Journal of Korea Multimedia Society Vol. 18, No. 3, March 2015(pp. 330-338)
http://dx.doi.org/10.9717/kmms.2015.18.3.330

뇌파 기반의 인증시스템을 위한 EEG 암호화 기법

김정숙†, 정장영††

An EEG Encryption Scheme for Authentication System based on Brain Wave

Jung-Sook Kim†, Jang-Young Chung††

ABSTRACT

Gradually increasing the value of the technology, the techniques of the various security systems to protect the core technology have been developed. The proposed security scheme, which uses both a Password and the various devices, is always open by malicious user. In order to solve that problem, the biometric authentication systems are introduced but they have a problem which is the secondary damage to the user. So, the authentication methods using EEG(Electroencephalography) signals were developed. However, the size of EEG signals is big and it cause a lot of problems for the real-time authentication. And the encryption method is necessary. In this paper, we proposed an efficient real-time authentication system applied encryption scheme with junk data using chaos map on the EEG signals.

Key words: EEG(Electroencephalography), Authentication System, Chaos Map, XOR Operation, Encryption, Brain Wave

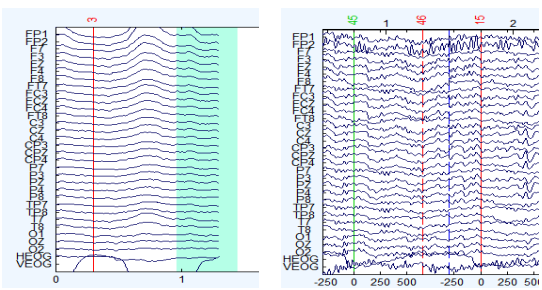
1. 서 론

점차 기술의 가치가 높아짐에 따라 핵심기술을 보호하기 위해 다양한 보안시스템의 기술이 날로 발전하고 있다. 현재 개발되고 있는 보안 시스템의 기술들은 사용자 인증 과정을 위해 비밀번호(password)와 다양한 정보를 함께 사용하여 인증하고 핵심기술을 보호한다. EMC사는 리스크기반 인증(risk-based authentication)이라는 새로운 방식의 인증기술을 선보였다. 이 기술은 사용자의 정상적인 행동의 데이터를 만들고, 그 데이터를 기반으로 이용자가 평상시와 다른 장소에서 로그인을 하거나 다른 컴퓨터를 사용하는 등 특이한 행동을 하면 위험점수가 올라가서 전화 확인 등의 추가 인증을 요구하는 방식이다. 하지만 이러한 인증시스템은 인증 시 사용되는 다양한 정보들이 도난 및 발췌가 가능한 정보들이어서 악의적인 사용자로 하여금 표적이 될 수 있다. 그리고 최근에는 디바이스를 이용한 인증시스템도 널리 사용되고 있다. 그 예로 구글에서 새로운 보안토근(hardware token)을 시범 운영하고 있다. 보안토근은 비밀번호를 재입력하는 과정 없이 USB 포트에 꽂거나 근거리무선통신(NFC)을 이용하여 모바일 기기에 터치만 하면 인증이 된다. 이는 분실의 위험이 존재하고 있으며, 사용자가 인지하고 있지 않은 상태에서 분실이 이뤄질 가능성도 있기 때문에 위험하다. 이러한 위험으로 인해 각막, 지문, 혈관, 안면, DNA 등을 이용한 바이오 메트릭(biometric) 기반의 인증시스템들이 개발되어 사용되고 있다[1]. 바이오 메트릭 기반의 생체인식 인증시스템은 타인에 의해 도용될 수 있는 확률이 낮아 비밀번호 인증보다 안전한 것으

※ Corresponding Author : Jung-Sook Kim, Address: (415-761) 97, Gimpodaehak-ro, Wolgot-myun, Gimpo-si, Geyonggi-do, Korea, TEL : +82-31-999-4659, FAX : +82-31-999-4775, E-mail : kimjs@kimpo.ac.kr
Receipt date : Jan. 9, 2015, Approval date : Feb. 8, 2015

† Division of SmartIT, Kimpo University
†† Dept. of Computer Eng., Dongguk University
(E-mail : sd109@dongguk.edu)
※ This work was supported by Research Fund of Kimpo University in 2015.

