Entropy Test Using the PPG Sensor of LED Light Source

Juyoung Kim* Sang Uk Shin**
*Information Security Research Division
*Electronics and Telecommunications Research Institute
*218, Gajeong-ro, Yuseong-gu, Daejeo
**Dept. of IT Convergence and Application Engineering
**Pukyoung National University
*45, Yongso-ro, Nam-Gu. Busan
Republic of Korea
ap424@etri.re.kr, shinsu@pknu.ac.kr

Abstract: - Biometric information security is an important issue in the BSN (Body Sensor Network). In particular, physiological sensor may be related to the patient's life. In recent, a case of insulin pump hacking was reported. To prevent these security risks, a secure communication protocol between BSNs is needed. Therefore a key generation method using a bio-signal is required.

In this paper, entropy test is performed to generate a key using bio-signals. In addition, an entropy test is performed for green, red and infrared LED light source to analyze an LED suitable for generating a key.

Key-Words: - PPG, Entropy test, Bio-signal

1 Introduction

Between BSN issues security in research on bio-signal. BSNs have many potential threats. In particular replay, inject message, spoofing attack is fatal to the patient. In particular Barnaby Jack warned that the risk of BSN hacking through the hacking of the insulin pump where 2012 RSA Conference. To prevent these risks, there is a protocol that secures communicates between BSNs. Symmetric key generates bio-signal from PPG sensor, generated key will be able to use secure communication between BSNs. Seed to generate bio-signal based symmetric key can be used PPI (PP interval) from PPG (photo-plethysmography) sensor. To create a symmetric key, the entropy of PPI should have sufficient randomness.

This paper presents entropy test by LED light source using acquired bio-signal from PPG. The test procedure is as follows

1) The collecting PPG signal from Green and Infrared LED
2) Remove non-randomness bit
3) AIS .31 based entropy test.

The rest of this paper is organized as follows. We research related work in section 2. Section 3 present collection and processing of PPG data. In section 4, entropy test and result analysis. We conclude the paper in Section 5

2 Relate Work

If collected big-signal is no randomness, there is a problem that can infer symmetric key. In G. H. Zhang. PPG and ECG data proved that is randomness by entropy calculation [1].

Node of BSNs have constraints such as low power, limited memory, low computation capability and low communication rate. K S Gupta et al. suggested biometric key generation and exchange scheme these environments. This scheme used hamming distance to perform synchronization between bio-signals [2]. Also, these were proposed physiological values-based security. This scheme summary as follows [3]:

1) PV(Physiological Value) synchronization and measurement and between nodes
2) Send hide the random key by PV_{send}
3) Random key extraction via ECF(Error Correction Function) and $PV_{receive}$
4) Data certification

Also fuzzy vault system proposed for key-agreement between two nodes in BANs [4].

3 PPG Data Collection and Processing

This section present collection and processing of PPG data

Before the entropy test, we analysis bit distribution of PPI using about 150,000 bits by green LED

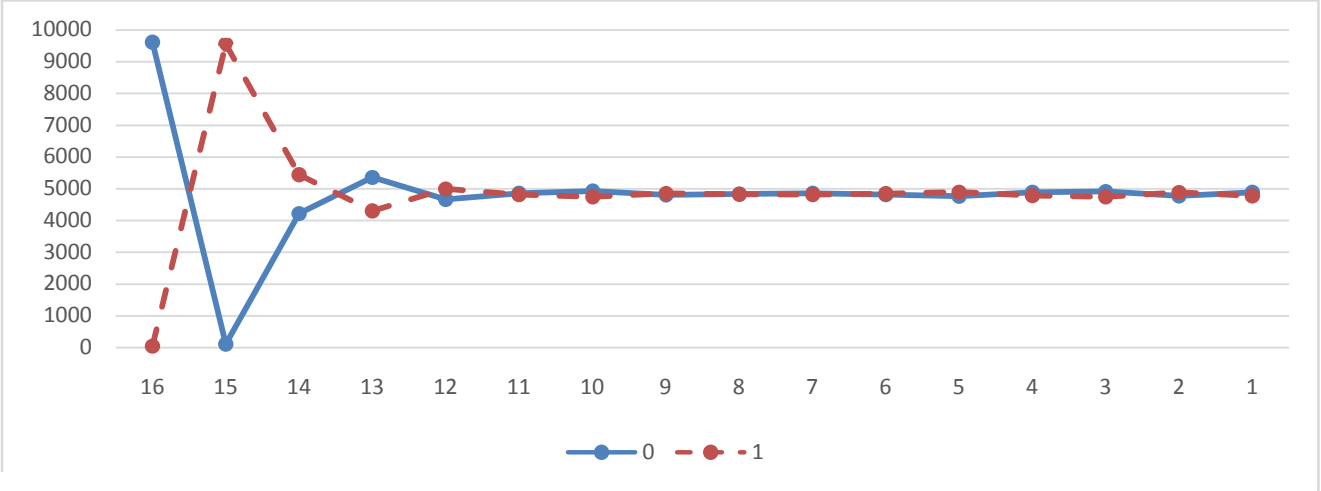

Figure 1: Bit distribution of PPI

The data collected from the PPG sensor are shown in the table1 below.

