Int J Pharma Bio Sci 2017 October; 8(4): (B) 159-165

Original Research Article Bioinformatics

International Journal of Pharma and Bio Sciences

ISSN
0975-6299

GENERATION OF BIOMETRIC SEQUENCE USING REAL TIME ELECTROCARDIOGRAM SIGNAL

[1]SRIKANTH MADIREDDY, [2]MOHANA.J, [3]C.KEERTHIKANTH AND [4]P. SRIHARI REDDY

[1,3,4]Student, ECE Department, Saveetha School of Engineering, Chennai.
[2]Assistant professor, ECE Department, Saveetha School of Engineering, Chennai

ABSTRACT

The prime aim of the paper is to generate a biometric key using real time electrocardiogram (ECG) signal. The advancement of body area network made the patient to be treated from anywhere. In such networks, it is important to see the data is authorized by the specific person. The data should be monitored to remain protected. To transmit the data from one node to another node or from one node to master node the data should be encrypted. For encryption, there should be key. In this paper, a key will be developed using real time electrocardiogram signal. From one person to another person the heartbeat will differ. RR variability where R is a point corresponding to the peak of QRS complex of the ECG wave and RR is the interval between successive RS and heart period variability. From the ECG wave the RR intervals are extracted and the difference between the RR intervals is taken and it is converted into binary format. By considering the ECG signal of different persons different keys can be developed and it will be random. These randomly generated ECG sequences can be used as security keys for encryption or authentication in a WBAN system.

KEYWORDS: ***Electrocardiogram(ECG), Wireless body area network(WBAN)Module, ADC, Zigbee.***

SRIKANTH MADIREDDY*

Student, ECE Department, Saveetha School of Engineering, Chennai.

Received on: 17-07-2017
Revised and Accepted on: 31-08-2017
DOI: http://dx.doi.org/10.22376/ijpbs.2017.8.4.b159-165

INTRODUCTION

Electrocardiogram (ECG) is a tool used to measure abnormalities present in the functioning of the heart. It is a recording of the bioelectrical activity of the heart representing the cyclical contraction and relaxation of atrium and ventricle. The most important features of the ECG include the information lying in the P, Q, R, S, and T waves corresponding to atrial and ventricular de-polarization or repolarization. The heart can function too fast, too slow, or with an irregular rhythm[1]. A heartbeat that is too fast is called Tachycardia. A heartbeat that is too slow is called bring together the better of the two worlds. Biometrics guarantees the identification of individuals based on measuring their personal unique features with a high degree of assurance, while cryptography mainly assures a high degree of trust in the transactions of information through the communication channel. The thought of combining both cryptography and biometrics is developed to have a security of data[2]. The data that is transferred should be monitored by the only authorized person. In case if the data is modified by the unauthorized person the patient life will be danger.[3] Therefore authentication is very important in Biometrics. The basic ECG signal is shown in the below Figure.

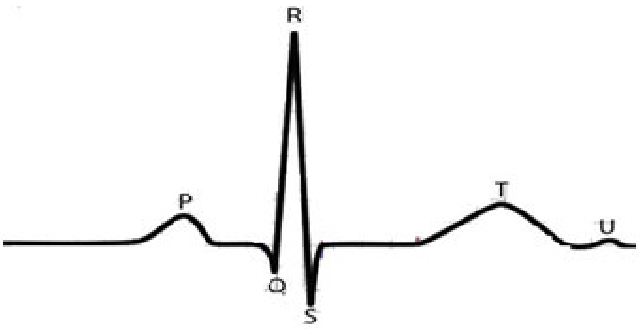

Figure 1
ECG waveform

Bradycardia. Most arrhythmias are harmless, but some can be serious or even life threatening. ECG is mostly responsible for patient monitoring and diagnosis[4]. The An sample ECG signal shows P-QRS-T waves. The electrocardiogram translates the heart's electrical activity into line tracings on paper[5]. The crest and trough in the line tracings are called waves. (Figure 1) The P wave will record through upper heart chambers which is atria. The QRS wave will get through the movement of electrical impulses by lower heart chambers which is ventricles (Figure 1) The ST segment shows when the ventricle is contracting but there will be no electricity combination of biometrics and cryptography is becoming a matter of interest for some researchers due to the fact that this combination can Figure1: ECG waveform flows through it and it usually appears as a straight line in between QRS complex and the T wave[6]. (Figure 1) The T wave shows when the lower heart chambers are resetting electrically and preparing for the next muscle contraction. (Figure 1) As shown in Figure 1 the ECG signal is taken for certain a amount of time. From the signal R interval peaks will be identified and from that, a key will be generated in a certain format[7-9]. The RR interval is shown in (Figure 2)

