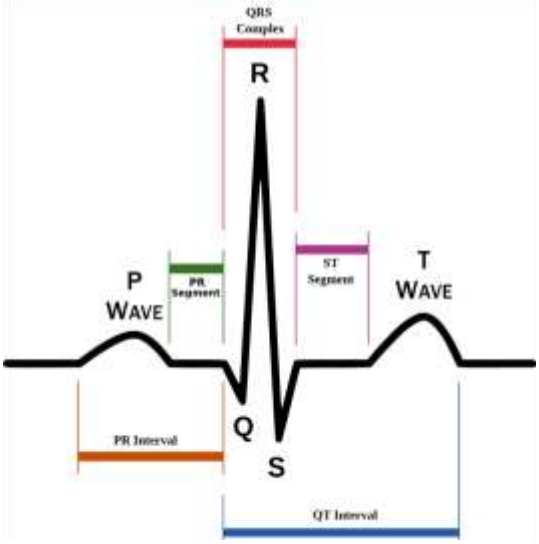

Fig.3 A Typical ECG Wave

The ECG wave is a regular pattern comprising of the P,Q,R,S, and T waves respectively. The inter-pulse interval or the IPI is computed between two consecutive pulses of the ECG. The IPI can be estimated utilizing either of the following intervals:

1) PP
2) QQ
3) RR
4) SS
5) TT
6) QRS-QRS

The above parameters are often termed as the features of IPI. However, prior to the evaluation or extraction of the features, data pre-processing needs to be done.

II. DATA PRE-PROCESSING AND FEATURE EXTRACTION

The ECG is generally very sensitive to noise and disturbance effects while capturing, storage and transmission synonymous with almost all common physiological signals. The most common types of noise and disturbance encountered in using the ECG signal as the physiological signal are the following [10]-[11]:

1) Power Line Interference
2) Baseline Drift
3) EMG (muscle contraction)
4) Motion Artefacts.

It has been found that the above disturbances are primarily in the low frequency range of 50-60 Hz. Hence its necessary to filter them out. The mathematical model for the same is implemented by employing a high pass filtering (HPF) mechanism given by:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

$\mathbf{H(f) = k; f \geq f_L (1)}$
$\mathbf{H(f) = 0; f \leq f_L (2)}$
Here,
f_L represents the higher cut-off frequency
k is a constant
F represents frequency
H represents response
H(f) represents frequency dependent frequency response

A graphical representation for the same is shown:

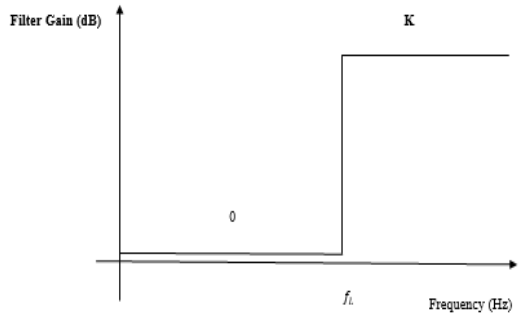

Fig.4 Typical HPF response

The feature extraction phase is extremely challenging and critical for the random binary stream (RBS) generation [12]. The feature extraction stage comprises of two fundamental operations i.e.

1) Peak Detection
2) Interval Computation

The peak detection phase is identifying the samples among the pre-processed data which can be touted as peaks, for which the mathematical condition used is:

$\mathbf{S_{k-1} < S_k > S_{k+1}}$ **(3)**

Here,
S_k is a present sample
S_{k+1} is a subsequent sample
S_{k-1} is a subsequent sample

Now, this relation may often render false positives due to the fact that the evaluation of peaks is often erroneous in nature due to variations in amplitudes. To rectify this, the squaring operation can be useful in increasing the difference among peaks. It is mathematically given by:

Le the sample state take up a discrete time scale of S_n
Here,
$\mathbf{S_n \epsilon [S_1, S_2 \dots \dots \dots S_n] \forall n}$ **(4)**
n is the number of elements in the sample space.
Let the difference in the amplitudes of the peaks be given by the first difference operator:

