International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.321-330
http://dx.doi.org/10.14257/ijsia.2016.10.9.31

Parallel Encryption Method on Brain Wave for a Person Authentication

Jung-Sook Kim[1] and Jang-Young Chung[2]

[1]*School of Smart IT, Kimpo University*
97, Gimpodaehak-ro, Wolgot-myun, Gimpo-si, Gyenggi-do, 10020, Korea
kimjs@kimpo.ac.kr
[2]*IoT convergence Lab.*
Penta Security Systems Inc., Seoul, Korea
e-mail: sd109@dongguk.edu

Abstract

In this paper, we proposed an efficient parallel encryption scheme on brain wave for user authentication using the chaos maps and junk data. Two different methods were proposed. The first method uses the fixed block size of brain wave and uses variable block size of junk data. The second method uses variable block size of brain wave and variable block size of junk data. Two methods are same processing phase. The only difference is the block size of brain wave. Especially, the person authentication using unstructured data requires the real-time processing. And many researchers have been developed the encryption method with fixed maps. However, it has better security that variable maps are used for generating the random number in chaos maps. And we developed a parallel encryption method using the threads. To execute two encryption schemes, two threads are created. The one manages the process that generates five phase chaos maps and another thread manages the encryption scheme. The processing phase of the encryption scheme is composed of five phase. As a result, the encrypted brain-wave signals are produced well and the processing time for authentication is reasonable in real-time.

Keywords*: Parallel Encryption Method, Brain Wave, Person Authentication, Chaos Map, Variable Size of a Junk Data. Thread*

1. Introduction

Most of the security systems on the market can be penetrated by hacking or a mistake by one the authorized personnel. And many researchers have been studied a biometrics for security. Biometrics is the process of uniquely identifying individuals on the base of one or more physical or behavioral characteristics. Physiological biometrics is related to the physical characteristics of the body such as a fingerprint, the face, and DNA; whereas behavioral biometrics is related to the person's behavior such as the typing rhythm, gait, and signature. The brain wave pattern of every individual is unique, and brain wave signals can be used for biometric authentication. However, Secondary damage to the user is a problem in biometrics. A brain-wave has no shape and a malicious user may not cause secondary damage to a user. The advantage of using brain-wave signals is that they satisfy all of the above-mentioned requirements, unlike other techniques. The use of brain activity for person authentication has several advantages: (1) it is confidential (as it corresponds to a mental task), (2) it is very difficult to mimic (as similar mental tasks are person dependent), (3) it is almost impossible to steal (as the brain activity is sensitive to the stress and mood of the person; an aggressor cannot force the person to reproduce his/her mental pass-phrase). There are two types of brain wave signals - positive and

ISSN: 1738-9976 IJSIA

negative signals. The positive and negative signals can be clearly distinguished and the hacker could easily know an obvious fact. As a result, if a user sends brain wave signals to an authentication system using a network, a malicious user could easily capture the brain-wave signals. Then, the malicious user could access the authentication system using the captured brain wave signals. However, developed encryption schemes such as AES, RSA, and ECC are difficult to use for the encryption of brain wave signals because the user authentication system must provide authentication in real-time. And, an unstructured data such as a brain wave, image data, voice data, and *etc*, requires a different encryption method. However, these encryption schemes cause overhead and these encryption schemes cannot guarantee user authentication in real time. In addition, the dataset containing the brain wave signals is large and the transfer time is long. As a result, a fast encryption method is required for user authentication [1-13]. In this paper, we propose a parallel efficient encryption scheme using chaos maps and a junk data on the brain wave signals for person authentication in real-time. Two different methods were proposed. The first method use the fixed block size of brain wave and use variable block size of junk data. The second method use variable block size of brain wave and variable block size of junk data. Two methods are same processing phase. The only difference is the block size of brain wave. Especially, the person authentication using unstructured data requires the real-time processing. And many researchers have been developed the encryption method with fixed maps. However, it has better security that variable maps are used for generating the random number in chaos maps. And we developed a parallel encryption method using thread. To execute two encryption schemes, two threads created. The one manages the process that generates five phase chaos maps and another thread manages the encryption scheme. The process of the encryption scheme is needed five phase chaos maps. The chaos maps generate the random numbers to divide the brain-wave signals and junk data with variable size blocks and to apply a XOR and the permutation operations on encryption scheme. As a result, the parallel processing time is shorter than encryption processing time. Also, the first method has good encryption processing time than the second method. The reason is that a nonlinear method is used for collecting the information during the XOR operation execution on brain wave using chaos map. However, the security of the second method is good than the first method.

