(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0071023
(43) 공개일자 2025년05월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06N 3/0455* (2023.01)
H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
G06N 3/0455 (2023.01)
(21) 출원번호 10-2023-0157551
(22) 출원일자 2023년11월14일
심사청구일자 2023년11월14일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웰 카운티2단지)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 13 항

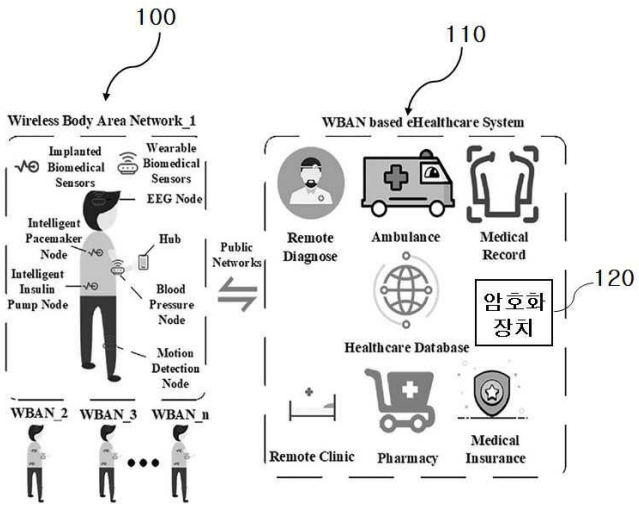
(54) 발명의 명칭 **E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치 및 방법**

(57) 요 약

E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치 및 방법은 의료 및 건강 관리 환경을 위한 고유한 무선 통신 프로토콜을 제공하기 위한 것으로, 생체 신호의 자연적 난수성(randomness)을 포함하는 이중 혼돈 암호화(double chaotic encryption) 방법을 제공할 수 있다.

본 발명은 시스템의 보안을 보장할 수 있고, 노이즈 등 다중 공격에 저항할 수 있으며, 일반 텍스트 이미지의 경우 암호화 시간이 0.1초를 넘지 않아 시스템의 실시간 요구 사항을 보장할 수 있는 효과가 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/001 (2013.01)
H04L 9/0866 (2013.01)
H04L 2209/88 (2013.01)

명 세 서

청구범위

청구항 1

이중 카오스 암호화 장치에 있어서,

초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출하는 EEG(Electroencephalogram) 고유값 추출부;

상기 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 하이브리드 의사 난수 생성기를 생성하는 제어부; 및

상기 의사 난수 생성기에서 생성된 난수열과 WBAN(wireless body area network)에 대한 EEG(Electroencephalogram) 고유값을 기반으로 이중 카오스 암호 기법을 적용하는 이중 카오스 암호화 처리부를 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치.

청구항 2

청구항 1에 있어서,

상기 EEG 고유값 추출부는,

시간 도메인 특징 및 주파수 도메인 특징을 갖는 EEG 신호를 추출하고, 상기 시간 도메인 특징과 상기 주파수 도메인 특징을 연결하여 다중 도메인 특징을 형성한 후, 오토인코더를 사용하여 시간 도메인 영역과 주파수 도메인 영역 간의 관계를 마이닝하여 상기 뇌파 신호를 표현하기 위한 깊은 다중 도메인 특징을 얻는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치.

청구항 3

청구항 1에 있어서,

상기 EEG 고유값 추출부는,

대뇌 피질에서 EEG(Electroencephalogram)를 캡처하고, 상기 캡처된 EEG에서 6개의 EEG 데이터—상기 EEG 데이터는 하기의 수학식 1로 정의됨—의 채널이 선택되고, 상기 각 EEG 데이터에서 시간 도메인 특징을 시간 도메인에서의 EEG 표현—상기 시간 도메인에서의 EEG 표현은 하기의 수학식 2로 정의됨—으로 추출하며, 상기 각 EEG 데이터에서 주파수 도메인 특징을 주파수 도메인에서의 EEG 표현—상기 주파수 도메인에서의 EEG 표현은 하기의 수학식 3으로 정의됨—으로 추출하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치.

[수학식 1]

$$x \in \mathbb{R}^{s \times c \times f}$$

여기서, 상기 s는 샘플수, 상기 c는 선택된 채널, 상기 f는 샘플링 지점, 상기 c는 6임.

[수학식 2]

$$x_t \in \mathbb{R}^{s \times c \times t}$$

여기서, t는 시간 도메인 특징 벡터의 길이임.

[수학식 3]

$$x_f \in \mathbb{R}^{s \times c \times p}$$

여기서, p는 5개 주파수 대역의 값임.

청구항 4

청구항 3에 있어서,

상기 시간 도메인 특징과 상기 주파수 도메인 특징의 상관 관계를 마이닝하기 위한 오토인코더 모델을 생성하고, 상기 생성한 오토인코더 모델을 이용하여 상기 시간 도메인 특징 $x_t \in \mathbb{R}^{s \times c \times t}$ 과 상기 주파수 도메인 특징 $x_f \in \mathbb{R}^{s \times c \times p}$ 을 얻으며, 상기 x_t 와 상기 x_f 는 각각 오토인코더에 입력하고, 상기 오토인코더에서 뉴런 수가 최소인 완전 연결(Fully Connected, FC) 계층을 사용하여 각각 h_t 및 h_f 를 나타내는 깊은 시간 도메인 특징(deep time domain feature)과 깊은 주파수 도메인 특징(deep frequency domain feature)을 출력하는 오토인코더 생성부를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치.