$\mathbf{\nabla_n = S_n - S_{n-1}}$ **(5)**

Now considering the fact that the squaring difference would yield larger differences compared to the linear differences, we obtain:

$\mathbf{\nabla_n^2 = S_n^2 - S_n^2}$ **(6)**

The evaluation of the peaks becomes more accurate since the following relation holds true for the monotonic increase of the square function:

$\mathbf{\nabla_n^2 > \nabla_n}$ **(7)**

The most reliable is however the RR or QRS based IPI evaluation due to higher strength compared to the other peaks.

III. PROPOSED APPROACH

3.1 Random Bit Generation

The random bit generation is often termed as the RBS (Random Bit Stream) generation which can be implemented by invoking the Discrete Time Markov Chain (DTMC) in honour of Andrie Markov. The DTMC is characterized by the property that the RBS of indexed in discrete time index (n) with the future indices being independent of past indices give the present index.
Let the discrete time space of **T** be **N** (discrete time) for the continuous time space [0,∞]. Thus

$\mathbf{T \in [0, \infty]}$ **(8)**

If the index is sampled with a sampling period of T_s, where it satisfies the Shannon's condition,

$\mathbf{\frac{1}{T_s} \geq 2f_m}$ **(9)**

Where,
T_s is the sampling time
f_m is the maximum frequency of the samples
Then considering T_s=1, we obtain the DTMC stream as X_n which is given by:

$\mathbf{P(X_{s+t} \epsilon A | F_s) = P(X_{s+t} \epsilon A | X_s) \nabla s, T \in U}$ **(10)**

Here,
X represents a state
s is the time metric
t is a delayed metric
P is the probability space
A is the state space
Xs is a previously existent state
U is the universal state of spaces
Considering the State Space vectors S_1&S_2 being given by:

$\mathbf{S_1 = X_s}$ **(11)**

And

$\mathbf{S_1 = F_s}$ **(12)**

If the conditional probabilities of Fs and Xs are same, it indicates mutual exclusiveness of the future and past DTMC states. This is clearly in accordance with the mathematical definition of DTMC clearly given by the dummy variable substitution:

$\mathbf{P\left(\frac{D}{S_1}\right) = P\left(\frac{D}{S_2}\right)}$ **(13)**

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

Where,

$$\mathbf{D = X_{s+t} \epsilon A} \quad \textbf{(14)}$$

The entire process can be summarized in the proposed algorithm

3.2 Proposed Algorithm

The data is extracted from MIT-BIH db. The raw ECG data is then processed and filtered using the high pass operation mathematically given by:

Let

y(t) denote the output of the filter,

x(t) denote the raw ECG signal and

h(t) denote the impulse response of the filter. Then:

$$\mathbf{y(t) = x(t) * h(t)} \quad \textbf{(15)}$$

where * denotes convolution in the time domain.

It should be noted that the sampling frequency of the filter should follow the Nyquist criteria i.e.

$$\mathbf{f_s \geq 2f_m} \quad \textbf{(16)}$$

Here,

fs denotes the sampling frequency and

fm denotes maximum frequency

Next the squaring operation is employed to increase the first difference method (DOM).

$$\mathbf{Sqr_{sig} = [y(t)]^2} \textbf{(17)}$$

Where,

Sqr_sig is the signal obtained after the filtering operation.

The 2nd difference operator is employed to yield the metric $\mathbf{\nabla_n^2}$ which results in the computation of the IPI vector.

Further, the RBS is generated using the DTMC given by:

$$\mathbf{X = [X_1, X_2 \ldots\ldots\ldots\ldots\ldots\ldots X_n]} \quad \textbf{(18)}$$

The multi transition DTMC is employed in this process which performs better than the single transition Markov chain.