The structure of this paper is organized as follows: In Section 2, we briefly explain the related researches and Section 3 presents two encryption methods that use two threads for parallel encryption scheme on brain wave using chaos maps and junk data for person authentication. Section 4 presents the experimental results. Finally, the conclusions and plans for future study are discussed in Section 5.

2. Related Work

2.1. EEG Encryption System using Chaos Algorithm

In the paper, the authors use Microsoft's Visual Studio Development Kit and the C# programming language to implement a chaos-based electroencephalogram (EEG) encryption system with three encryption levels. A chaos logic map, an initial value, and a bifurcation parameter for the map are used to generate level I chaos based EEG encryption bit streams. Two encryption-level parameters are added to these elements to generate level II chaos-based EEG encryption bit streams. An additional chaotic map and a chaotic address index assignment process are added to implement a level III chaos-based EEG encryption system. Eight 16-channel EEG signals are tested using the encryption software. The encryption speed is the lowest, and encryption is the most robust for the level III system. The test results show that the encryption results are superior, and the EEG signals are completely recovered when the correct deciphering parameter is applied. However, an input parameter error, *e.g.*, a 0.00001% initial point

error, will cause chaotic encryption bit streams, and 16-channel EEG signals will not be recovered [6].

3. EEG Encryption Method

3.1. System Structure

The parallel encryption scheme is composed of two parts. The one is for generating the random number using chaos map and another is for managing the encryption. In order to parallel processing, two threads are created. Figure 1 shows the system structure.

