Original Article
International Journal of Fuzzy Logic and Intelligent Systems
Vol. 16, No. 1, March 2016, pp. 59-63
http://dx.doi.org/10.5391/IJFIS.2016.16.1.59

ISSN(Print) 1598-2645
ISSN(Online) 2093-744X

Development of Efficient Encryption Scheme on Brain-Waves Using Five Phase Chaos Maps

Jung-Sook Kim[1] and Jang-Young Chung[2]
[1]School of Smart IT, Kimpo University, Gimpo, Korea
[2]Penta Security Systems Inc., Seoul, Korea

ljfis

Abstract

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. However, if 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. In addition, the dataset containing the brain-wave signals is large and the transfer time is long. However, user authentication requires a real-time processing, and an encryption scheme on brain-wave signals is necessary. In this paper, we propose an efficient encryption scheme using a chaos map and adaptive junk data on the brain-wave signals for user authentication. As a result, the encrypted brain-wave signals are produced and the processing time for authentication is reasonable in real-time.

Keywords: Adaptive junk data, Brain-wave, Chaos maps, Encryption scheme, User authentication system

1. Introduction

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. The uniqueness of the brain wave signals is particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain at the backside of the head is the best place to measure brainwaves, related to the visual sense. A brain wave signal is a unique physiological characteristic of an individual. A number of published reports have indicated that there is sufficient depth in the recording of brain wave signals, rendering it suitable as a tool for person authentication. Person authentication aims to accept or to reject a person claiming an identity, i.e., comparing a biometric data to one template. The need for a new behavioral biometric is derived from the need to secure important facilities and information. Most of the security systems on the market can be penetrated by hacking or a mistake by one the authorized personnel. The advantage of using brain-wave signals is that they satisfy all of the above-mentioned requirements, unlike other techniques. The use of brain

Received: Mar. 4, 2016
Revised : Mar. 22, 2016
Accepted: Mar. 24, 2016

Correspondence to: Jung-Sook Kim
(kimjs@kimpo.ac.kr)

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 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. 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. Furthermore, a brain wave is a highly correlated and a hacker can easily obtain the information. As a result, a fast encryption method is required for user authentication [1-12]. In this paper, we propose an efficient encryption scheme using chaos maps and adaptive junk data on the brain wave signals for person authentication in real-time. The process of the encryption scheme consists of five phases.

The structure of this paper is organized as follows: In Section 2, we briefly present the related works. Section 3 describes the brain wave encryption scheme using chaos maps and adaptive junk data for person authentication and Section 4 presents the experimental results. Finally, the conclusions and plans for future study are discussed in Section 5.

2. Related Works

2.1 Image Encryption Based on Chaotic Maps

The adaptation of certain invertible chaotic 2D maps on a torus or square is shown to create new symmetric block encryption schemes. These schemes are especially useful encrypting large amounts of data; such as digital images or electronic databases. A chaotic map is first generalized by introducing parameters and then discretized to a finite square lattice of points that represent pixels or some other items of data. Although the discretized map is a permutation and thus cannot be chaotic, it shares a certain sensitivity and mixing properties with its continuous counterpart as long as the number of iterations remains small. It is shown that the permutations behave as typical random permutations for the 2D baker map. The discretized map is further extended to 3D and consists of a simple diffusion mechanism. As a result, a block product encryption scheme is obtained. To encrypt an N×N image, a ciphering map is iteratively applied to the image. This paper repots an extension of the work of Pichler and Scharinger, who first introduced encryption schemes based on a 2D Baker map [4].

2.2 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. Encryption Scheme Using Five Phase Chaos Maps

We developed an encryption scheme that transforms the positive signals into negative signals in order using a chaos map and adaptive junk data for person authentication system. The process of the encryption scheme consists of five phases. First, the brain wave and a secret key are generated. Then, the first chaos map is generated to divide the brain-wave signals into several blocks. The size of blocks is fixed 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 executes an XOR operation. Next, a permutation operates on each brain

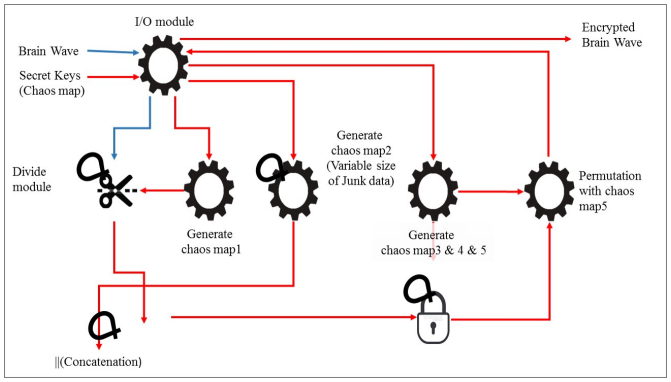

Figure 1. Encryption scheme on a brain-wave.