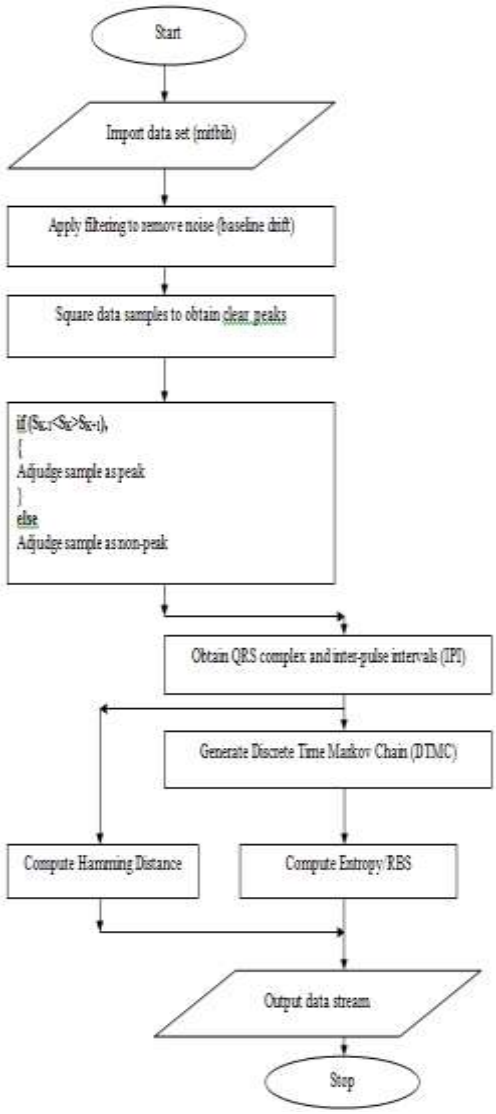

Fig. 5 Flowchart of Proposed System

Subsequently, compute the hamming distance (H) and Entropy (E)

Given two vectors u, v ∈ F n, the hamming distance

between u and v, d(u, v), to be the number of places where u and v differ. Mathematically,

$$\mathbf{H = |U| - |V|} \quad \textbf{(19)}$$

The entropy is computed for the random process as:

$$\mathbf{H(X) \triangleq -\sum_{x \in X} P_x(x) log[P_x(x)]} \textbf{(20)}$$

Here,

H is the entropy

X is the random variable

x is any value that the random variable can attain

P is the probability

log represents the logarithm to the base 2.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

IV. RESULTS

The results obtained are enunciated subsequently. The files of the raw data are loaded in the form of .mat files and processed further. The MIT-BIHdb is used for the purpose.

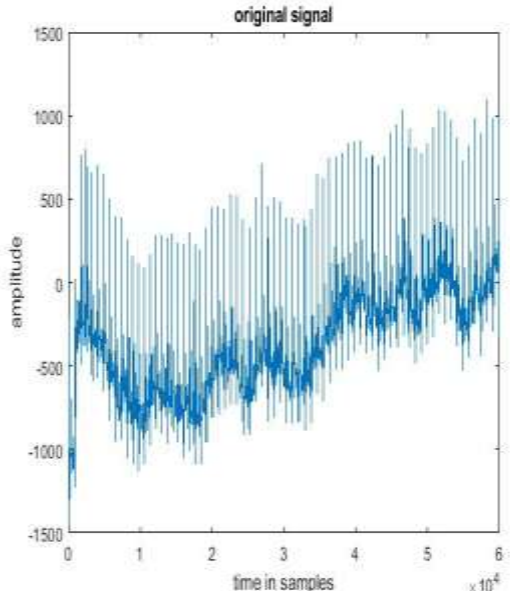

Fig.6 Original Data Sample

The figure above depicts the original data sample with the noise or the baseline drift.