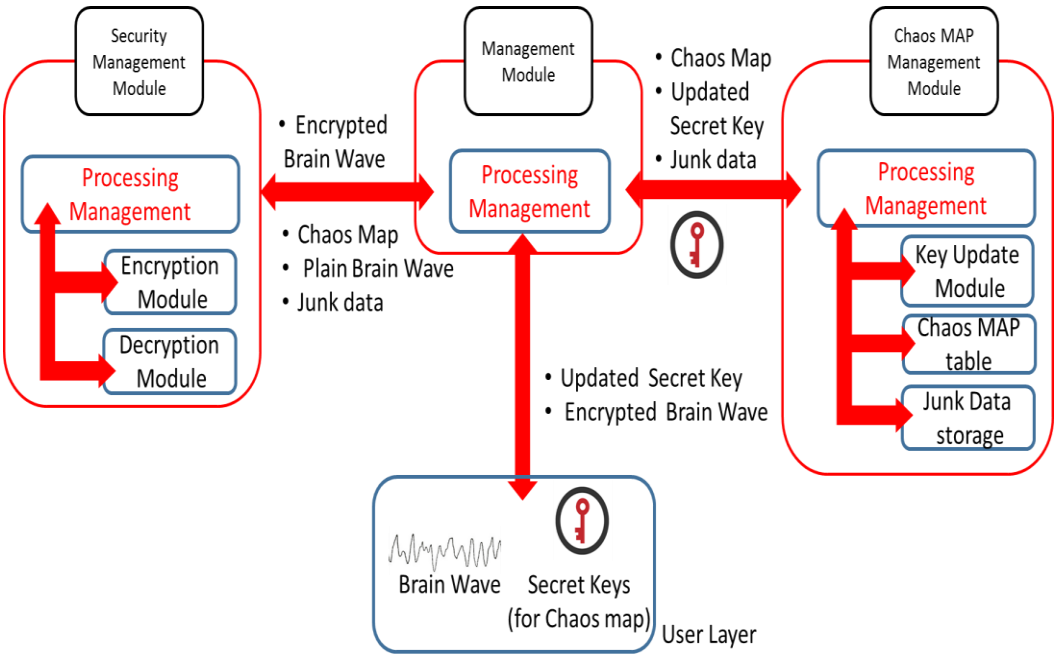

Figure 1. System Structure

3.2. Process of the Encryption Scheme

The process of the parallel encryption scheme consists of two threads each encryption method. At first, the brain wave and a secret key are generated. Then, the one thread executes five phase chaos maps. The first phase chaos map is generated to divide the brain-wave signals into several blocks. The size of blocks is variable and determined by the first chaos map. The second phase generates the junk data. The size of junk data is determined by the second chaos map and is variable. The brain wave signals have a uniform pattern and the junk data are inserted into the brain wave signal in order to disorder the uniform pattern. The third chaos map generates a random number to execute an XOR operation. Next, a permutation operates on each brain wave block using the fourth chaos map. Finally, the fifth chaos map executes the permutation on the brain wave. And another thread processes the each phase encryption scheme using the random numbers which are received by the chaos maps generator agent. As a result, an encrypted brain-wave is produced.

The chaos maps use a logistic map, and the following to generate a random number using chaos maps.

$$x_{n+1} = ax_n(1 - x_n), \quad 3.56 < a < 4, \quad 0 < x_n < 1 \tag{1}$$

Table 1 summarizes the values of a and x_n for the first phase chaos map. Each phase of chaos map is used by a different number for a and x_n. Moreover, three experiments were carried out.

Table 1. Values of the a, x_n, X_0, and X_1

	a	x_n	X_0	X_1
Experiment # 1	3.58	0.73	0.78123456789	3.781234567891
Experiment # 2	3.68	0.83	0.88123456789	3.781234567891
Experiment # 3	3.78	0.93	0.91233456789	3.781234567891

Table 2 summarizes the values of a and x_n for the second phase chaos map for generating the junk data and variable block size of junk data.

Table 2. Values of the a, x_n, X_0, and X_1.

	a	x_n	X_0	X_1
Experiment # 1	3.581	0.731	0.78123456789	3.781234567891
Experiment # 2	3.681	0.831	0.88123456789	3.781234567891
Experiment # 3	3.781	0.931	0.91233456789	3.781234567891

Next, the junk data are generated using formula (2) and inserted into the brain-wave signals by formula (3). The generated random number using second chaos maps divides two parts. Because the first half is used to junk operation and the other half is used to junk data. The value of y in formula (2) is defined by the user as a fixed number. The value of y used for the experiment is 123. The value of z in formula (2) is fixed and defined by the user. The value of z in experiment is 10.

The size of junk data = $(X_{n+1} * y) / z$ (2)

For(i < the size of junk data)
{
junk[i] = $X_n + 1$
} (3)

The third chaos map generates the 2-hold size random number (ChaosMap3_1[size of brain wave] and ChaosMap3_2[size of brain wave]) then brain wave size for XOR operation. After that, the generated maps merge into one chaos map order by the first map (ChaosMap3_1[ ]) of third chaos map. Then, the merged map (ChaosMap3_2[ ]) generated for XOR operation. And the brain wave signals are encrypted as follows by the chaos map

Encrypted data = **((Brain-Wave**[ ] x 10^9) **XOR** ChaosMaps3_2[ ] **x** 10^9 **MOD** prime number) / 10^9 (4)