로 생각되어 왔지만 시스템을 도입하는데 많은 비용이 소요되고 느리다는 단점을 가지고 있다. 뿐만 아니라 악의적인 사용자가 인증 시스템 사용자에게 직접적인 신체의 피해를 입힐 수 있고 이로 인해 핵심 기술 유출 외에도 사용자에게 2차적인 피해까지 입힐 수 있다. 따라서 바이오 메트릭 기반의 인증시스템을 이용하면서도 사용자에게 2차적인 피해를 줄일 수 있는 기술이 필요하다. 이에 본 논문에서는 바이오 메트릭 중에서 유출 위험성이 적은 뇌파 데이터(EEG, Electro Encephalo Graphy)를 이용하여 인증 시스템을 제안하고 이를 구현하였다. 뇌파 데이터의 경우 무형의 데이터이고 외부적으로 보이지 않은 데이터이기 때문에 사용자의 2차 피해를 줄일 수 있고, 도난이나 유출이 될 가능성이 적다. 그러나 뇌파 데이터를 이용하는 경우, 실시간으로 인증이 가능해야 하나 뇌파 데이터의 양이 너무 방대하다. 2분 동안 측정된 뇌파데이터의 양이 100MB 이상이 되며, Fig. 1의 (a)와 (b)처럼 뇌파의 종류가 포지티브와 네거티브 데이터 두 가지 종류가 있다. 이 때 뇌파 데이터를 중간에서 캡쳐하여 데이터를 분석하여 재생공격이나 기타 공격이 가능하다. 즉 포지티브 데이터와 네거티브 데이터는 그 차이가 분명하게 나타나며, 따라서 악의적인 공격자가 쉽게 분별이 가능하다. 따라서 뇌파 데이터로 인증을 할 경우 기밀성을 보장하기 위해 암호화 기법이 필요하다. 하지만 기존의 암호화 알고리즘인 AES, RSA, ECC 등을 적용하게 되면 많은 문제점이 발생될 수 있다. 그 이유는 먼저 뇌파 데이터가 대용량 데이터로 근접 데이터의 상관계수가 높아 유추하기가 쉽다. 그리고 대용량 데이터인 경우 데이터의 양으로 통계적 공격을 하기 쉽다. 마지막으로 대용량 데이터의 암호화하는데 많은 오버헤드가 발생한다. 따라서 뇌파 같이 대용량의 데이터를 이용하여 실시간으로 인증을 할 경우, 속도가 빠른 암호화 기법이 필요하다. 이에 본 논문에서는 실시간으로 인증이 가능하도록 뇌파 데이터에 카오스 맵을 이용한 XOR 연산을 수행하여 암호화하는 기법을 제안하였다. 시뮬레이션 한 결과 뇌파 데이터가 무질서한 형태를 보여 악의적인 공격자가 확인하거나 분석 시 어려움이 있는 네거티브한 뇌파 데이터의 형태를 보였다. 그리고 인증은 실시간으로 이루어져야 의미 있는 사용이라고 할 수 있으며, 본 논문에서 제안한 기법을 시뮬레이션 한 결과 실시간으로 인증이 가능함을 보여 주었다. 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구를 살펴하고 3장에서 뇌파 데이터를 이용한 인증 프로토콜을 제안하며, 4장에서 실험한 내용과 결과를 기술하고 마지막으로 5장에서 결론을 내리고 향후 연구 방향을 살펴본다.



(a) Stable EEG (Positive EEG)　　(b) Unstable EEG (Negative EEG)

Fig. 1. (a) Stable EEG(Positive EEG) (b) Unstable EEG (Negative EEG).

2. 관련 연구

2.1 EEG(Electro Encephalo Graphy)

EEG는 뇌의 활동을 기록하는 기법으로 이와 비슷한 기법은 FMRI(Functional Magnetic Resonandce Imaging)와 MEG(Magnetoencephalography) 등이 있다. 이러한 뇌파는 4개의 사인파로 구성되어있으며, 다음의 Table 1과 같다. 측정은 약 0.5~100μV 자극을 출력하여 표시한다.

2.2 뇌파 기반의 인증 시스템들

Riera 등이 제안한 멀티모달 인증 알고리즘은 EEG와 ECG(Electrocardiography) 신호를 기반으로 제안되었다[2]. 뇌파 신호를 각 변화마다 측정하여 푸리에 변화를 이용하여 이용한 인증방법이다. 이 기법은 97.9% 의 인증 성공률을 가지고 있다. 하지만 측정 방법이 32개의 채널을 이용하였으며, 이로 인해

Table 1. Types of Brain wave

Types	Contents
Alpha	8-13 Hz Breaking
Beta	4-7.5 Hz Wake
Theta	16-26 Hz Sorking
Delta	05-4 Hz Sleep

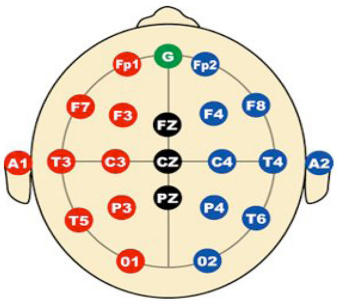


Fig. 2. Standard electrode position.