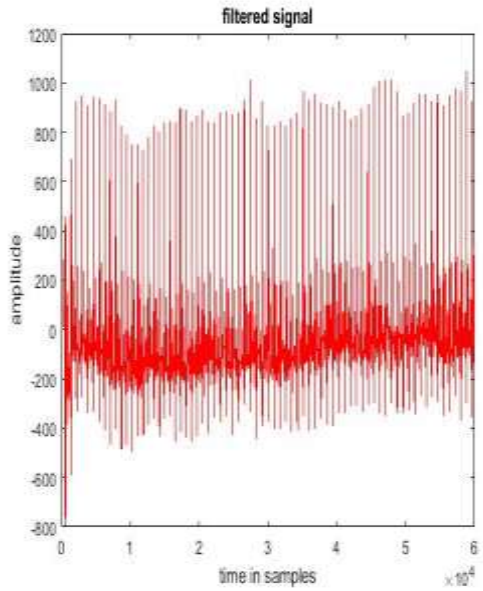

Fig.7 Filtered Data Sample

The figure above depicts the data samples after filtering out the baseline drift.

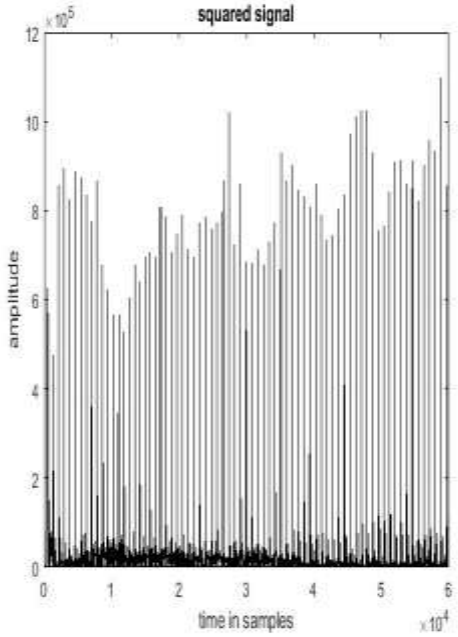

Fig.8 Squared Data Sample

The figure above depicts the squared version of the data samples. It makes easier to detect the peaks.

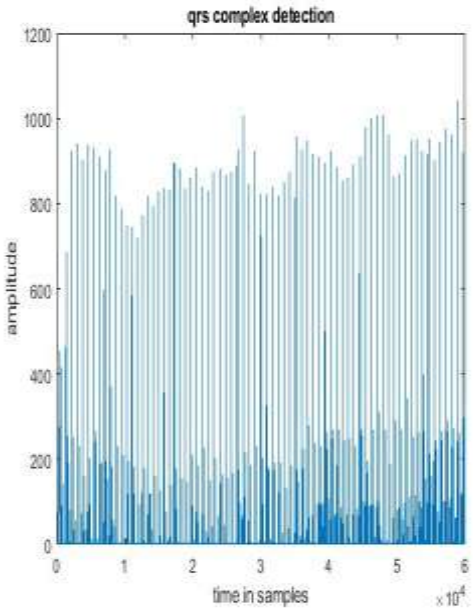

Fig.9 QRS Complex Detection

The figure above depicts the QRS complex that is detected.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

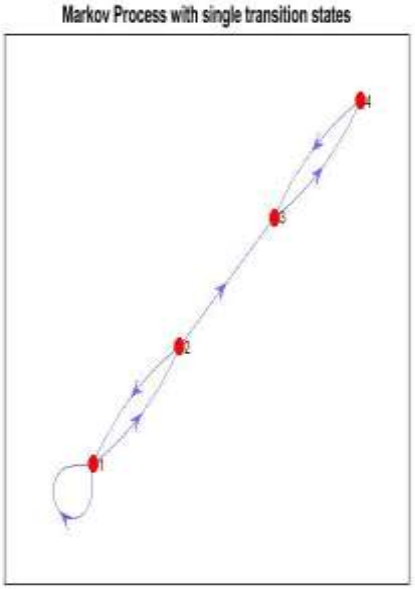

Fig.10 Single Transition Markov Chain

The figure above depicts the transition states of a discrete time Markov Chain with single transitions.