[수학식 4]

$$h_t = E(x_t)$$

[수학식 5]

$$h_f = E(x_f)$$

[수학식 6]

$$x_t \approx D(E(x_t))$$

[수학식 7]

$$x_f \approx D(E(x_f))$$

여기서, $E(\cdot)$ and $D(\cdot)$ 는 인코더(Encode)와 디코더(Decode)의 오퍼레이션(Operation)임.

청구항 5

청구항 4에 있어서,

상기 오토인코더 생성부는,

하기의 수학식 8를 이용하여 상기 깊은 시간 도메인 특징(deep time domain feature) h_t 과 상기 깊은 주파수 도메인 특징(deep frequency domain feature) h_f 를 병합하여 다중 도메인 특징(multi domain features) x_m 을 얻는 단계; 및

하기의 수학식 9에 의해 다중 도메인 특징 x_m 을 인코더에 입력하여 깊은 다중 도메인 특징(deep multi domain features) h_m 을 출력하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카

오스 암호화 장치.

[수학식 8]

$$x_m = concat(h_t, h_f)$$

여기서, x_m 은 h_t 와 h_f 를 병합하여 얻어진 다중 도메인 특징임.

[수학식 9]

$$h_m = E(x_m)$$

청구항 6

청구항 1에 있어서,

상기 이중 카오스 암호화 처리부는,

상기 의사 난수 생성기의 출력으로 (0, 1) 범위의 무작위성을 갖는 카오스 시퀀스(Chaotic Sequence) Xn을 얻고, 상기 카오스 시퀀스(Chaotic Sequence) Xn을 하기의 수학식 10에 대입하여 암호화에 사용되는 이진 시퀀스(Binary Sequence) Sn을 얻고, I(M, N)으로 표현되는 평문의 유효 정보를 길이가 n = M × N × 8인 이진 시퀀스(Binary Sequence) In으로 변환하며, 암호문 시퀀스 스트림 Zn은 하기의 수학식 11를 이용하여 랜덤 시퀀스 스트림 상기 Sn과 평문 시퀀스 스트림 상기 Xn을 XOR 연산을 통해 얻는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치.

[수학식 10]

$$S_n = \begin{cases} 1, & x_n > 0.5 \\ 0, & x_n < 0.5 \end{cases}$$

[수학식 112]

$$encryption_p rocessZ_n = S_n \oplus I_n$$

청구항 7

초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출하는 단계;

상기 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 하이브리드 의사 난수 생성기를 생성하는 단계; 및

상기 의사 난수 생성기에서 생성된 난수열과 WBAN(wireless body area network)에 대한 EEG(Electroencephalogram) 고유값을 기반으로 이중 카오스 암호 기법을 적용하는 단계를 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

청구항 8

청구항 7에 있어서,

상기 초기 인자로 추출하는 단계는,

시간 도메인 특징 및 주파수 도메인 특징을 갖는 EEG 신호를 추출하는 단계; 및

상기 시간 도메인 특징과 상기 주파수 도메인 특징을 연결하여 다중 도메인 특징을 형성한 후, 오토 인코더를 사용하여 시간 도메인 영역과 주파수 도메인 영역 간의 관계를 마이닝하여 상기 뇌파 신호를 표현하기 위한 깊은 다중 도메인 특징을 얻는 단계를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를

위한 이중 카오스 암호화 방법.

청구항 9

청구항 7에 있어서,

상기 초기 인자로 추출하는 단계는,

대뇌 피질에서 EEG(Electroencephalogram)를 캡쳐하는 단계;

상기 캡쳐된 EEG에서 6개의 EEG 데이터－상기 EEG 데이터는 하기의 수학식 1로 정의됨－의 채널이 선택되는 단계;

상기 각 EEG 데이터에서 시간 도메인 특징을 시간 도메인에서의 EEG 표현－상기 시간 도메인에서의 EEG 표현은 하기의 수학식 2로 정의됨－으로 추출하는 단계;

상기 각 EEG 데이터에서 주파수 도메인 특징을 주파수 도메인에서의 EEG 표현－상기 주파수 도메인에서의 EEG 표현은 하기의 수학식 3으로 정의됨－으로 추출하는 단계를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

[수학식 1]

$$x \in \mathbb{R}^{s \times c \times f}$$

여기서, 상기 s는 샘플수, 상기 c는 선택된 채널, 상기 f는 샘플링 지점, 상기 c는 6임.

[수학식 2]

$$x_t \in \mathbb{R}^{s \times c \times t}$$

여기서, t는 시간 도메인 특징 벡터의 길이임.

[수학식 3]

$$x_f \in \mathbb{R}^{s \times c \times p}$$

여기서, p는 5개 주파수 대역의 값임.