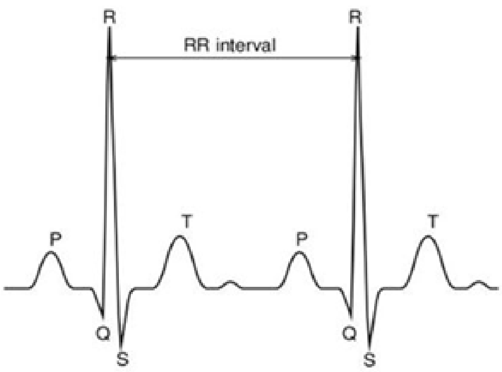

Figure 2
RR interval

Related work

They are number of methods and techniques to generate a key for transmission of data. But in this paper, we will use a real time ECG to provide the key. So, that the randomness of the signal will be improved. In this section, we will see different methods and techniques to generate the ECG key.[10] Lin Yao, Bing Liu Guowei Wu[11] proposed an algorithm to generate a biometric key using heart rate variability and intervals. The novelty used here is heart rate variability, interpulse interval. In this protocol, ECG as the dynamic biometrics is utilized to verify between a biosensor and CU. The idea of using ECG comes from the observation that the human body is dynamic and complex and the physiological state of a subject is quite randomness and time variance. ECG is characteristically collected and utilized in many identification applications, which is in accordance with the data minimization principle. In our protocol, we prefer the symmetric cryptographic algorithm. Based on the Biometric Encryption, a symmetric cryptographic key is established between every biosensor and CU. The purpose of this scheme is to provide a mutual trust between every biosensor and CU. At the same time, a session key is generated. ECG as the biometrics is collected and utilized. Our protocol includes two phases the key binding stage and key generation stage. During key binding, a session key is bound with ECG to produce Bioscrypt. During key generation, CG can recover the session key with Bioscrypt. It can't generate random keys Guanglou Zheng, Gengfa Fang, Rajan Shankaran[12] proposed an algorithm to generate a biometric sequence using fiducial points. The novelty used here is Wavelet transforms, random binary sequence, wireless body area network. The proposed MFBSG algorithm uses multiple fiducial points to obtain five feature values from one heart beat cycle. Compared to BS generation algorithms that are solely IPI-based, this scheme improves the time efficiency of BS generation, and thus achieves the design goal of low-latency, a basic requirement in a WBAN system. Here in this paper, the peak intervals are taken for the same signal in a consecutive way. For generating a 128-bit BS requires at least 32 IPIs, which means that the sensor node has to successfully detect at least 33 consecutive heart beats. Compared with the solely IPI-based schemes, the time required for generating a BS by using this algorithm is reduced significantly, thereby achieving the key goal of low-latency for WBAN sensors. These random BSes can be used as security keys for encryption or authentication, or be used to facilitate key distribution. The output will be of low latency but it has complex computations. J. MOHANA & V. THULASIBAI [13] proposed an algorithm to generate a key using RSA Encryption algorithm. The novelty used here is OFDM System, Rayleigh Fading, To avoid the reputed complexity of factoring large integers the factoring problem, RSA an algorithm for public-key cryptography was described. RSA is for Ron Rivest, Adi Shamir and Leonard Adleman, who took the initiation to describe the algorithm in 1977. The modulation system used on all the carriers is QPSK. The carriers are separated by a gap of around 1/Ts, where Ts is symbol period. The maximum bit rate available is 2bit/s/Hz of the bandwidth. This Figure is decreased by the inefficiency (signal redundancy) of the guard interval, the null symbol and the error coding. The same decryption processes will be done at the next step in which the process explained previously. Finally, the transmitted 128 bit key data received by the decryption process. H. A. Garcia-Baleon, V. Alarcon-Aquino[14] proposed an algorithm to generate a cryptographic key using wavelets. The successfully recovering of the key depends on a combination of a user password, a biometric sample, and a token, which stores the user password hash, the random locked biometric key hash, the encrypted random vector permutation (RVP), and error-correction information. The design presented in this paper ensures that the compromise of two factors at most will not let to the attacker reveal the biometric key. The cryptographic algorithms are highly exact. The modification of a single bit at the input drives to a completely different result at the output. However, the biometric information is highly fuzzy. It depends on the devices used to acquire the sample, background-random noise, and other factors. The possibilities of getting the same biometrics sample in two different acquisition times are almost zero. It is necessary to avoid storing a sample in the centralized database because this could lead to