많은 계산량을 필요로 한다. 그리고 Palaniappan 등이 제안한 멀티플 멘탈 인식 모델 기법은 뇌파 측정 시 전극의 위치별로 신호를 모아 측정하는 기법이다[2]. 뇌파 측정 시 다음의 Fig. 2에 있는 C3, C4, P3, P4, O1, O2의 전극 위치로부터 전기신호를 받아서 측정하는 것으로서 측정된 벡터정보를 이용해서 인증을 하게 된다. Cempirek 등이 제안한 기법은 신경네트워크를 이용한 기법이다[2]. 180초 동안의 뇌파 기록을 통해서 22.5초 단위로 분할하고 이 데이터를 통해서 인증을 하게 된다. 또한 데이터 가중치가 더해져서 이를 이용한 매칭과정에서 인증을 하게 된다. Sun이 제안한 기법은 신경망 네트워크를 통해서 인증을 하는 기법이다. 이 기법의 경우 이미지와 같은 데이터를 사용자에게 인지 시키고 반응시간을 측정하고 반응할 때의 데이터에서 데이터를 분석하고 이를 이용하여 인증하는 방법이다. 하지만 위의 연구들은 순수하게 뇌파의 데이터만을 가공하지 않고 이용하기 때문에 악의적인 공격자에게 노출될 경우 재사용의 문제가 남아있다. 이에 사용될 뇌파 데이터가 노출이 되더라도 악의적인 사용자에게 혼돈을 줄 기법이 필요하다[2].

2.3 카오스 기반의 EEG 암호화 기법들

카오스 맵의 특징은 초기입력 값과 입력되는 파라미터에 의해서 민감한 결과를 보이며, 결과들이 균일한 분포를 보이는 것이 특징이다. 가장 많이 사용되는 로지스틱 맵(Logistic Map)의 경우 개체수의 변화량을 수학적으로 처리한 것으로서 암호학 분야에서 널리 사용되었다[3,4,5]. 로지스틱 맵 함수 $x_{n+1}=\lambda x_n(1-x_n)$을 이용한 것으로, 이때 λ($3.57 < \lambda < 4$)와 x_0($0 < x_0 < 1$)를 두 개의 값으로 정의하여 사용한다.

0 < 증가율 ≦ 1
  다음 개체 수는 0으로 수렴
1 < 증가율 ≦ 2
  다음 개체 수는 1 - (1 / α)로 수렴 (1)
2 < 증가율 ≦ 3.5699
  다음 개체 수는 주기배가 상태
3.5699 < 증가율 < 4
  다음 개체 수는 혼돈 상태

로지스틱 맵 외에 가장 많이 사용되는 맵으로서 텐트 맵(Tent Map)이 있다. 텐트맵은 일차원의 부분함수이며, 로지스틱 맵과 같이 0과 1구간의 정의역을 가지고 있다.

$$f_\alpha(x)=\begin{cases}\dfrac{x}{\alpha}, & 0\le x\le\alpha\\ \dfrac{x-1}{\alpha-1}, & \alpha<x\le 1\end{cases} \quad (2)$$

$$f_\alpha^{-1}(y)=\alpha y \quad \text{or} \quad 1+(\alpha-1)y$$

텐트맵 역시 카오스 맵의 특징인 초기 값과 입력 파라미터에 의한 민감성과 균등성을 가지고 있기 때문에 많은 분야에서 사용되고 있다[3-5]. 기존의 DES와 AES의 경우 텍스트 데이터를 위한 암호화 알고리즘들이었으며, 데이터양이 많은 EEG나 이미지 그리고 영상정보에서는 계산량과 시간 오버헤드가 발생하기 때문에 이를 해결하기 위한 카오스 맵을 기반으로 한 EEG 암호화 기법들이 제안되었다. Lin등은 2012년 오프라인에서 사용가능한 C#으로 작성한 카오스 맵 기반 암호화 기법을 제안하였다. 제안된 기법의 경우 사용되는 카오스 맵의 파라미터 사용범위를 지정하여 암호화되는 EEG 데이터를 암호화 레벨별로 다룬 점이 특징이다[6-8]. 하지만 오프라인 기반에서 제안된 기법이며, 암호화 레벨에 중점을 두어 암호화 과정을 진행했기 때문에 실시간 인증에서 사용되기에는 검증과정이 필요하다. 그리고 2009년 1차원 카오스 맵을 이용한 스크램블링 기반의 EEG 암호화 기법을 제안한 바 있다. 하지만 카오스 맵 기반에서 스크램블링을 하여 암호화를 진행할 경우 정렬 알고리즘이 사용된다. 하지만 역 정렬 시에 정렬과 역 정렬의 과정을 거쳐야 하며, 이는 계산 량과 시간 오버헤드가 발생한다. 스크램블링에 관한 오버헤드 문제는 이미 카오스 맵 기반의 암호화 기법에서 문제가 제기된 적이 있으며, 이를 해결하기 위한 병

렬기법이 제안된 사례가 있다[5].

2.4 카오스 기반의 인증 시스템

Ashby등은 EEG 데이터를 이용하여 인증하기 위해 SVM을 이용하여 오류율을 줄이고자 하였다.

EEG 데이터가 항상 같은 데이터를 가지지 않는 특징을 기반으로 하여 인증을 하고자 하였고 이때 SVM을 이용하여 오류율에 관한 문제를 해결하고자 했다. Ashby등이 제안한 방법은 150초 동안에 기록을 하고 EEG 데이터에서 자기회기 계수 외 3가지 특징을 추출해서 보관한다. 보관 된 데이터는 SVM 트레이닝을 통해 사용할 수 있는 데이터로 추출하고 이를 정규화 한다[9]. 정규화 된 데이터는 인증 시 사용된다. 그 외에 Zúquete등과 Marcel등도 EEG 데이터를 이용하여 인증 시스템을 제안하였다[10]. 하지만 이들의 시스템은 EEG 데이터의 오류율에 초점을 맞췄을 뿐 다양한 공격으로 부터 강성에 대한 검증은 이뤄지지 않았다.