청구항 10

청구항 9에 있어서,

상기 시간 도메인 특징과 상기 주파수 도메인 특징의 상관 관계를 마이닝하기 위한 오토인코더 모델을 생성하는 단계;

상기 생성한 오토인코더 모델을 이용하여 상기 시간 도메인 특징 $x_t \in \mathbb{R}^{s \times c \times t}$ 과 상기 주파수 도메인 특징 $x_f \in \mathbb{R}^{s \times c \times p}$ 을 얻는 단계; 및

상기 x_t 와 상기 x_f 는 각각 오토인코더에 입력하고, 상기 오토인코더에서 뉴런 수가 최소인 완전 연결(Fully Connected, FC) 계층을 사용하여 각각 h_t 및 h_f 를 나타내는 깊은 시간 도메인 특징(deep time domain feature)과 깊은 주파수 도메인 특징(deep frequency domain feature)을 출력하는 단계를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

[수학식 4]

$$h_t = E(x_t)$$

[수학식 5]

$$h_f = E(x_f)$$

[수학식 6]

$$x_t \approx D(E(x_t))$$

[수학식 7]

$$x_f \approx D(E(x_f))$$

여기서, $E(\cdot)$ and $D(\cdot)$ 는 인코더(Encode)와 디코더(Decode)의 오퍼레이션(Operation)임.

청구항 11

청구항 10에 있어서,

하기의 수학식 8를 이용하여 상기 깊은 시간 도메인 특징(deep time domain feature) h_t 과 상기 깊은 주파수 도메인 특징(deep frequency domain feature) h_f 를 병합하여 다중 도메인 특징(multi domain features) x_m 을 얻는 단계; 및

다중 도메인 특징 x_m 을 인코더에 입력하여 하기의 수학식 9와 같이, 깊은 다중 도메인 특징(deep multi domain features) h_m 을 출력하는 단계를 더 포함하 는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

[수학식 8]

$$x_m = concat(h_t, h_f)$$

여기서, x_m 은 h_t 와 h_f 를 병합하여 얻어진 다중 도메인 특징임.

[수학식 9]

$$h_m = E(x_m)$$

청구항 12

청구항 10에 있어서,

상기 의사 난수 생성기를 생성하는 단계는,

상기 오토인코더 모델을 시간 도메인 오토인코더, 주파수 도메인 오토인코더, 다중 도메인 오토인코더를 생성하는 단계;

상기 시간 도메인 오토인코더, 상기 주파수 도메인 오토인코더, 상기 다중 도메인 오토인코더를 통해 상기 EEG 신호의 다중 도메인 특징을 얻을 수 있는 단계를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

청구항 13

청구항 7에 있어서,

상기 이중 카오스 암호 기법을 적용하는 단계는,

상기 의사 난수 생성기의 출력으로 (0, 1) 범위의 무작위성을 갖는 카오스 시퀀스(Chaotic Sequence) Xn을 얻는 단계;

상기 카오스 시퀀스(Chaotic Sequence) Xn을 하기의 수학식 10에 대입하여 암호화에 사용되는 이진 시퀀스(Binary Sequence) Sn을 얻는 단계;

I(M, N)으로 표현되는 평문의 유효 정보를 길이가 n = M × N × 8인 이진 시퀀스(Binary Sequence) In으로 변환하는 단계; 및

암호문 시퀀스 스트림 Zn은 하기의 수학식 11를 이용하여 랜덤 시퀀스 스트림 상기 Sn과 평문 시퀀스 스트림 상기 Xn을 XOR 연산을 통해 얻는 단계를 더 포함하는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법.

[수학식 10]

$$S_n = \begin{cases} 1, & x_n > 0.5 \\ 0, & x_n < 0.5 \end{cases}$$

[수학식 112]

$$encryption_processZ_n = S_n \oplus I_n$$

발명의 설명

기 술 분 야

[0001] 본 발명은 이중 카오스 암호화 장치에 관한 것으로서, 더욱 상세하게는 의료 및 건강 관리 환경을 위한 고유한 무선 통신 프로토콜을 제공하기 위한 것으로, 생체 신호의 자연적 난수성(randomness)을 포함하는 이중 혼돈 암호화(double chaotic encryption) 방법을 제공할 수 있는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 즉각적인 E-헬스케어 서비스에 대한 근본적인 기술 지원으로서 무선 신체 영역 네트워크(Wireless Body Area Network, WBAN)는 최근 몇 년간 과학 및 산업계에서 큰 주목을 받아 왔다. 이는 의료 및 의료 상황을 위한 고유한 무선 통신 프로토콜을 정의한다.

[0003] 그러나 WBAN의 네트워크 및 데이터 보안에 대한 우려는 WBAN의 급속한 발전에 걸림돌이 되었다.