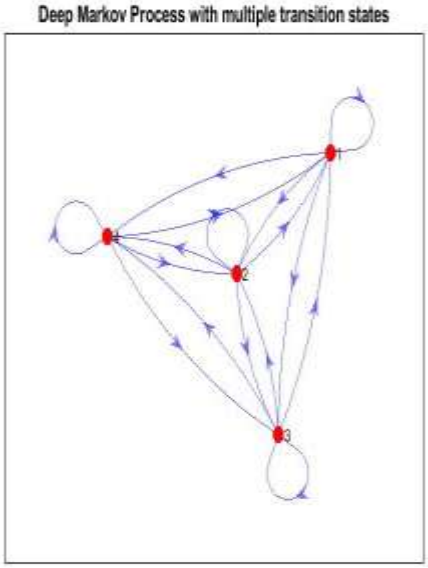

Fig.11 Multiple Transition Deep Markov Chain

The figure above depicts the deep Markov chain with possible multiple transitions.

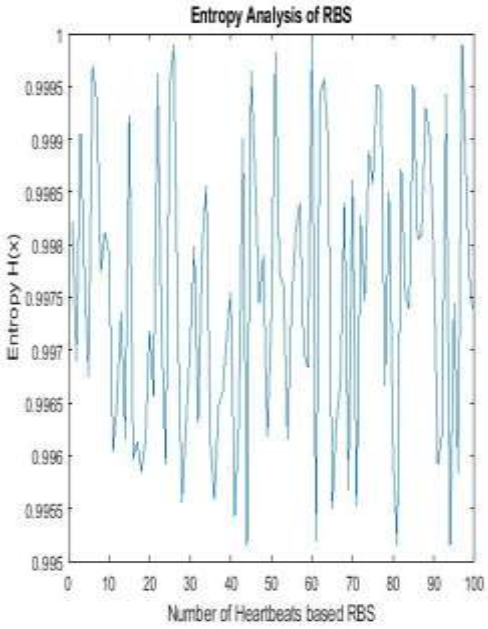

Fig.12 Variation of Entropy w.r.t. RBS

The figure above depicts the variation of the entropy as a function of the RBS generated.

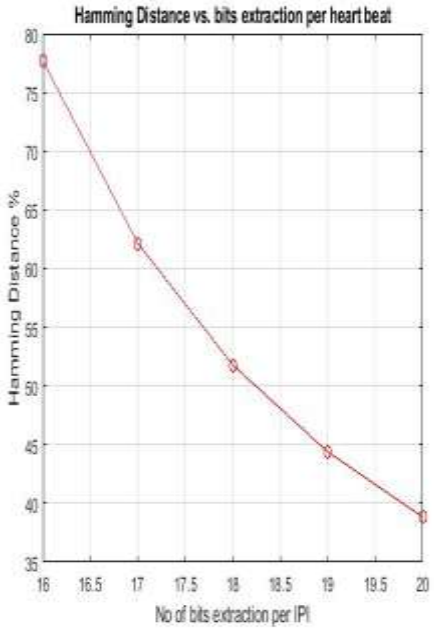

Fig.10 Variation of Hamming Distance w.r.t. No. of extracted bits/IPI

The figure above depicts the variation of the Hamming distance as a function of the number of bits extracted per IPI

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 712-718 www.ijaem.net ISSN: 2395-5252