security concerns. Then, we propose to add several error-correction techniques like Hadamard and Reed-Solomon codes that produce a vector from which the biometric information cannot be derived. Neha Sharma Nidhi Yadav [15] proposed an algorithm to generate an intelligent security key. They introduce two frameworks, namely, feature extraction with/without fiducial detection, for ECG-based biometric recognition. In ECG monitoring, commonly encountered types of premature heart beats are the premature ventricular contraction. In this paper, they emphasize a case study that focuses on the mechanism of an intelligent security system, which ensures that our heartbeats can serve as a strong medium protecting against spoofing and hacking. The most promising benefit regarding the possibility of using the way the heart beats as a biometric is the fact that the biometric feature solves one of the biggest concerns regarding biometrics today namely: Liveness testing. One cannot measure the electrical activity of a human heart if the heart and thus the human are not alive. It is demonstrated that human identification via the ECG is feasible and highly effective. The ECG's robust nature against falsification makes it rather promising for security systems. It didn't discuss about the potential of applying ECG based identification under nonfunctional factors, such as stress aging and drug usage. M. J. BURKE M. NASOR[16] proposed a model to design and development of an ECG simulator intended for use in the testing calibration and maintenance of electrocardiographic equipment. When the simulator is first powered up default values are initialized for the user defined parameters of the signal. These values are then fed to the LCD followed by a message requesting the user to enter modified values as required. The keyboard is then scanned for data entered and the parameter values progressively updated as appropriate, both internally in the microcontroller and on the display. The 80C31 microcontroller used, IC1, is a part of the Intel 8051 family operating from a 12MHz crystal connected with capacitors C1 and C2. This microcontroller has an efficient 8-bit CPU, 256 bytes of internal RAM, two 16-bit timers, 4 external 8 bit ports and a range of internal and external interrupt lines as well as the customary general purpose and control registers. The hardware for the simulator was initially developed on a breadboard and next a prototype was constructed on two printed circuit boards, one containing the microcontroller and digital circuitry and the other containing the analogue output conversion circuitry. Extreme care should be there the analogue circuitry particularly with regard to grounding and shielding. B. Vuksanovic and M.Alhamdi[17] proposed a system for Biometric Recognition Using Analytic and AR Modeling Extracted Parameters in this the QRS complex is the most important feature of the ECG signal. Without the accurate knowledge of the QRS complex location, P and T waves are hard to detect and distinguish from each other. Most of the QRS detection methods depend heavily on filtering stage followed by averaging according to a threshold value. This threshold value is used to distinguish between noise signal and the QRS complex and is usually chosen according to the peak height or peak location of ECG signal. The short-time Fourier transform (STFT) was also in use after ECG filtering stage in order to identify QRS complex. In this the analytic features are usually being extracted by analyzing and localizing certain fiducial points from the ECG signals. In order to extract analytic features of ECG window or beat, procedure similar to is followed. As the R peak is already detected using QRS detection, Q, S, P and T amplitudes are localized by finding local maxima and minima separately around R position of each window. Biometrics-based human detection is essentially a patient recognition problem which involves preprocessing, feature extraction and classification stages. The electrocardiogram is an emerging biometric modality that has seen about 13 years of development reported in the peer-reviewed literature and as such deserves a systematic review and discussion of the associated methods and findings. In particular, the classification of methodologies in ECG based biometry relies on the feature extraction and categorization schemes. Due to this technique, the output will have more complex issues. Ming Li Xin Li [18] proposed a system for verification of ECG using heartbeat level and segment level. In this In the pre-processing, we first estimated and removed the baseline wander by a band pass filter. Second, we applied the filtering and smoothing frontend in to further clean