[0004] WBAN의 무단 액세스 및 불법 데이터 변조는 사용자에게 중요한 문제를 일으킬 수 있으므로 표준에서 보안 방법으로 타원 곡선 공개키 암호화(Elliptic Curve Public Key Cryptography, ECC) 및 고급 암호화 표준(Advanced Encryption Standard, AES)도 권장한다. 그러나 최근 몇 년 동안 웨어러블 및 이식형 의료 및 장기 건강 모니터링 장치의 급속한 성장 이후 이러한 전통적인 방법이 WBAN에 적합한 보안 방법인지에 대해 의문을 제기하는 연구자와 엔지니어가 점점 늘어나고 있다. 주된 이유는 제한된 하드웨어 자원과 전원 공급 장치로 인해 ECC 및 AES의 복잡한 계산을 거의 지원할 수 없기 때문이다. 따라서, 낮은 하드웨어 복잡성과 높은 데이터 암호화 강도의 요구 사항을 충족할 수 있는 경량 데이터 암호화 방법을 설계하고 구현하는 방법이 WBAN 연구 커뮤니티에서 뜨거운 주제가 되었다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국 등록번호 제10-1083429호

발명의 내용

해결하려는 과제

[0006] 이와 같은 문제점을 해결하기 위하여, 본 발명은 의료 및 건강 관리 환경을 위한 고유한 무선 통신 프로토콜을 제공하기 위한 것으로, 생체 신호의 자연적 난수성(randomness)을 포함하는 이중 혼돈 암호화(double chaotic encryption) 방법을 제공할 수 있는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치 및 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명의 특징에 따른 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치는,

[0008] 초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출하는 EEG(Electroencephalogram) 고유값 추출부;

[0009] 상기 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 하이브리드 의사 난수 생성기를 생성하는 제어부; 및

[0010] 상기 의사 난수 생성기에서 생성된 난수열과 WBAN(wireless body area network)에 대한 EEG(Electroencephalogram) 고유값을 기반으로 이중 카오스 암호 기법을 적용하는 이중 카오스 암호화 처리부를 포함한다.

[0011] 본 발명의 특징에 따른 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 방법은,

[0012] 초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출하는 단계;

[0013] 상기 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 하이브리드 의사 난수 생성기를 생성하는 단계; 및

[0014] 상기 의사 난수 생성기에서 생성된 난수열과 WBAN(wireless body area network)에 대한 EEG(Electroencephalogram) 고유값을 기반으로 이중 카오스 암호 기법을 적용하는 단계를 포함한다.

발명의 효과

[0015] 전술한 구성에 의하여, 본 발명은 시스템의 보안을 보장할 수 있고, 노이즈 등 다중 공격에 저항할 수 있으며, 일반 텍스트 이미지의 경우 암호화 시간이 0.1초를 넘지 않아 시스템의 실시간 요구 사항을 보장할 수 있는 효과가 있다.

[0016] 본 발명은 현실 세계의 무작위성을 포함하는 WBAN에서 추출된 뇌파 고유값을 카오스 장치에서 초기값의 보안 문제를 해결하여 여러 공격에 저항할 수 있는 보안 시스템을 구축할 수 있는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시예에 따른 WBAN 및 E-헬스케어 서비스 시스템의 전체 구성을 나타낸 도면이다.

도 2는 본 발명의 실시예에 따른 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치의 구성을 나타낸 도면이다.

도 3은 본 발명의 실시예에 따른 PLCM 분기 다이아그램을 나타낸 도면이다.

도 4는 본 발명의 실시예에 따른 LTM 분기 다이아그램을 나타낸 도면이다.

도 5는 본 발명의 실시예에 따른 6개의 EEG 데이터의 채널을 나타낸 도면이다.

도 6은 본 발명의 실시예에 따른 시간 도메인 특징과 주파수 도메인 특징의 상관 관계를 나타낸 도면이다.

도 7은 본 발명의 실시예에 따른 카오스 매핑을 기반으로 한 의사 난수 생성기를 생성하는 과정을 나타낸 도면이다.

도 8은 본 발명의 실시예에 따른 이중 카오스 암호화 프로세스를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0019] 본 발명에서는 생체 신호인 뇌전도(Electroencephalogram, EEG)를 추가하여 자연적 무작위성을 포함하는 이중 카오스 암호화 방법을 제공한다. 처음에는 초기값의 자연스러운 무작위성을 보장하기 위해 깊은 다중 영역 특징을 포함하는 3차원 고유값을 카오스 기반 의사 난수 생성기의 초기 요소로 추출한다. 그런 다음 두 개의 카오스 맵인 PLCM(Piecewise Linear Map)과 LTM(Coupled Logistic-Tent Map)을 기반으로 하는 하이브리드 의사 난수 생성기를 생성하며, 이는 높은 무작위성과 낮은 하드웨어 복잡도의 장점을 가지고 있다. 마지막으로 WBAN에 대한 EEG 고유값을 기반으로 한 이중 카오스 암호화 방법을 제공한다.

[0020] 도 1은 본 발명의 실시예에 따른 WBAN 및 E-헬스케어 서비스 시스템의 전체 구성을 나타낸 도면이고, 도 2는 본 발명의 실시예에 따른 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치의 구성을 나타낸 도면이다.

[0021] 본 발명은 WBAN(Wireless Body Area Network)(100) 및 WBAN를 기반으로 한 E-헬스케어 서비스 시스템(110)을 포함한다.

[0022] WBAN(Wireless Body Area Network)(100)은 인체 내부에서 작동하는 이식형 장치나 인체 외부에서 작동하는 웨어러블(wearable) 센서가 생체 신호를 수집하고 이를 바탕으로 몸 상태를 분석해 원격 의료 진단 및 치료 등을 수행할 수 있는 네트워크이다.