4. Implementation and Results

4.1. Encryption Results

The system was implemented using MS Xamarin Studio Community Version 6.0.1(Mono 4.4.1) C#, MATHLAB 2010, Neuroscan, and E-Prime on a computer equipped with an Intel CPU running at Core i7 (2.2 GHz), 16 GB of RAM, and 1 TB HDD. The brain-wave signals sampled at a frequency of 250 Hz and filtered from 0.1 to 30 Hz. In addition, they were obtained by the lexical decision task of E-prime. A subject sees four words one at a time to produce the positive brain wave signals and negative brain wave signals. The test is repeated 100 times. The words for the experiments are 4 words for positive signals and 4 words for negative signals and the initial values for the experiments are summarized in Table 1 and Table 2. Figure 2 shows a positive brain-wave signal that is encrypted using the proposed two methods.

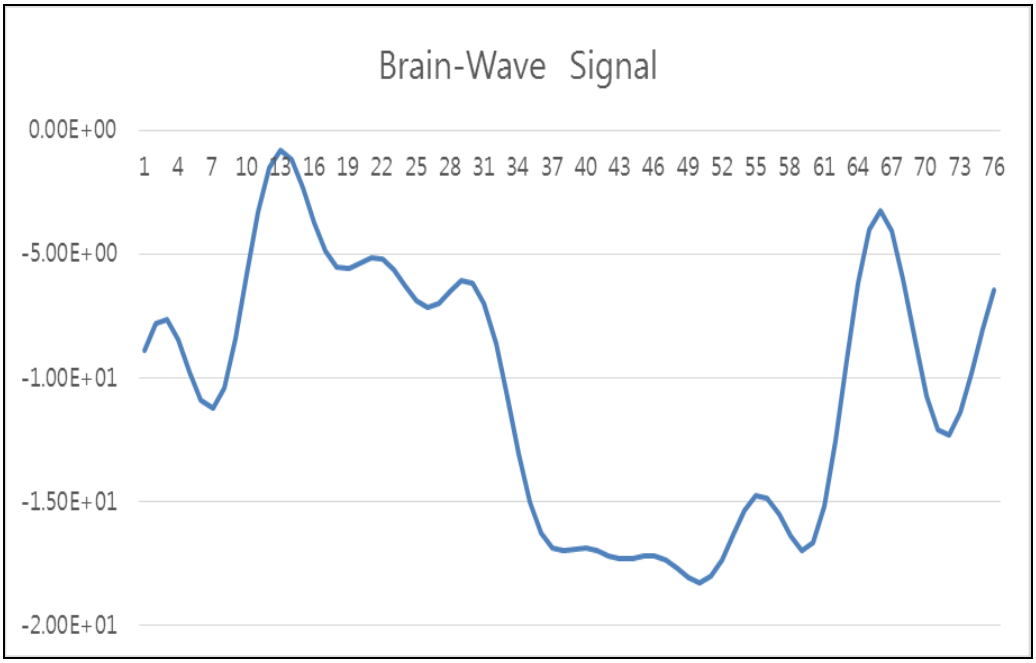

Figure 2. Positive Brain Wave Signal

Figure 3 shows the encrypted results on the positive signals using the initial values of the experiment # 1 in Table 1 for the first phase chaos map and the second initial value is the experiment # 1 in Table 2. Also, the experimented encryption method is the second that has variable block size of the brain wave by generated the first phase chaos map and variable block size of the junk data by generated the fourth phase chaos map. As you can see in Figure 3 and 4, the results are different because the chaos map generated the random number per each operation. However, the encryption process and method is same.