the data. Then, we adopted two different QRS detectors, namely ecg wave from and Peak detection from for the R-peak detection. To investigate the performance of the proposed system, we used the public available PTB database from Physio Net. The reasons to select the PTB database for evaluation is as follows: 1)PTB database contains 549 recordings from 290 individuals, among which 52 subjects are healthy and the rest 238 subjects suffer from a variety of cardiac disorders which enables us to evaluate the performance for cardiac irregular conditions. After QRS R-peak detection, we could get two different sets of Rpeaks. For each QRS detector, let us denote the sample frequency fs as 1000, the number of beats as N, Di as the data associated with the ith beat, RRpre i and RRpost i as the RR interval of the ith beat measured against the previous and post R peaks respectively. In the time domain normalization, each beat is normalized to a 201 dimensional vector based on the associated phase values .By coverting ecg raw data into vector it takes more time to generate a key. Noureddine belgacem, Fethi bereksi-reguig[19] proposed a model to to identify a person using ECG signal. ECG varies among individuals due to the variations in anatomy and physiology of the heart. Normally, a progressive change in individual anatomy takes place from birth to adolescence (16 years of age). It has resulted that some options of graph varies throughout aging. A glance of change in normal limits of ECG parameters with age. These changes are not consistent and vary from one individual to another. Therefore, it is harder to make any generalization. A biometric system is essentially a pattern recognition problem and thus the methodology for this experiment can be broken down into 4 parts: (i) experimental setup, (ii) preprocessing, (iii) feature extraction and (iv)classification. Each part will be explained in detail in the following subsections. The ECG recorded from the palms has more noise than the ECG recorded from the torso, but the waveform morphologies are the same as the Lead I ECG. The EMG interference and baseline wander become more significant when ECGs are recorded from palms; that is, the signal-to-noise ratio (SNR) of the chest ECG signal is higher than of the palm ECG signal. The long-term changes of an individual's ECG signals and their implications for implementing a practical biometric system also need to be tested. Yogendra Narain Singh1, S. K. Singh[20] proposed a model to evaluate the electrocardiogram for authentication. In this the ECG signal which is acquired from the individuals is preprocessed for quality check. From noise and artifact it makes the necessary correction of the signal. ECG delineation includes detection of P, Q, R, S, and T waves with their dominant fiducials from each heartbeat. Feature extraction also determines the time intervals, amplitudes and angle features from dominant curves of its wave- forms. Finally, authentication and decision are taken by comparing the stored template and the query sample. The performance of the ECG the ECG database preysio Bank archives. In particular, we tested the performance of the multi biometric systems obtained from the fusion of ECG with face biometric and ECG with fingerprint biometric. In addition, the ECG information is intrinsic to every person so it is hard to steal and impossible to manipulate. The quality of signal is to be checked on daily basis. Peter Kovacs [21] proposed a model to generate ECG signal based on geometrical features. They justified thei work By using numerical and geometrical parameters, which are of diagnostical importance, the generated signal can be interpreted as a biomedical signal with important diagnostical intervals such as QRS, QT, PR etc. On the other side this model gives us a mathematical control over the signal. In our interpretation ECG signals are curves with prescribed parameters, including derivatives, curvature etc. In this paper they presented an algorithm which generates realistic synthetic ECG signals. This algorithm, among others, can be used for testing new methods in ECG processing. The proposed algorithm was implemented in MATLAB. The methods used for processing ECG signal requires databases with a high amount of test signals. In order to generate such databases we need to vary our parameters. In addition we have to keep the typical geometrical and diagnostical properties related to the actual ECG type. Therefore we define the ECG pro le by means of the upper and the lower bounds of the parameters. These bounds are typical to certain kinds of cardiac abnormalities. Filtering and synthesis not done clearly which takes more time to generate the signal.