[0023] E-헬스케어 서비스 시스템(110)은 다수의 WBAN(100)으로부터 수신된 신체 센싱 정보를 이용하여 E-헬스케어 서비스를 제공하는 모든 기관, 장치, 서버를 포괄하는 개념일 수 있다.

[0024] E-헬스케어 서비스 시스템(110)은 원격 클리닉 병원, 약국, 앰블런스, 원격 진료 서비스, 이중 카오스 암호화 장치 등을 모두 통칭하는 시스템이다. 본 발명에서는 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치(120)를 중점으로 설명하기로 한다.

[0025] 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 E-헬스케어 서비스를 위한 생체 신호 기반의 의학정보 보호를 위한 이중 카오스 암호화 장치(120)는 신호 수신부(121), 제어부(122), 저장부(123), EEG 고유값 계산부(124), 오토인코더 생성부(125), 의사 난수 생성기(126), 이중 카오스 암호화 처리부(127)를 포함할 수 있다.

[0026] 신호 수신부(121)는 다수의 WBAN(100)으로부터 각각의 개인의 EEG(Electroencephalogram) 신호를 수신할 수 있다. EEG 신호는 WBAN에서 전송되는 가장 일반적인 생리학적 뇌파 신호 중 하나이다.

[0027] 뇌파는 고전적인 생체 신호로서 인간의 대뇌피질의 신경활동을 전기의 형태로 객관적으로 반영하며, 그 성격은 비정상적이고 더 큰 개인차와 카오스로 현실 세계에 대한 거대한 불확실성을 내포하고 있다.

[0028] 의료 및 건강 관리 목적의 가장 일반적인 활력 징후 중 하나인 EEG는 지난 수십 년 동안 널리 연구되어 왔다. 특히 최근에는 뇌 컴퓨터 인터페이스의 발달로 감정 인식, 간질 감지, 운전 보조 등 뇌파 기반 연구가 실생활 상황에 성공적으로 적용되고 있다.

[0029] EEG 신호는 WBAN에서 전송되는 가장 일반적인 생체 신호 중 하나이다.

[0030] 제어부(122)는 신호 수신부(121)로부터 수신된 EEG 신호를 저장부(123)에 저장할 수 있다.

[0031] EEG 고유값 계산부(124)는 이중 카오스 암호화 장치(120)의 초기 요인의 무작위성을 보장하기 위해 WBAN에서 시간 영역 및 주파수 영역 특징을 갖는 EEG 고유값을 계산한다.

[0032] 보다 구체적으로, EEG 고유값 계산부(124)는 원시 다중 채널 EEG 신호의 시간 도메인 특징 및 주파수 도메인 특징이 첫 번째 단계에서 추출된다.

[0033] 본 발명의 이중 카오스 암호화 장치(120)는 낮은 전력 소모와 구현의 복잡도 특성으로 인해 카오스 맵을 기반으로 한 경량 인증 및 암호화 방식은 사물인터넷(IoT), 웨어러블 디바이스 등 저전력 시스템에서 널리 활용되고 있다.

[0034] 본 발명에서는 WBAN에 대한 EEG 고유값을 기반으로 한 이중 카오스(Chaotic) 스트림 암호화 방법을 제공한다.

[0035] 현실 세계의 자연적 무작위성을 포함하는 WBAN에서 추출된 EEG 고유값을 이중 카오스 암호화 장치(120)에서 초기값의 보안 문제를 해결하기 위한 초기 요소로 계산할 수 있다.

[0036] PLCM 및 LTM의 캐스케이드는 생성된 시퀀스의 무작위성을 효과적으로 개선하고 시퀀스는 NIST 테스트를 통과할 수 있다.

[0037] EEG 고유값 계산부(124)는 이중 카오스 암호화 장치(120)의 초기값의 무작위성을 보장하기 위해 WBAN에서 시간 영역 및 주파수 영역 특징을 갖는 EEG 고유값을 계산한다.

[0038] 보다 구체적으로, EEG 고유값 계산부(124)는 원시 다중 채널 EEG 신호의 시간 영역 및 주파수 영역 특징이 추출된다. 신호 처리 방법은 원시 다중 채널 EEG에서 보다 보편적인 표현을 추출하는데 도움이 되고, 계산 비용도 줄일 수 있다.

[0039] 다음으로, 비지도 학습 방법과 오토인코더를 적용하여 각각 시간 영역과 주파수 영역의 심층 특징을 추출한다.

[0040] 이는 EEG 획득 과정에서 피할 수 없는 잡음 영향을 해결하는데 도움이 되는 잡음 입력을 수용할 수 있으며 자동 특징 선택을 실현할 수 있다.

[0041] 마지막으로 깊은 시간 도메인 특징과 깊은 주파수 도메인 특징을 연결하여 다중 도메인 특징을 형성한 후 오토인코더를 사용하여 시간 도메인과 주파수 도메인 간의 관계를 마이닝하여 깊은 다중 도메인 특징을 얻는다. 깊은 다중 도메인 특징은 EEG 신호를 표현하기 위해 사용된다.