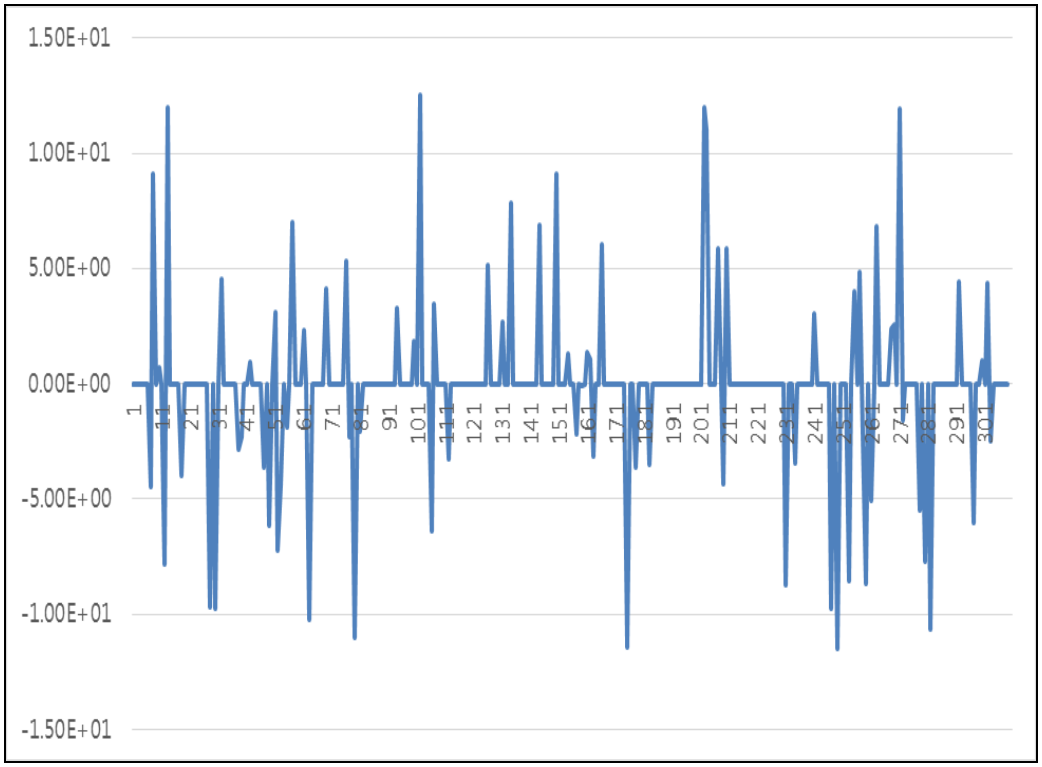

Figure 3. The First Result of the Second Method

Figure 4 shows the encrypted results on the positive signals using the initial values of the experiment # 2 in Table 1 for the first phase chaos map and the second initial value is the experiment # 2 in Table 2.