2.5 샤논의 정보이론

사논(Claude Elwood Shannon)의 정보이론은 불확실성과 불예측성에 관한 이론으로 카오스 맵은 이런 유사한 성질을 가지고 있으며 혼돈과 확산 성질을 만족해야 한다. 혼돈은 연관성 또는 통계적 패턴 관계성을 낮게 하기 위함이며, 키와 암호화된 평문과의 관계를 복잡하게 하기 위해서이다. 그리고 확산은 평문의 정보들이 암호문에 영향을 주는 것을 말한다. 이 성질들 중 한 가지만 만족할 경우 효과가 낮을 뿐 아니라 공격에 노출되기 쉬우며, 두 가지 성질을 만족하여야 좋은 보안 기법이 될 수 있다[3-5,11,12].

그리고 뇌파 데이터를 이용한 인증시스템의 편리성에 관한 연구도 같이 진행되어야 한다[13].

3. 정크데이터를 가진 EEG 암호화 기법

EEG 데이터는 양이 매우 방대하기 때문에 강성이 강한 암호화를 수행하기 위해 혼돈과 확산 이 두 성질을 동시에 만족시키는 카오스 맵을 이용하여 순열과 치환과정을 수행하면서 암호화 과정을 거칠 경우 연산을 하는 계산과 시간 오버 헤드가 발생한다. 따라서 본 논문에서는 실시간 인증에 효율적으로 사용될 수 있는 EEG 암호화 기법을 제안하고, 실시간으로 인증이 될 수 있는지에 대한 검증 과정을 거쳤다. 다음의 Fig. 3은 본 논문에서 제안한 기법의 구조도를 보여 주고 있다.

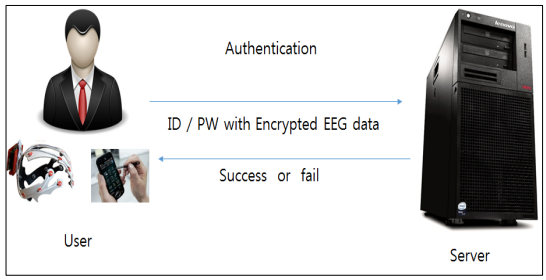


Fig. 3. Framework of the authentication using EEG.

사용자는 인증을 위해서 자신이 사용하게 될 이미지나 단어를 보고 뇌파를 저장하게 되며, 이때 기록된 뇌파는 최소 100회 이상의 표본에서 평균값을 구해서 이용한다. 그리고 인증 과정에서 사용자는 자신의 뇌파 기록 시 사용된 동일한 이미지나 단어를 연상하여 뇌파 정보를 사용한다. 하지만 이때 사용자의 뇌파는 포지티브 한 데이터이기 때문에 악의적인 사용자가 쉽게 알 수가 있다. 따라서 본 논문에서는 사용자의 뇌파 데이터 인증 시 악의적인 사용자가 인지하게 어렵게 하기 위해 카오스 맵을 이용해서 포지티브 데이터를 네거티브하게 변환하여 사용하고자 한다. 이때 실시간 인증과정에서 사용될 수 있도록 카오스 맵을 적용한 과정에서 계산과 시간이 많이 필요한 순열과정 대신에 EEG 정보 사이에 정크 데이터를 삽입한다. 본 논문에서 사용된 카오스 식은 다음 식 (3)과 같다.

$$x_{n+1} = a x_n (1 - x_n) \quad a = 3.59,\ x_1 = 0.8 \tag{3}$$

다음의 Fig. 4는 본 논문에서 제안한 EEG 데이터가 암호화 키에 의해서 암호화 되는 과정을 개략적으로 표현한 것이며, 이를 단계별로 상세하게 기술하면 다음과 같다. 그림에서 카오스 맵은 EEG 데이터를 암호화하기도 하지만 무작위 위치에 삽입되는 정크 데이터 역시 생성하여 삽입하는 과정을 보여주고 있다.

① 사용자에게 사용자만 친숙한 이미지나 단어를 인지시킨다. 실험은 최소 100회 이상 실시한다.

② 이때 사용되는 뇌파데이터는 전체 표준 맵을 사용하지 않고, 위의 Fig. 2에서와 같이 자신이 원하는 위치의 데이터를 이용한다.