[0042] 제어부(122)는 신호 수신부(121)를 통해 다수의 WBAN(100)으로부터 서로 다른 시간에 수집된 EEG 데이터를 수집하여 저장부(123)에 저장한다.

[0043] 제어부(122)는 원시 EEG 데이터의 경우 200Hz의 샘플링 주파수를 서브샘플링에 사용하고, 1 내지 75Hz의 필터를 사용하여 관련 없는 다른 주파수 대역을 필터링하여 EEG 데이터를 획득할 수 있다.

[0044] EEG 고유값 계산부(124)는 저장부(123)에 저장된 EEG 데이터에서 시간 영역 특징과 주파수 영역 특징을 추출한다.

[0045] EEG 고유값 계산부(124)는 초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출할 수 있다.

[0046] 본 발명은 기밀성 유지를 위해 암호화에 사용되는 키 값과 데이터 암호화의 과정에 복수의 카오스 사상을 기반으로 암호화한다.

[0047] EEG 고유값 계산부(124)는 하기의 수학식 1에 의해 조각별 선형 카오스 맵을 나타내고, 하기의 수학식 2에 의해 결합형 로지스틱 텐트 맵을 나타낼 수 있다.

[0048] 도 3은 본 발명의 실시예에 따른 PLCM 분기 다이아그램을 나타낸 도면이고, 도 4는 본 발명의 실시예에 따른 LTM 분기 다이아그램을 나타낸 도면이다.

[0049] 조각별 선형 카오스 맵(Piecewise Linear Chaotic Map, PLCM)

[0050] PLCM은 일반적인 1차원 카오스 매핑이고, 이중 카오스 암호화 시스템에 사용하며, 이를 다음의 수학식 1과 같이 표현할 수 있다.

수학식 1

$$y_{n+1} = \begin{cases} y_n/p, & 0 < y_n < p \\ (y_n - p)/(0.5 - p), & p \le y_n < 0.5 \\ (1 - y_n - p)/(0.5 - p), & 0.5 \le y_n < 1 - p \\ (1 - y_n)/p, & 1 - p \le y_n < 1 \end{cases}$$

[0051]

[0052] 도 3에 도시된 바와 같이, 초기값 y(0)과, 구조 매개변수 P를 갖는 조각별 선형 카오스의 분기 구조를 보여준다.

[0053] 초기값 y(0)의 값 간격은 (0, 1)이고, p 는 (0, 1/2)이다. 이때 이중 카오스 암호화 시스템은 카오스 상태에 들어가고, 반복에 의해 생성된 시퀀스는 의사 난수(pseudo-random) 특성을 갖게 된다. 이 시점에서 이중 카오스 암호화 시스템은 다음과 같은 특징을 갖는다.

[0054] (1) 출력 시퀀스는 간격 (0,1) 내에서 이동한다.

[0055] (2) 출력 궤도에는 델타형 자기 상관 함수가 있다.

[0056] (3) 균일하고, 불변의 확률밀도함수를 갖는다.

[0057] 결합형 로지스틱 텐트 맵(Coupled Logistic-Tent map, LTM)

[0058] LTM은 Logistic 매핑과 Tent 매핑을 결합한 새로운 종류의 1차원 카오스 매핑으로, 하기의 수학식 2와 같다.

[0059] LTM을 이중 카오스 암호화 장치의 의사 난수 생성기로 활용하여 난수열을 생성할 수 있다.

[0060] LTM의 분기 다이어그램은 도 4에 표시되어 있다. 가로축은 구조적 매개변수를 나타내고, 세로축은 구조적 매개변수가 이 값을 취할 때 얻은 시퀀스의 0-1 분포를 나타낸다. 도 4에서 볼 수 있듯이, 시퀀스는 구조적 매개 변수의 선택적 범위 내에서 간격에 고르게 분포되어 있으며, 이는 시퀀스가 통계적 특성을 잘 가지고 있음을 나타낸다.

수학식 2

$$x_{n+1} = \begin{cases} mod(\mu x_n(1 - x_n) \\ \quad +(4 - \mu)x_n/2, 1), when \quad x_n < 0.5; \\ mod(\mu x_n(1 - x_n) \\ \quad +(4 - \mu)(1 - x_n)/2, 1), when \quad x_n \ge 0.5. \end{cases}$$

[0061]

[0062] EEG 고유값 계산부(124)는 시간 도메인 특징 및 주파수 도메인 특징을 갖는 EEG 신호를 추출한다.

[0063] 원시 다중 채널 EEG 신호의 채널은 먼저 다중 채널 EEG 특징 계산 비용을 줄이고 딥러닝 기반 모델의 매개변수의 수를 줄여 모델의 수렴 속도를 가속화하고 최종적으로 성능을 향상시키기 위해 선택된다. 모델의 성능. 그 후, EEG 신호로부터 시간 영역 및 주파수 영역 특징이 얻어지며, 이는 다양한 영역에서 EEG를 간결하고 강력하게 나타낼 수 있다.

[0064] 도 5는 본 발명의 실시예에 따른 6개의 EEG 데이터의 채널을 나타낸 도면이다.