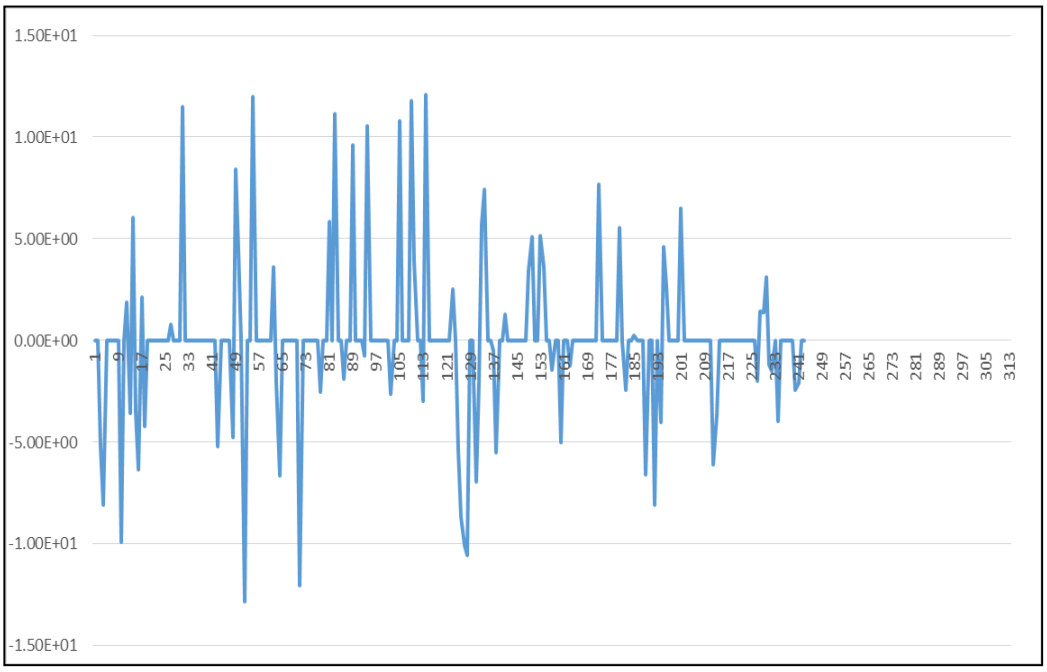

Figure 4. The Second Result of the Second Method

Figure 5 shows the encrypted results on the positive signals using the initial values of the experiment # 1 in Table 1 for the first phase chaos map and the second initial value is the experiment # 1 in Table 2. Also, the experimented encryption method is the first that has variable block size of the brain wave by generated the first phase chaos map and variable block size of the junk data by generated the fourth phase chaos map. As I said before, the results of Figure 5 and Figure 6 are different because the chaos map generated the random number per each operation. However, the encryption process and method is same.

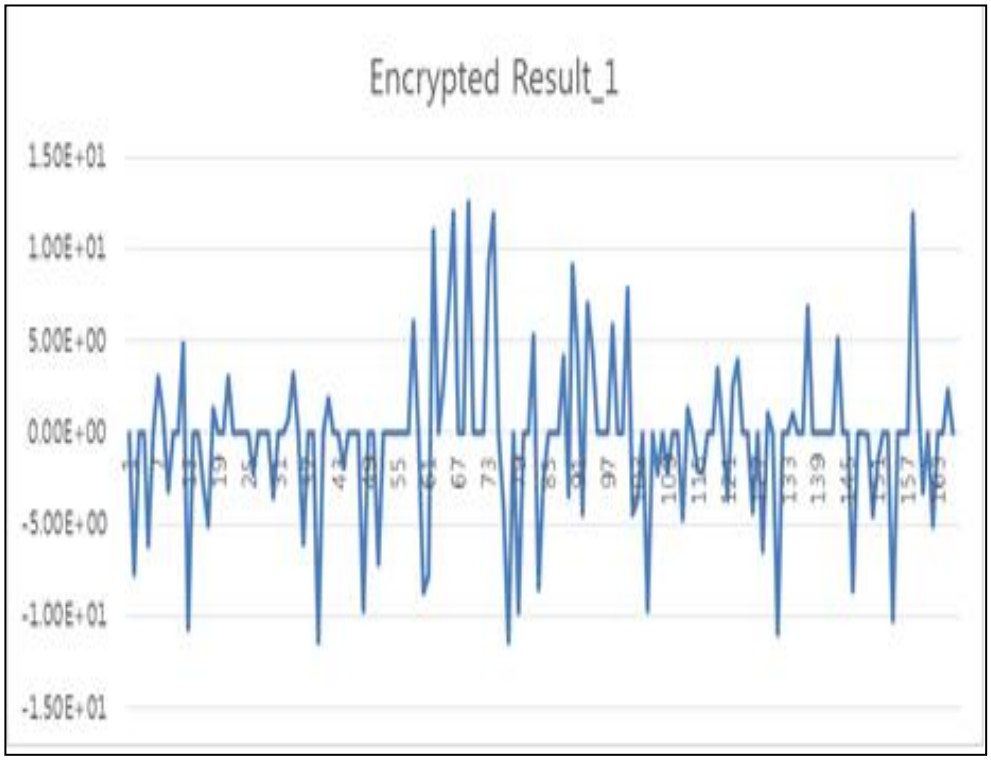

Figure 5. The First Result of the First Method

Figure 6 shows the encrypted results on the positive signals using the initial values of the experiment # 2 in Table 1 for the first phase chaos map and the second initial value is the experiment # 2 in Table 2.