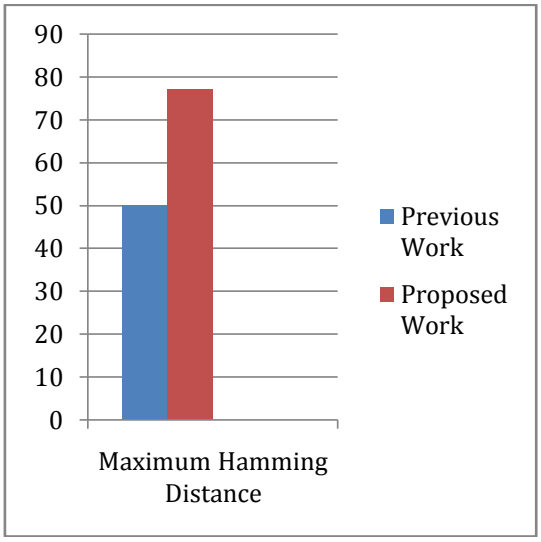

Figure.11 Comparative Hamming Distance Analysis

The figure above depicts the comparative hamming distance of previous work and proposed work

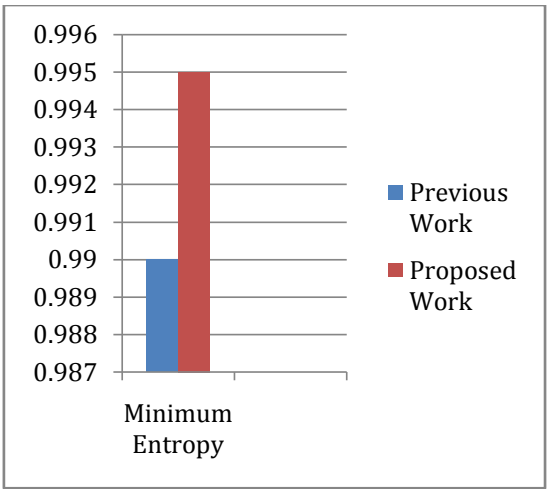

Figure.12 Comparative Entropy Analysis

The figure above depicts the comparison minimum entropy of previous and proposed work

CONCLUSION

The paper presents an approach for RBS generation using the DTMC that would help to secure WBAN data transfer. Pre-processing of the data is done using high pass filter operation. It can be observed from the previously furnished mathematical model and corresponding results that the proposed technique achieves better results compared to previously existing techniuqes [1]. While hamming distance is a measure of the distinctiveness among the different bit streams, the entropy indicates the average information content of the ransom bit streams. An enhancement in both the parameters indicates the efficacy of the proposed technique.

REFERENCES

[1]. Sandeep Pirbhulal, Heye Zhang, Wanqing Wu, Subhas Chandra Mukhopadhyay, "Heart-Beats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks", IEEE 2018

[2]. Peyman Dodangeh, Amir Hossein Jahangir, "A biometric security scheme for wireless body area networks" Elsevier 2018

[3]. AmelArfaoui, Asma ben Letaifa, Ali Kribeche, Sidi Mohammed Senouci, Mohamed Hamdi, "A Stochastic Game for Adaptive Security in Constrained Wireless Body Area Networks" IEEE 2018

[4]. Amit Samanta, Sudeep Mishra, "Dynamic Connectivity Establishment and Cooperative Scheduling for QoS-Aware Wireless Body Area Networks" IEEE 2018

[5]. X Li, MH Ibrahim, S Kumari, AK Sangaiah, V Gupta, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks", Elsevier 2017

[6]. Z Li, H Wang, M Daneshmand, "Secure and efficient key generation and agreement methods for wireless body area networks", IEEE 2017

[7]. AA Omala, KP Kibiwott, F Li, "An efficient remote authentication scheme for wireless body area network", Springer 2017

[8]. N Yessad, S Bouchelaghem, FS Ouada "Secure and reliable patient body motion based authentication approach for medical body area networks", Elsevier 2017

[9]. D He, S Zeadally, N Kumar, JH Lee, "Anonymous authentication for wireless body area networks with provable security" IEEE 2016

[10]. H Moosavi, FM Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks", IEEE 2016

[11]. C Hu, H Li, Y Huo, T Xiang, "Secure and efficient data communication protocol for wireless body area networks" IEEE 2016

[12]. MH Ibrahim, S Kumari, AK Das, M Wazid, "Secure anonymous mutual authentication for star two-tier wireless body area networks", Elsevier 2016.