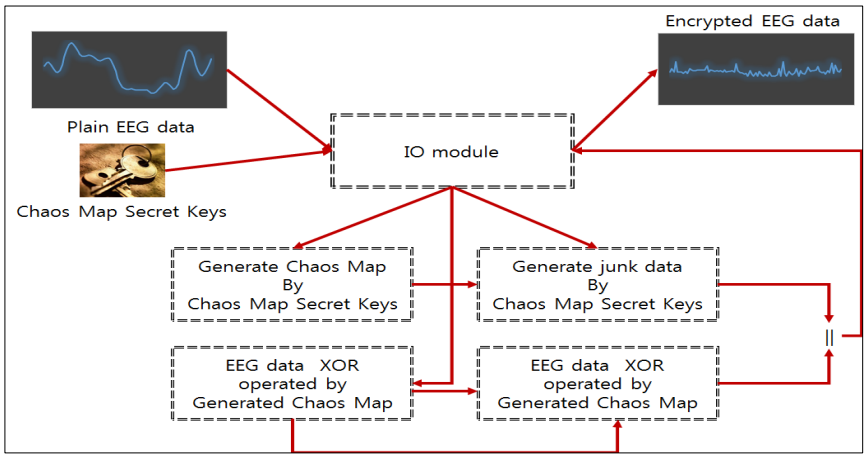


Fig. 4. Flowchart of the encryption using EEG.

③ 이렇게 얻은 데이터를 인증을 위한 데이터로 활용하며, 여기에 가중치를 더한 데이터를 사용한다.

④ 위의 ③의 데이터를 기준으로 400밀리 세컨드까지 측정 한 데이터를 저장한다. 사용자는 인증을 하기 위하여 자신이 선택한 위치의 자극을 측정하고 이 데이터를 카오스 맵을 이용한 난수와 XOR 연산을 수행하고, 다음의 식 (5)를 이용하여 정크 데이터를 생성하고 식 (6)에 의한 알고리즘에 의해 이를 삽입하여 서버에 보내게 된다.

⑤ 서버 측에서는 받은 데이터를 사용자와 서버만 알고 있는 카오스 맵 키를 이용해서 복호화 한다.

⑥ 뇌파 데이터가 오면 뇌파의 중간 값 그리고 n400, p300 등을 측정하여 유사도를 판단한다.

데이터의 암호화 과정은 식 (3)과 식 (4)를 이용하여 암호화 과정을 거친다.

$$x_{n+1} = ax_n(1-x_n)$$
$$Encrypted\,EEG\,Block_n = ((x_n \times random\,number) \bmod 256) \otimes EEG\,Block_n \quad (4)$$

정크 데이터를 구하기 위한 식은 아래의 식 5와 같이 연산되며, 정크데이터 입력은 사용자가 임의의 파라미터 입력과 mod 연산을 위한 파라미터로 구성된다. y의 정보는 0~255의 정보를 가지며 본 논문에서는 255를 이용하였다. y값에 따라 생성되는 정크데이터의 랜덤 값의 범위도 변한다.

$$x_{n+1} = ax_n(1-x_n)$$
$$junk_n = x_{n+1} \bmod y \quad (5)$$

다음의 식 6은 EEG 데이터 블록이 XOR 연산 후 정크 데이터의 삽입을 결정하는 알고리즘이다. 파라미터 Z의 경우 사용자 정의로 입력이 되며, 불규칙하게 입력이 된다.

$$x_{n+1} = ax_n(1-x_n)$$
$$\text{if}(junkn\%z \equiv 0)$$
$$insert\ junk_n\ into\ EEGdata \quad (6)$$

그리고 아래 Fig. (5)는 암호화된 뇌파 데이터에 정크데이터가 삽입된 EEG 데이터이다.

4. 실험 결과 및 고찰

본 논문에서 사용한 실험 환경은 Intel i7 3.07Ghz, Ram : 4GB, HDD : 1TB, language : visual studio 2010 C#, matlab 2010, 뉴로스캔, 그리고 E-Prime 이다. 실험은 먼저 본 논문에서 제안한 EEG 암호화 기법이 강성을 가질 수 있는지 검증하는 시뮬레이션 실험을 수행하였다. 그리고 암호화 하는 과정과 복호화 하는 과정의 시간을 측정하여 실시간으로 이루어져야 하는 인증시스템에서 사용할 수 있는지를 확인하였다. 시뮬레이션을 수행할 때 사용자에게 포지티

Table 2. Words for Positive and Negative EEG

	Positive EEG	Negative EEG
Word 1	어머니	김이부시닛다
Word 2	아버지	자기비멉
Word 3	한 국	구시잔소
Word 4	서 울	비김수주

브 EEG 데이터와 네거티브 EEG 데이터를 얻기 위해 사용한 단어 예는 다음 Table 2와 같다. 포지티브 EEG 데이터를 얻기 위해서 친숙한 단어를 사용하였으며 네거티브 EEG 데이터를 얻기 위해서는 랜덤하고 친숙하지 않은 단어를 사용하였다. 파일럿은 한명으로 하여 총 4개의 워드 당 100번씩 수행하여 데이터의 평균정보를 이용하였다. 시뮬레이션 할 때는 다음의 Table 2의 예들 중 워드 1의 EEG 데이터를 이용한 결과를 측정하고 분석하였다.