Project overview

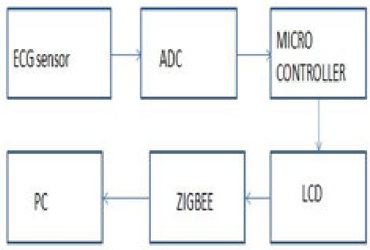

Figure 3
Block diagram of extraction of RR interval and transferring to PC via zigbee

ECG sensor
The ECG sensor is attached to the patient the use of disposable electrodes on the left and proper aspect of the chest. The sign obtained from the frame is filtered and amplified. The sensor outputs an analog sign that's then converted through the analog-to-digital converter (ADC). The serial to Bluetooth module transmits the digital output of the ADC to the cellular phone. At the cell phone the sampled ECG is displayed. Its frequency range will be 0.05 to 16Hz, sampling rate will be 470 samples/sec and the transmission will be 10 meters. Usually more than 2 electrodes are used and they can be combined into a number of pairs (For example: Left arm (LA), right arm (RA) and left leg (LL) electrodes form the pairs: LA+RA, LA+LL, RA+LL). The output from each pair is known as a lead. Each lead is said to look at the heart from a different angle. Different types of ECGs can be referred to by the number of leads that are recorded, for example 3-lead, 5-lead or 12-lead ECGs (sometimes simply "a 12-lead").

ADC 0809
ADC: It is used to convert analog signal to digital signal
The ADC0809 information procurement segment is a solid CMOS device with a 8-bit analog to-digital converter, 8 channel multiplexer and microprocessor control logic. The 8-bit A/D converter utilizes progressive guess as the transformation strategy. The converter includes a high impedance chopper settled comparator, a 256R voltage divider with simple switch tree and a progressive approximation register. The 8-channel multiplexer can specifically get to any of 8-single-ended analog signals.

ATMEL AT89S52
The AT89S52 is a low-control, elite CMOS 8-bit microcontroller with 8K bytes of in-framework programmable Flash memory. The gadget is made utilizing Atmel's high-thickness nonvolatile memory innovation and is perfect with the Indus-try standard 80C51 direction set and stick out. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory pro-grammars. By combining a versatile 8 bit CPU with in-system programmable Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcontroller which provides a highly-flexible and cost-effective solution to many embedded control applications. The AT89S52 provides the following standard features: 8K bytes of Flash, 256 bytes of RAM, 32 I/O lines, Watchdog timer, two data pointers, three 16-bit timer/counters, a six-vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator, and clock circuitry.

Zigbee module
ZigBee is a low-cost, low-power, wireless mesh network standard targeted at the features like long battery life devices in wireless control and monitoring applications. Zigbee devices have low latency, which additionally reduces average current. ZigBee chips are integrated with radios and with microcontrollers that have between 60-256 KB of flash memory. ZigBee operates in the industrial, research and medical (ISM) radio bands: 2.4 GHz in most fields worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band).The ZigBee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device, programmed with its creation, the control of its parameters and basic maintenance. In star networks, the main node must be the central node. Both trees and meshes allow the use of ZigBee routers for the communication at the network level.

Implementation
Binary Sequence generation process
The ECG signal is taken using ECG sensor and it will be amplified after that it will move to ADC and convert into digital and it will send to microcontroller. In microcontroller it will find the value of ECG and it will send to feature extraction process. Wavelets decompose signals into time-varying frequency (scale) components. Because signal features are often localized in time and frequency, analysis and estimation are easier when working with sparser (reduced) representations. The QRS complex consists of three deflections in the ECG waveform. The QRS complex reflects the depolarization of the right and left ventricles and is the most prominent feature of the human ECG.[22-23] Load and plot an ECG waveform where the R peaks of the QRS complex have been annotated by two or more cardiologists. The ECG data and annotations are taken from the MIT-BIH Arrhythmia Database. The data are sampled at 360 Hz. Automatic QRS detector can be built by wavelets to use in the applications like estimation of RR interval. There are two keys for using wavelets as general feature detectors:[24]

- The wavelet transform separates signal components into different frequency bands enabling a sparser representation of the signal.[25]
- It can often find a wavelet which resembles the feature you are trying to detect.