Table 1. Values of a and x_n

	a	x_n
Experiment # 1	3.58	0.73
Experiment # 2	3.68	0.83
Experiment # 3	3.78	0.93

wave block using the fourth chaos map. Finally, the fifth chaos map executes the permutation on the brain wave. As a result, an encrypted brain-wave is produced. Figure 1 shows the system structure.

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.

Next, the junk data are generated using Eq. (2) and inserted into the brain-wave signals by Eq. (3). The value of y in Eq. (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 Eq. (2) is fixed and defined by the user. The value of z in experiment is 10.

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

$$\text{For}(i < \text{the size of junk data})$$

$$\{\text{junk}[i] = X_n + 1\} \tag{3}$$

The brain wave signals are encrypted as follows by the chaos map

$$\text{Encrypted data} = ((\texttt{Brain-Wave}[\,] \times 10^9)\texttt{Xor}X_{n+1} \times 10^9 \text{ MOD prime number})/10^9. \tag{4}$$

Table 2. Words

	Positive brain-wave	Negative brain-wave
Word 1	Mother	Wrtrweyio
Word 2	Father	Bnkcktry
Word 3	Korea	Aewrqw
Word 4	Seoul	Sdfasdf

Table 3. Initial values

	X_0	X_1
Experiment # 1	0.78123456789	3.781234567891
Experiment # 2	0.88123456789	3.781234567891
Experiment # 3	0.91123456789	3.781234567891

4. Implementation and Results

The system was implemented using Visual Studio 2010 C#, MATHLAB 2010, Neuroscan, and E-Prime on a computer equipped with an Intel CPU running at i7 3.07 GHz, 6 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 listed in Table 2 and the initial values for the experiments are summarized in Table 3.

Figure 2 shows a positive brain-wave signal.

Figure 3 shows the encrypted results on the positive signals of the Figure 1 using the initial values of the experiment # 1 in Table 3

Figure 4 shows the encrypted result on the positive signals of the Figure 1 using the initial values of the experiment # 2 in Table 3.

The following Figure 5 shows the encrypted result on the positive signals of the Figure 1 using the initial values of experiment # 3 in Table 3.

In addition, we measured the processing time for encryption

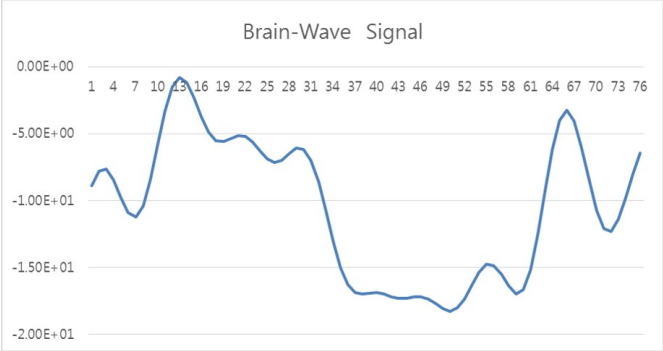

Figure 2. Positive brain wave signal.

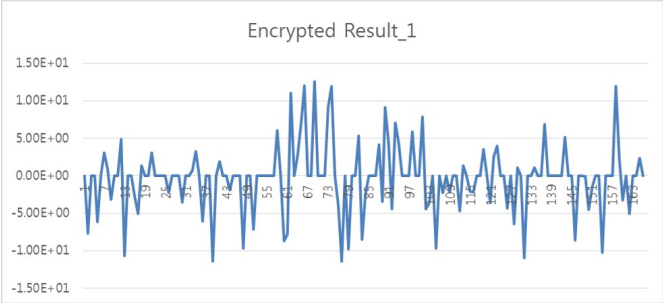

Figure 3. Encrypted result_1.

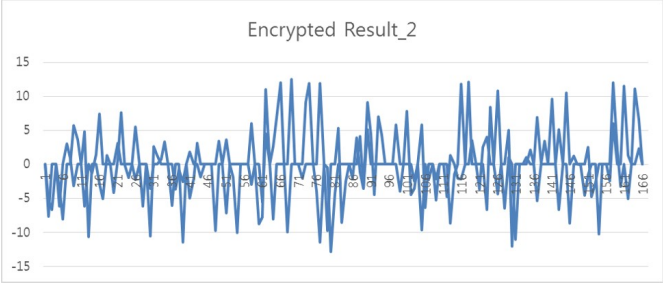

Figure 4. Encrypted result_2.