실험은 먼저 EEG 데이터에 정크 데이터를 삽입한 결과를 Fig. 5에서 보여주고 있다. 순열과정 대신에 카오스 맵을 기반으로 하여 임의의 위치에 정크 데이터가 삽입되는 것을 확인할 수 있으며, 위에서 제시한 식 5와 6에 의해서 생성과 삽입이 된다. 악의적인 사용자는 이를 구별하여 분석을 해야 하기 때문에 복호화 공격 시 강성을 가질 수 있다.

그리고 암호화 기법이 강성을 가지는지 실험한 결과, Fig. 6(a)의 경우는 위의 Fig. 2의 F4 위치의 포지티브 데이터이며 Fig. 6(b)은 로지스틱 맵을 적용한 결과이다. 사용자가 인증 시 사용한 그림이나 단어 등이 친숙할 경우 Fig. 6(a)와 같은 데이터가 측정이 될 것이며, 만약 악의적인 사용자가 사용할 경우 Fig. 6(b)가 측정이 된다. 뇌파 데이터의 경우 일정한 형식의 데이터이기 때문에 카오스 맵의 정보와 XOR 연

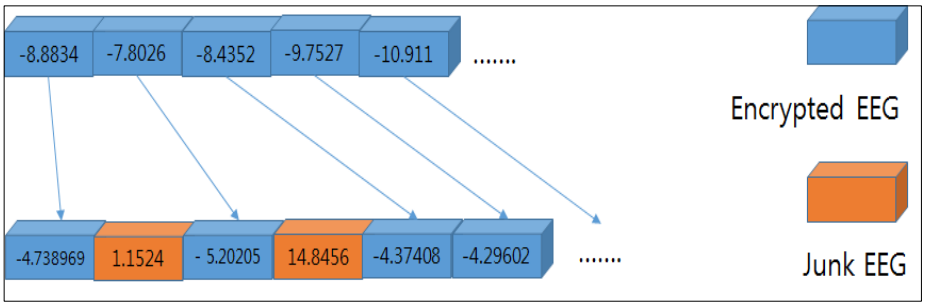


Fig. 5. Encrypted EEG and Junk EEG.

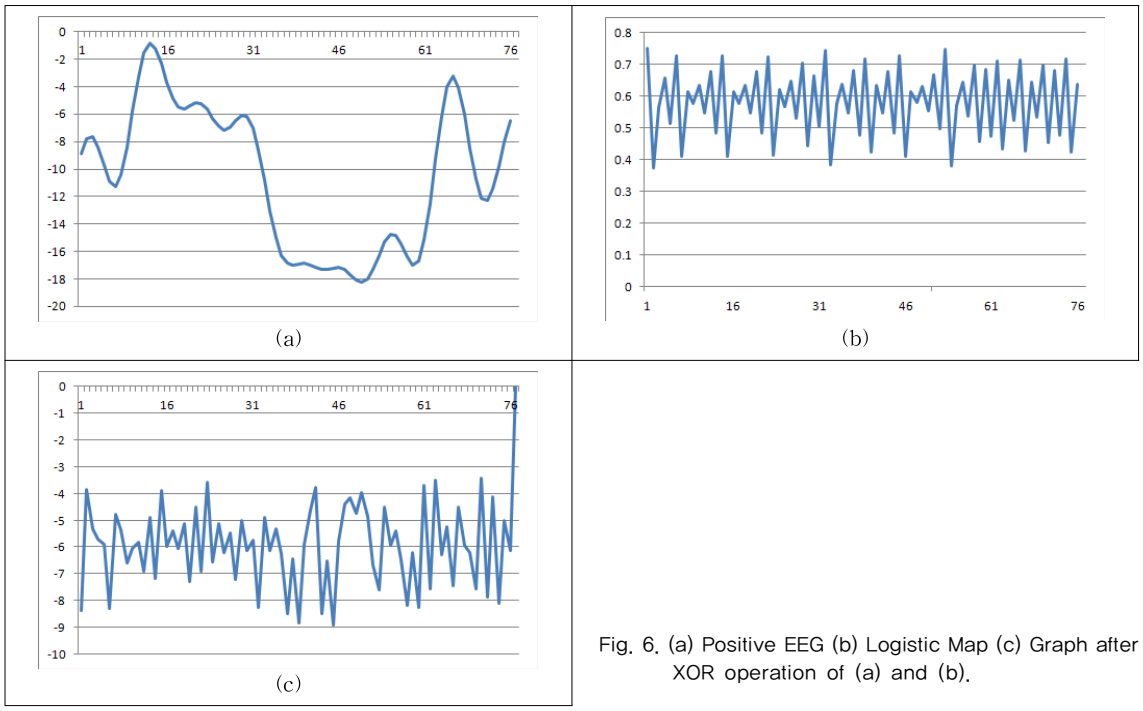


Fig. 6. (a) Positive EEG (b) Logistic Map (c) Graph after XOR operation of (a) and (b).