The 'sym4' wavelet resembles the QRS complex, which makes it a good choice for QRS detection At the command line, you can compare the values of tm(ann) and locs, which are the expert times and automatic peak detection times respectively. Enhancing the R peaks with the wavelet transform results in a hit rate of 100% and no false positives. The calculated heart rate using the wavelet transform is 88.60 beats/minute compared to 88.72 beats/minute for the annotated waveform. If it attempt to work on the square magnitudes of the original data, you find the capacity of the wavelet transform to isolate the R peaks makes the detection drawback more easier. Working on the unorganized data can cause misidentifications such as when the squared S-wave peak exceeds the R-wave peak around 10.4 seconds.

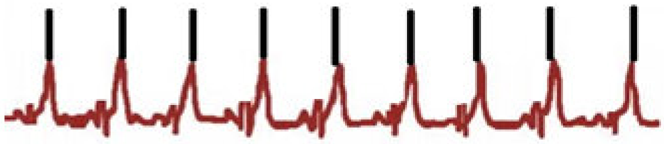

Figure 4
Set of RR intervals

An ECG signal is taken and it is processed so that set of R peaks will be detected and the value of two consecutive R peaks will be subtracted and the resultant value is calculated and it will change into different binary format. (Figure 4) All the interval values combined together and form the biometric sequence.

CONCLUSION

Generally, there are many methods to generate a biometric sequence like pseudo random generator and various techniques will be there but the randomness and latency will be low. But in this papert it can generated the biometric sequence using the real time ECG signal. The ECG signal parameters will change from person to person. The key generated will be different for different persons. Thus, it can improve the randomness by using real time ECG signal. Since, it can show randomness it can provide authentication of data.

CONFLICT OF INTEREST

Conflict of interest declared none.

REFERENCES

1. Ghaffari A, Homaeinezhad MR, Akraminia M, Atarod M, Daevaeiha M. A robust wavelet-based multi-lead electrocardiogram delineation algorithm. Medical engineering & physics. 2009 Dec 31;31(10):1219-27.
2. Pang L, Tchoudovski I, Bolz A, Braecklein M, Egorouchkina K, Kellermann W. Real time heart ischemia detection in the smart home care system. In Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the 2006 Jan 17; p. 3703-6.
3. Irvine JM, Israel SA, Scruggs WT, Worek WJ. eigenPulse: Robust human identification from cardiovascular function. Pattern Recognition. 2008 Nov 30;41(11):3427-35.
4. Juels A, Wattenberg M. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security 1999 Nov 1; p. 28-36.
5. Mallat S. Zero-crossings of a wavelet transform. IEEE Transactions on Information theory. 1991 Jul;37(4):1019-33.
6. Li M, Narayanan S. Robust ECG biometrics by fusing temporal and cepstral information. In Pattern recognition (icpr), 2010 20th international conference on 2010 Aug 23; p. 1326-29.
7. Mohana J, Bai VT. 128 bit key generations from the dynamic behavior of ECG for securing wireless body area network. ARPN Journal of Engineering and Applied Sciences. 2015;10(18):8048-51.
8. Mohana J, Bai VT. Implementation of Efficient Cryptographic Algorithm Based on Dynamic Biometric Key Generation Technique. Sensor Letters. 2016 Oct 1;14(10):1044-8
9. Mohana J, Thulasibai V. Biometric Monitoring System for Multi Sensor Multi-modal Node Architecture. International Journal of Computer Applications in Engineering Sciences. 2013;3:26-30.
10. Gupta S, Kaur P. WBAN Health Monitoring System Using TEEN Protocol: Threshold Sensitive Energy Efficient Network Protocol. International Journal of Innovative Science, Engineering & Technology. 2015 Oct;2(10).
11. Yao L, Liu B, Wu G, Yao K, Wang J. A biometric key establishment protocol for body area networks. International Journal of Distributed Sensor Networks. 2011 Aug 14;7(1):282986.
12. Zheng G, Fang G, Shankaran R, Orgun MA, Zhou J, Qiao L, Saleem K. Multiple ECG Fiducial Points-Based Random Binary Sequence Generation for Securing Wireless Body Area Networks. IEEE J Biomed Health Inform. 2017 May;21(3):655-63.
13. Mohana. J, Thulasibai.V. ECG key gen using RSA Encryption technique and transmission by OFDM system over Rayleigh Fading Channel.