Table 1: Data Collection

Values	means
LED1 PPI(green)	LED of green PPI value
LED2 PPI (red)	LED of red PPI value
LED3 PPI (infrared)	LED of infrared PPI value
LED1 1st Derivatives	Green LED PPI of 1st Derivatives value
LED2 1st Derivatives	Red LED PPI of 1st Derivatives value
LED3 1st Derivatives	Infrared LED PPI of 1st Derivatives value
LED1 2nd Derivatives	Green LED PPI of 2nd Derivatives value
LED2 2nd Derivatives	Red LED PPI of 2nd Derivatives value
LED3 2nd Derivatives	Infrared LED PPI of 2nd Derivatives value

PPI is first and second differentiated for the extract peak interval. The collected data are converted to 16bit binary data. If 17bit is exceeded, remove the left bit and set it test.

Figure1 shown distribution of 0 and 1 for each digit. 16~13 digits were unevenly distributed.. Therefore, we used 12bits data for entropy test.

4 Entropy Test

We used AIS .31 test for entropy test. AIS .31 is a random generator an evaluation method made by BSI (Bundesamt für Sicherheit in der Informationstechnik, Feder Office Information Security). Total 8 tests are provided, and tests are summarized in the table below [5][6].

Table 2 Statistical tests of AIS.31

Class	Test	Mean
P1, P2	T0 (disjointness test)	Subsequent members are Pairwise different.
	T1 (mono bit test)	Tests based on the assumption that the 0 and 1 are equal
	T2 (poker test)	Suitable test for 4bits block
	T3 (runs test)	Test for the number of run which has *l*-length.
	T4 (long run test)	Check up the occurrence run of length ≥ 34.

	T5 (autocorrelation test)	Whether the range of Range verification of autocorrelation values
P2	T6 (uniform distribution test)	Uniform distribution test using ratio of 0's and 1's
	T7 (comparative test)	Goodness of fit test for blocks by comparison.
	T8 (entropy test)	Estimate entropy as minimum distance of blocks.

P1 class needs at least 20,000 bits to perform. But T0 test needs 720,000 bits. In this paper P1 class was performed without T0, 12bit and 11bit data from PPG sensor was used to test.

5 Analysis

T1 to T5 tests were performed using 18 PPG data. The test results are shown in the table below.

Table 3: Data Collection (P:Pass F: Fail)

TEST / DATA	T1	T2	T3	T4	T5
LED1_PPI_12bit	P	P	P	P	P
LED1_PPI_11bit	P	P	P	P	P
LED2_PPI_12bit	P	P	P	P	P
LED2_PPI_11bit	P	P	P	P	P
LED3_PPI_11bit	P	P	P	P	P
LED3_PPI_12bit	P	P	P	P	P
LED1_1deriv._12bit	P	P	P	P	F
LED1_1deriv._11bit	P	P	P	P	P
LED2_1deriv._12bit	P	P	P	P	P
LED2_1deriv._11bit	P	P	P	P	P
LED3_1deriv._12bit	P	P	P	P	P
LED3_1deriv._11bit	P	P	P	P	P
LED1_2deriv._12bit	P	P	P	P	F
LED1_2deriv._11bit	P	P	P	P	P
LED2_2deriv._12bit	P	P	P	P	F
LED2_2deriv._11bit	P	P	P	P	P
LED3_2deriv._12bit	P	P	P	P	P
LED3_2deriv._11bit	P	P	P	P	P

Green LED PPI data is passed test. But first and second derivatives data are not passed T5 test. 12bit second derivatives data of red LED is not passed T5 test. On the other hand, infrared LED all data is passed T1 to T5 test. T5 test is an autocorrelation test with a significance level of 10^{-6}. In this case, accept region range is $2326< T <2674$ based on 20,000 bits.

6 Conclusion

This paper, we collect the PPI data for each LED light source, the data were processed for randomness. Also, we analysis entropy test of PPG data. As a result, infrared LED of data most passed the entropy test

In the future, more data needs to be collected for P2 class test and synchronization between sensors is needed.

Acknowledgements: This work was supported by the ICT R&D program of MSIP/ IITP[B0117-16-1002, Feasibility Study of Blue IT based on Human Body Research]

References:

[1] G. H. Zhang, Carmen C. Y. Poon, and Y. T. Zhang, A Biometrics Based Security Solution for Encryption and Authentication in Tele-Healthcare Systems, *2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2009*

[2] Sriram Cherukuri, Krishna K Venkatasubramanian , Sandeep K S Gupta, BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body, *Proceedings of the 2003 International Conference on Parallel Processing Workshops*, 2003,

[3] KRISHNA K. VENKATASUBRAMANIAN and SANDEEP K. S. GUPTA, Physiological Value-Based Efficient Usable Security Solutions for Body Sensor Networks, *ACM Transactions on Sensor Networks*, Vol.6, No.5, 2010

[4] Krishna K. Venkatasubramanian, Ayan Banerjee, Sandeep Kumar S. Gupta, PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks, *IEEE TRANSACTIONS*

ONINFORMATION TECHNOLOGY INBIOMEDICINE, Vol.14, No.1, 2010

[5] BSI, A proposal for Functionality classes for random number generators, 2011

[6] Hojoong Park, Ju-Sung Kang, Yongjin Yeom, Probabilistic Analysis of AIS.31 Statistical Tests for TRNGs and Their Applications to Security Evaluations, *Journal of the Korea Institute of Information Security and Cryptology*, 2016