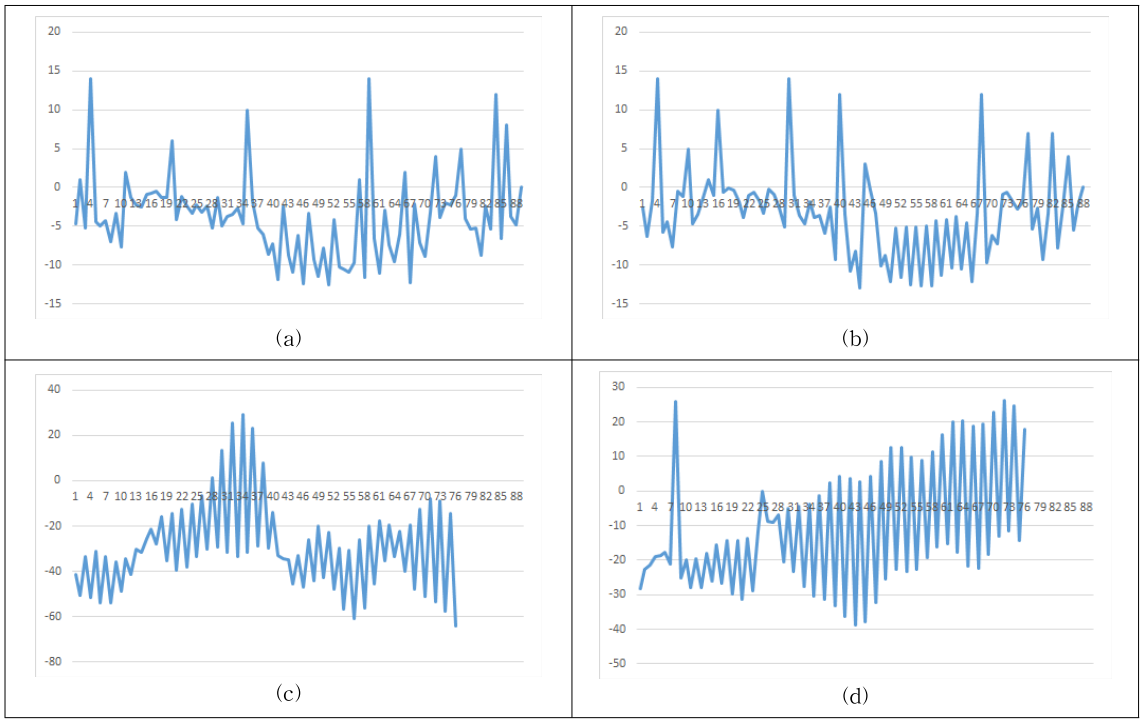


Fig. 7. (a) Eccrypted EEG 1, (b) Eccrypted EEG 1, (c) Negative EEG 1, (d) Negative EEG 2.

산을 할 경우 매번 같은 일정한 형식의 데이터가 나올 수 있다. 이때 악의적인 사용자는 유사성을 분석하여 복호화 시 어려움을 가질 수 있다. Fig. 6(c)는 위 2개의 데이터를 XOR 연산 후 데이터이며 Fig. 6(b)처럼 불안전한 즉 네거티브 데이터로 나타난다. 포지티브 데이터는 Fig. 6(a)처럼 부드러운 그래프를 그리며, 네거티브 그래프의 경우 Fig. 7(c)와 (d)처럼 급변하는 데이터로 표현이 된다. Fig. 6의 (c)가 Fig. 7의 (c)와 (d)의 특징을 가지고 있으며, 악의적인 사용자로 하여금 복호화 하는데 강성을 가진다. Fig. 7의 (a)와 (b)는 포지티브 EEG 데이터를 암호화 한 결과이며 (c)와 (d)는 EEG 네거티브 데이터이다. 암호화된 데이터와 네거티브 데이터를 비교한 것이다. Fig. 7번의 모든 데이터들이 Fig. 6의 (a)와 비교해보면 EEG 데이터의 변화량이 많은 불안한 형태인 네거티브 데이터로 보인다.

또한 인증시스템에서 사용할 수 있기 위해서는 실시간으로 인증이 가능해야 하므로 암호와 시간을 측정한 결과이다. 실험은 암호화 하는 과정의 시간을 측정하였으며, 약 1000회 암호화 과정 시간을 측정하였다. 평균 암호화 시간은 0초 0000353 밀리세컨드가 측정 되었으며, 복호화도 이와 비슷한 시간이 측정되었다. 그리고 비교 실험 결과 중 널리 사용되는 샤논의 정보 이론을 따른 AES의 경우 0초0005466 밀리세컨드가 측정이 되었다. 이는 본 논문에서 제안한 기법이 기존의 AES와 비교해 약 10배의 빠른 성능을 보인다. 따라서 실시간으로 이루어지는 인증시스템에 적용할 수 있으며, 다수의 사용자가 사용하여도 오버헤드 없이 사용이 가능함을 보여준다.