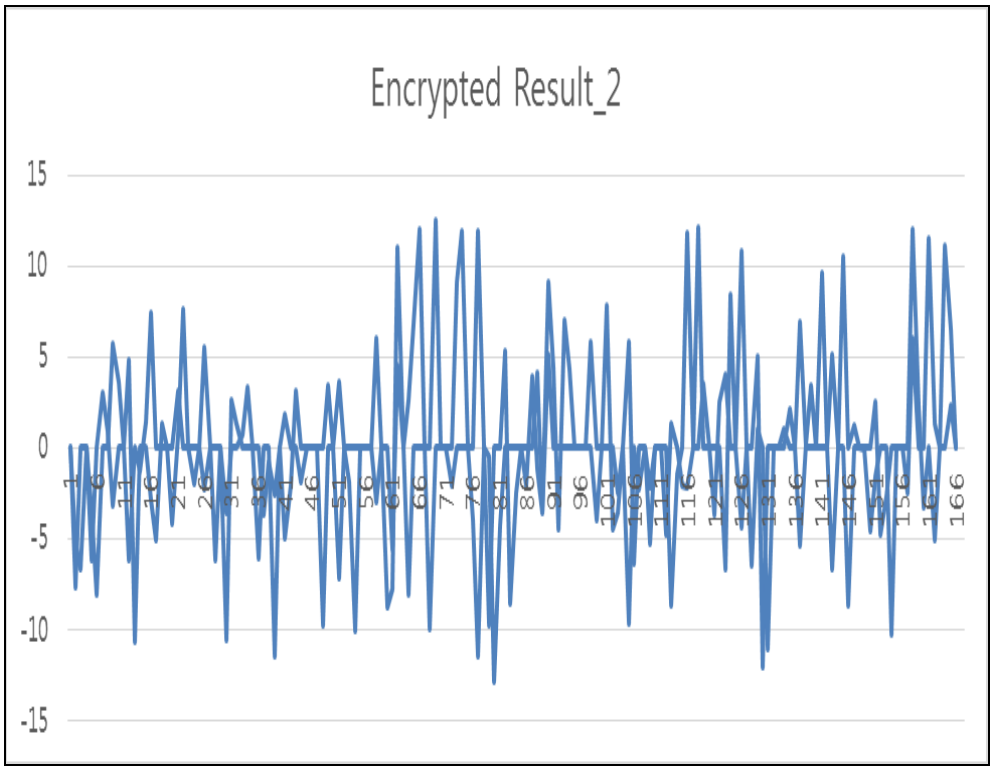

Figure 6. The Second Result of the First Method

4.2. Encryption Processing Time

Table 1 shows the results of the encryption processing time on two proposed methods. The parallel processing time is shorter than encryption processing time. Also, the first method has good encryption processing time than the second method. The reason is that a nonlinear method is used for collecting the information during the XOR operation execution on brain wave using chaos map. However, the security of the second method is good than the first method.

Table 3. Processing Time

Encryption method	Encryption processing time	Parallel encryption processing time
First	0.005262 (sec)	0.004204 (sec)
Second	0.007989 (sec)	0.006358 (sec)

5. Conclusions and Future Study

In this paper, we proposed two efficient parallel encryption methods using five phase chaos maps and adaptive junk data on brain wave signals for user authentication in real time. The first method use the fixed block size of brain wave and use variable block size of junk data. The second method use variable block size of brain wave and variable block size of junk data. A chaos map generates random numbers that may not easily predict a statistical analysis in authentication system. . As I said before, the encryption results are different because the chaos map generated the random number per each operation. Especially, the person authentication using unstructured data requires the real-time processing. And many researchers have been developed the encryption method with fixed maps. However, it has better security that variable maps are used for generating the random number in chaos maps. As a result, the encrypted brain wave signal is produced well and the processing time for authentication is reasonable in real time. The parallel processing time is shorter than encryption processing time. Also, the first method has good encryption processing time than the second method. The reason is that a nonlinear method is used for collecting the information during the XOR operation execution on brain wave using chaos map. However, the security of the second method is good than the first method. In the future, we will develop a more efficient shift or matrix operation to generate a more secure encryption system on brain waves.