[0065] EEG 고유값 계산부(124)는 도 5와 같이, 대뇌 피질에서 EEG(Electroencephalogram)를 캡처하고, 캡처된 EEG에서 6개의 EEG 데이터의 채널이 선택된다.

[0066] 6개의 EEG 데이터의 채널을 사용하면 주어진 작업에 모든 뇌 전극을 사용하는 것과 유사한 효과를 얻을 수 있다.

[0067] 따라서, 실제 적용을 위한 웨어러블, 타당성 및 실시간 성능에 대한 요구 사항을 고려하여 도 5에 원으로 표시된 FT7, T7, TP7, FT8, T8 및 TP8이라는 6개의 EEG 데이터의 채널이 선택된다.

[0068] EEG 데이터는 $x \in \mathbb{R}^{s \times c \times f}$ 로 정의된다. 여기서, s는 샘플수, c는 선택된 채널, f는 샘플링 지점을 나타낸다. c는 6과 동일하다.

[0069] EEG 고유값 계산부(124)는 각 EEG 데이터에서 시간 도메인 특징을 시간 도메인에서의 EEG 표현로 추출한다.

[0070] EEG 고유값 계산부(124)는 각 EEG 데이터의 샘플에서 시간 도메인 특징을 시간 도메인에서의 EEG(뇌파) 표현으로 추출한다.

[0071] $x \in \mathbb{R}^{s \times c \times f}$ 의 경우, $x_t \in \mathbb{R}^{s \times c \times t}$ 로 표현된 시간 도메인 특징을 갖는 EEG는 특징 추출 후에 얻어질 수 있다. 여기서, t는 시간 도메인 특징 벡터의 길이를 나타낸다.

[0072] 딥모델의 계산 속도를 향상시키고, 특징 크기 간의 차이가 딥모델에 미치는 영향을 줄이기 위해서 각 EEG 데이터의 모든 특징에 대해 정규화가 수행되며, 이는 다음의 수학식 3과 같다.

수학식 3

[0073]
$$\overline{X_i} = \frac{X_i - X_{min}}{X_{max} - X_{min}}$$

[0074] 여기서, $\overline{X_i}$ 와 X_i 는 각각 정규화 전 i번째 샘플의 특징을 나타내고, X_{min} 와 X_{max}는 각각 특징의 최소값과 최대값을 나타낸다.

[0075] EEG 고유값 계산부(124)는 각 EEG 데이터에서 주파수 도메인 특징을 주파수 도메인에서의 EEG 표현으로 추출한다.

[0076] EEG 데이터의 주파수 도메인 특징들은 PSD(Power Spectra Density)가 널리 사용되며, EEG 감정 인식, 알츠하이머 뇌파 분석, 수면 감지 등에 성공적으로 적용된다.

[0077] 본 발명에서는 중첩되지 않는 1초 원도우창을 갖는 단시간 고속 푸리에 변환을 적용하여 5개 대역의 PSD를 계산한다.

[0078] 일부 중요한 주파수 대역은 뇌 기능과 관련이 있다. 예를 들어 1 내지 3Hz 대역은 무의식과 관련이 있고, 4 내지 7Hz 대역은 뇌 기능에 중요한 역할을 한다.

[0079] 무의식에서의 역할, 8 내지 13Hz는 일반적으로 편안한 정신 상태와 관련이 있고 두정엽과 후두엽에서 더 활동적이며, 14 내지 30Hz는 활동적인 정신 상태와 관련이 있고 전두엽 피질에서 더 긍정적이며, 30 내지 50Hz는 주의력, 의식, 학습 과정과 관련이 있다.

[0080] 따라서, EEG 고유값 계산부(124)는 위의 5개 주파수 대역의 PSD를 계산할 수 있으며, 그 결과 주파수 영역의 EEG(뇌파) 표현은 $x_f \in \mathbb{R}^{s \times c \times p}$ 가 얻어진다. 여기서, p는 5개 대역의 값을 나타낸다. 주파수 영역의 EEG(뇌파) 표현은 시간 도메인의 특징과 동일하다. 상기 수학식 3은 주파수 도메인의 특징을 정규화하는데 사용될 수 있다.

[0081] 오토인코더 생성부(125)는 EEG를 보다 완벽하고 간결하게 표현하기 위해서는 시간 도메인(Domain)과 주파수 도메인 간의 상관 관계를 마이닝하기 위한 심층 오토인코더 모델을 생성한다. 이러한 접근법의 전체 프레임워크는 도 6에 나와 있다. 도 6은 본 발명의 실시예에 따른 시간 도메인 특징과 주파수 도메인 특징의 상관 관계를 나타낸 도면이다.

[0082] 오토인코더 생성부(125)는 오토인코더 모델(도 6과 같은 연산)을 이용하여 시간 도메인 특징 $x_t \in \mathbb{R}^{s \times c \times t}$ 과 주파수 도메인 특징 $x_f \in \mathbb{R}^{s \times c \times p}$ 을 얻을 수 있다.

[0083] 오토인코더 생성부(125)는 x_t 와 x_f 를 각 오토인코더에 입력하고, 오토인코더에서 뉴런 수가 최소인 완전 연결(Fully Connected, FC) 계층을 사용하여 각각 h_t 및 h_f 를 나타내는 깊은 시간 도메인 특징(deep time domain feature)과 깊은 주파수 도메인 특징(deep frequency domain feature)을 출력한다.