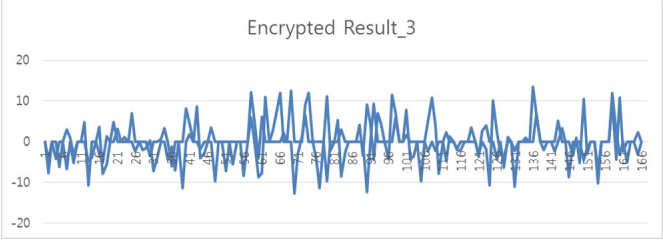

Figure 5. Encrypted result_3.

and compared it with the time for the AES encryption scheme. AES is very popular and based on information theory by Claude Elwood Shannon. The experiment was repeated 1,000 times. The average processing times of the proposed method and AES are 0.0001748 and AES is 0.0005466 ms respectively. The proposed method is faster than AES and is sufficient for person authentication.

5. Conclusions and Future Research

Person authentication aims to accept or to reject a person claiming an identity, i.e., comparing a biometric data to one template. The need for a new behavioral biometric is derived from the need to secure important facilities and information. Secondary damage to the user is a problem in biometrics. A brain wave signal is a unique physiological characteristic of an individual. Moreover, the brain wave has no shape and a malicious user may not cause secondary damage to a user. However, user authentication requires real time processing and an encryption scheme on brain wave signals is necessary. In this paper, we proposed an efficient encryption scheme using five phase chaos maps and adaptive junk data on brain wave signals for user authentication in real time. A chaos map generates random numbers that may not easily predict a statistical analysis in authentication system. As a result, the encrypted brain wave signal is produced and the processing time for authentication is reasonable in real time. We will develop a more efficient permutation operation to generate a more secure encryption system on brain waves.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgements

This work was supported by Research Fund of Kimpo University in 2016.

References

[1] 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, pp. 330-338, 2015. http://dx.doi.org/10.9717/kmms.2015.18.3.330

[2] D. D. Patil, N. A. Nemade, and K. M. Attarde, “Iris recognition using fuzzy system,” *International Journal of Com-*

puter Science and Mobile Computing, vol. 2, no. 3, pp. 14-17, 2013.

[3] W. Khalifa, A. Salem, M. Roushdy, and K. Revett, "A survey of EEG based user authentication schemes," in *Proceedings of the 8th International Conference on Informatics and Systems (INFOS'12)*, Cairo, Egypt, 2012, pp. 55-60.

[4] J. Fridrich, "Image encryption based on chaotic maps," in *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, Orlando, FL, 1997, pp. 1105-1110. http://dx.doi.org/10.1109/ICSMC.1997.638097

[5] C. F. Lin, S. H. Shih, J. D. Zhu, and S. H. Lee, "Implementation of an offline chaos-based EEG encryption software," in *Proceedings of 14th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, Korea, 2012, pp.430-433.

[6] C. F. Lin, S. H. Shih, J. D. Zhu, S. H. Lee, and C. W. Liu, "C# Based EEG Encryption System Using Chaos Algorithm," in *Proceedings of the 1st WSEAS International Conference on Complex Systems and Chaos (COSC'13)*, Morioka, Japan, 2013.

[7] C. F. Lin and C. H. Chung, "A chaos-based visual encryption mechanism in integrated ECG/EEG medical signals," in *Proceedings of 10th International Conference on Advanced Communication Technology (ICACT'08*), Gangwon-do, Korea, 2008, pp. 1903-1907. http://dx.doi.org/10.1109/ICACT.2008.4494157

[8] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost electroencephalogram (EEG) based authentication," in *Proceedings of 5th International IEEE/EMBS Conference on Neural Engineering (NER),* Cancun, Mexico, 2011, pp. 442-445. http://dx.doi.org/10.1109/NER.2011.5910581

[9] A. Zuquete, B. Quintela, and J. P. S. Cunha, "Biometric authentication using brain responses to visual stimuli," in *Proceedings of the 3rd International Conference on Bio-inspired Systems and Signal Processing (Biosignals2000)*, Valencia, Spain, 2010, pp. 103-112.

[10] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949. http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x

[11] W. Stallings, *Network Security Essentials: Applications and Standards*, 5th ed. Upper Saddle River, NJ: Pearson Education, 2013.

[12] T. J. Lee and K. B. Sim, "EEG based vowel feature extraction for speech recognition system using international phonetic alphabet," *Journal of Korean Institute of Intelligent Systems*, vol. 24, no. 1, pp. 90-95, 2014. http://dx.doi.org/10.5391/JKIIS.2014.24.1.090

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.

E-mail: kimjs@kimpo.ac.kr

Jang-Young Chung received a B.S. degree in Computer & Information Security from Deajeon University, Deajeon, Korea in 2006, and received a M.S. degree in computer engineering from Dongguk University, Seoul, Korea in 2009. 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.

E-mail: sd109@dongguk.edu