IJECIERD 2014 Aug; 4(4):1-12. Available from http://www.tjprc.org/publishpapers/2-16-1403249106-absECG%20KEY%20GEN%20USING %20RSA%20ENCRYPTION%20TECHNIQUE%20AND%20TRANSMISSION%20BY%20OFDM%20SYSTEM%20OVER%20RAYLEIGH%20FADING%20CHANNEL.pdf

14. Garcia-Baleon HA, Alarcon-Aquino V. Cryptographic key generation from biometric data using wavelets. InElectronics, Robotics and Automotive Mechanics Conference, 2009. CERMA'09. 2009 Sep 22; pp. 15-20.
15. Neha Sharma, Nidhi Yadav, An Intelligent Security: A Heart to My Key. IJARCSMS, 2016; 4(1): 297-301. Available from: http://www.ijarcsms.com/docs/paper/volume4/issue1/V4I1-0001.pdf
16. NASOR MB. A Microcontroller-Based Precision ECG Signal Generator.
17. Vuksanovic B, Alhamdi M. Analysis of Human Electrocardiogram for Biometric Recognition Using Analytic and AR Modeling Extracted Parameters. Int J Eng Res Appl. 2014 Nov 1;4(6):428.
18. Li M, Li X. Verification based ECG biometrics with cardiac irregular conditions using heartbeat level and segment level information fusion. In Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on 2014 May 4: p. 3769-73.
19. Belgacem N, Bereksi-Reguig F, Nait-Ali A, Fournier R. Person identification system based on electrocardiogram signal using Lab VIEW. International Journal on Computer Science and Engineering. 2012 Jun 1;4(6):974.
20. Singh YN, Singh SK. Evaluation of Electrocardiogram for Biometric Authentication. J. Information Security. 2012 Jan 1;3(1):39-48.
21. Ch.Tanmaya , N.Syamala , P.Rajesh , B.Pavannadh , B.Sridhar, Analysis of ECG Signal for Detecting Heart Blocks Using Signal Processing Techniques, IJIRCCE, 2016; 4(3):3778-84. Available from: https://www.ijircce.com/upload/2016/march/192_ANALYSIS.pdf
22. Li M, Li X. Verification based ECG biometrics with cardiac irregular conditions using heartbeat level and segment level information fusion. In Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on 2014 May 4; p. 3769-73).
23. Zhang J, Woods R, Duong TQ, Marshall A, Ding Y, Huang Y, Xu Q. Experimental study on key generation for physical layer security in wireless communications. IEEE Access. 2016;4:4464-77.
24. Taddei A, Distante G, Emdin M, Pisani P, Moody GB, Zeelenberg C, Marchesi C. The European ST-T database: standard for evaluating systems for the analysis of ST-T changes in ambulatory electrocardiography. Eur Heart J. (EAJ) 1992 Sep 1;13(9):1164-72.
25. Venkatasubramanian KK, Banerjee A, Gupta SK. PSKA: Usable and secure key agreement scheme for body area networks. IEEE Trans Inf Technol Biomed. 2010 Jan;14(1):60-8.

Reviewers of this article

Dr.C.R.Bharathi (AMIE, ME, Pd.D)

Associate professor, Dept. of ECE,
Vel Tech University,
Chennai, Tamilnadu, India.

Prof.Dr.Prapurna Chandra Rao

Assistant Proffessor, KLE University,
Belgaum, Karnataka, India.

Prof.Dr.K.Suriaprabha

Asst. Editor , International Journal
of Pharma and Bio sciences.

Prof.P.Muthuprasanna

Managing Editor , International
Journal of Pharma and Bio sciences.

We sincerely thank the above reviewers for peer reviewing the manuscript