References

[1] J.-S. Kim and J.-Y. Chung, "EEG Encryption Scheme for a Person Authentication", Proc. of Applied Science and Engineering for Better Human Life, ASEHL Seris, Jeju, Korea, vol. 6, **(2016)** August 16-19, pp. 53-56.
[2] J.-S. Kim and J.-Y. Chung, "Development of Efficient Encryption Scheme on Brain-Waves Using Five Phase Choas Maps", IJFIS, vol. 16, no. 1, **(2016)**, pp. 59-63.
[3] J.-S. Kim and J.-Y. Chung, "An EEG Encryption Scheme for Authentication System Based on Brain Wave", Journal of Korea Multimedia Society, vol. 18, no. 3, **(2015)**, pp. 330-338.
[4] D. D. Patil, N. A. Nemade and K. M. Attarde, "Iris Recognition Using Fuzzy System", *IJCSMS*, vol. 2, Issue. 3, **(2013)**, pp. 14-17.

[5] W. Khalifa, A. Salem, M. Roushdy and K, Revett, "A Survey of EEG based user authentication schemes", *The 8th International Conference on INFOrmatics and Systems(INFOS2012), IEEE,* pp. 55-66.
[6] C. F. Lin, S. H. Shih, J. D. Zhu and S. H. Lee, "Implementation of An Offline Chaos-based EEG Encryption Software", *Advanced Communication Technology (ICACT) 14th Int. Conf*, **(2012)**, pp. 430-433.
[7] C. F. Lin, S. H. Shih, J. D. Zhu, S. H. Lee and C.W. Liu, "C# based EEG encryption system using chaos algorithm", *Proc. 1st Int. Conf. Compl. Syst. Chaos (COSC'13)*, **(2013)**.
[8] C. F. Lin and C. H. Chung, "A chaos-based visual encryption mechanism in integrated ECG/EEG medical signals", *Advanced Communication Technology ICACT 10th Int Conf*, vol. 3, **(2008)**, IEEE.
[9] C. Ashby, A. Bhatia, F. Tenore and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication", *In Neural Engineering (NER), 5th International IEEE/EMBS Conf*, **(2011)**, pp. 442-445.
[10] A. Zúquete, B. Quintela and J.P. da Silva Cunha, "Biometric Authentication using Brain Responses to Visual Stimuli", *BIOSIGNALS*, **(2011)**, pp. 103-112.
[11] C. Shannon, "Communication Theory of Secrecy Systems", *Bell Systems Journal*, vol. 28, **(1949)**, pp. 659–715.
[12] W. Stallings, "Network security essentials: applications and standards", **(2013)**.
[13] S. Bensegueni and A. Bennia, "ECG Signal Compression Using a Sinusoidal Transformation of Principal Components", IJSEIA, vol. 10, no. 1, **(2016)**, pp. 59-68.

Authors

Jung-Sook Kim, received the B.S., M.S., and Ph.D. degrees in computer engineering from Dongguk University, Seoul, Korea in 1993, 1995 and 1999, respectively. She is a professor in school of Smart IT at Kimpo University. Her research interests include in the fields of intelligent systems, IT convergence, and distributed and parallel system.

Jang-young Chung, received a B.S. degree in Computer & Information Security from Deajeon University, Deajeon, Korea in 2006, and received the M.S. and Ph. D. degree in computer engineering from Dongguk University, Seoul, Korea in 2009 and 2015. He is a manager in IoT convergence Lab. at Penta Security Systems Inc.. His research interests include image security, authentication protocol, data privacy, parallel encryption, cloud security, and biometric security.