5. 결 론

본 논문에서는 바이오 메트릭 중에서 뇌파 데이터를 이용한 인증시스템을 제안하였고, 암호와 및 복호화 하는 시간이 빠른 암호와 기법을 개발하고 이를 시뮬레이션 하였다. 뇌파 데이터의 경우 무형의 데이터이고 외부적으로 보이지 않은 데이터이기 때문에 사용자의 2차 피해를 줄일 수 있고, 도난이나 유출이 될 가능성이 적다. 그러나 뇌파 데이터를 이용하는 경우, 뇌파 데이터의 양이 너무 방대하여 실시간으로 인증이 가능하려면 빠른 시간 내에 암호화 할 수 있는 기법이 필요하다. 따라서 본 논문에서는 EEG 데

이터를 인증 시 자신이 선택한 위치의 자극을 측정한 EEG 데이터를 측정하고 이 데이터를 카오스 맵을 이용한 난수와 XOR 연산을 수행하는 인증 기법을 제안하여 강성을 가지는 것을 확인하였고, 또한 EEG 데이터에 카오스 맵을 이용하여 암호화를 하지만, 암호화에서 순열과정 대신에 속도가 빠른 정크 데이터를 삽입하는 기법을 개발해 적용하였다. 이들을 적용한 암호화와 복호화 과정의 시간을 측정하였더니 샤논의 정보 이론을 따른 AES와 비교하여 실시간으로 인증이 가능한 암호화 기법을 적용한 결과를 보여준다. 하지만 아직 실제 시스템 구현이 되지 않았기 때문에 검증에 대한 문제가 남아있다. 향후 연구로는 다수의 사용자에 대한 데이터를 수집한 후 실제 시스템을 구현하여 제안 기법을 검증할 수 있도록 할 예정이다.

REFERENCES

[1] D.D. Patil, N.A. Nemade, and K.M. Attarde, "Iris Recognition using Fuzzy System," *International Journal of Computer Science and Management Studies*, Vol. 2, No. 3, pp. 14-17, 2013.

[2] W. Khalifa, A. Salem, M. Roushdy, and K, Revett, "A Survey of EEG based User Authentication Schemes," *Proceeding of The 8th International Conference on Inforrmatics and Systems,* pp. 55-60, 2012.

[3] J. FRIDRICH, "Image Encryption based on Chaotic Maps," *Proceeding of IEEE International Conference on Computational Cybernetics and Simulation,* pp. 1105-1110, 1997.

[4] J.Y. Chung and Y.S. Hong, "Encryption Scheme of Image Header Information for Security of Ultra High Resolution Images," *Proceeding of Korea Computer Congress 2012,* Vol. 39, No. 2C, pp. 107-109, 2012.

[5] J.Y. Chung and Y.S. Hong, "Parallel Image Encryption Schemes for Security of Ultra High Resolution Images," *Proceeding of Korea Computer Congress 2012,* Vol. 39, No. 1C, pp. 274-276, 2012.

[6] C.F. Lin, S.H Shih, J.D. Zhu, and S.H Lee, "Implementation of An Offline Chaos-based EEG Encryption Software," *Proceeding of Advanced Communication Technology International Conference*, pp. 430-433, 2012.

[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," *Proceeding of 1st International Conference Complex Systems and Chaos*, pp.59-62, 2013.

[8] C.F. Lin and C.H. Chung, "A Chaos-based Visual Encryption Mechanism in Integrated ECG/EEG Medical Signals," *Proceeding of Advanced Communication Technology ICACT 10th Intenational Conference*, Vol. 3, pp. 1903-1907, 2008.

[9] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, "Low-cost Electroencephalogram (EEG) based Authentication," *Proceeding of Neural Engineering, 5th International IEEE/EMBS Conference*, pp. 442-445, 2011.

[10] A. Zúquete, B. Quintela, and J.P. da Silva Cunha, "Biometric Authentication using Brain Responses to Visual Stimuli," *Biosignals*, pp. 103-112, 2010.

[11] C. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Journal,* Vol. 28. No. 4, pp. 659-715, 1949.

[12] W. Stallings, *Network Security Essentials : Applications and Standards*, Pearson Education, UK, 2013.

[13] S.I Shin, J.H Cho and M.N Kim, "Proposition for 4 Channel Frontal Lobe Electrode Configuration and Study on EOG Removal from Measured EEG," *Journal of Korea Multimedia Society*, Vol. 6, No. 1, pp. 167-175, 2003.

김 정 숙

1993년 동국대학교 컴퓨터공학과 공학사
1995년 동국대학교 대학원 컴퓨터공학과 공학석사
1999년 동국대학교 대학원 컴퓨터공학과 공학박사

2000년～현재 김포대학교 스마트IT학부 교수
2005년～현재 한국멀티미디어학회 이사
관심분야 : IT 융합, 인공 지능, 유전 및 분산 알고리즘

정 장 영

2006년 대전대학교 전산정보보호학과 이학사
2009년 동국대학교 대학원 컴퓨터공학과 공학석사
2015년 동국대학교 대학원 컴퓨터공학과 공학박사

관심분야 : 융합보안, 이미지 보안, 병렬 암호알고리즘, 생체보안