[0084] 오토인코더 생성부(125)는 오토인코더에서 뉴런 수가 최소인 완전 연결(Fully Connected, FC) 계층을 사용하여 각각 h_t 및 h_f 를 나타내는 깊은 시간 도메인 특징과 깊은 주파수 도메인 특징을 출력한다.

[0085] 오토인코더 생성부(125)는 시간 도메인과 주파수 도메인에서 EEG의 원래 정보를 유지할 수 있도록 h_t 및 h_f 를 생성한다.

[0086] h_t 및 h_f 는 다음의 수학식 4와 수학식 5의 인코더에 x_t 와 x_f 를 대입하여 생성한다.

수학식 4

[0087] $$h_t = E(x_t)$$

수학식 5

[0088] $$h_f = E(x_f)$$

[0089] 오토인코더 생성부(125)는 디코더에 h_t 및 h_f 를 대입하면, 다음의 수학식 6과 수학식 7과 같이, x_t 와 x_f 를 출력할 수 있다.

수학식 6

[0090] $$x_t \approx D(E(x_t))$$

수학식 7

[0091] $$x_f \approx D(E(x_f))$$

[0092] 여기서, $E(\cdot)$ and $D(\cdot)$ 는 인코더(Encode)와 디코더(Decode)의 오퍼레이션(Operation)을 나타낸다.

[0093] 오토인코더 생성부(125)는 하기의 수학식 8를 이용하여 깊은 시간 도메인 특징(deep time domain feature) h_t 과 깊은 주파수 도메인 특징(deep frequency domain feature) h_f 를 병합하여 다중 도메인 특징(multi domain features) x_m 을 얻는다.

수학식 8

[0094] $$x_m = concat(h_t, h_f)$$

[0095] 여기서, x_m 은 h_t 와 h_f 를 병합하여 얻어진 다중 도메인 특징을 나타낸다.

[0096] 오토인코더 생성부(125)는 하기의 수학식 9에 의해 다중 도메인 특징 x_m 을 인코더에 입력하여 깊은 다중 도메인 특징(deep multi domain features) h_m 을 출력하는

수학식 9

[0097] $$h_m = E(x_m)$$

[0098] 다중 도메인 특징 간의 상관 관계 및 상보성을 마이닝하기 위해 오토인코더를 활용하여 EEG 표현을 나타내는데 사용되는 깊은 다중 도메인 특징 h_m 을 얻는다.

수학식 10

[0099] $$x_m \approx D(E(x_m))$$

[0100] 오토인코더 생성부(125)는 입력 차원이 다르고, 학습 목적이 다르기 때문에 시간 도메인 오토인코더, 주파수 도메인 오토인코더 및 다중 도메인 오토인코더를 각각 구성할 수 있다.

[0101] 3가지 타입의 오토인코더의 세부 사항은 아래의 표 1과 같다.

표 1

The details of three autoencoder.

Time-domain autoencoder				
Layer		Output shape	Connected to	Model output
Encoder	Dense1	(None,32)	Input	Dense4
	Dense2	(None,16)	Dense1	
	Dense3	(None,16)	Dense2	
	Dense4	(None,8)	Dense3	
Decoder	Dense5	(None,16)	Dense4	
	Dense6	(None,16)	Dense5	
	Dense7	(None,32)	Dense6	
	Dense8	(None,54)	Dense7	
Frequency-domain autoencoder				
Layer		Output shape	Connected to	Model output
Encoder	Dense1	(None,32)	Input	Dense4
	Dense2	(None,16)	Dense1	
	Dense3	(None,16)	Dense2	
	Dense4	(None,8)	Dense3	
Decoder	Dense5	(None,16)	Dense4	
	Dense6	(None,16)	Dense5	
	Dense7	(None,32)	Dense6	
	Dense8	(None,30)	Dense7	
Multi-domain autoencoder				
Layer		Output shape	Connected to	Model output
Encoder	Dense1	(None,16)	Input	Dense4
	Dense2	(None,8)	Dense1	
	Dense3	(None,8)	Dense2	
	Dense4	(None,3)	Dense3	
Decoder	Dense5	(None,8)	Dense4	
	Dense6	(None,8)	Dense5	
	Dense7	(None,16)	Dense6	
	Dense8	(None,16)	Dense7	

[0102]

[0103] 오토인코더 생성부(125)는 시간 도메인 오토인코더, 주파수 도메인 오토인코더, 다중 도메인 오토인코더를 통해 상기 EEG 신호의 다중 도메인 특징을 얻을 수 있다.

[0104] 오토인코더는 뉴런 수가 가장 적은 완전 연결(Fully Connected, FC)이다.

[0105] 오토인코더에서 활성화 함수는 Tanh로 설정되고 손실 함수는 평균 제곱 오차로 정의되며, 최적화 도구는 Adam이다.

[0106] h_m 은 개인 간에 EEG의 차이가 크기 때문에 개인별로 맞춤화되어 암호화 알고리즘의 성능 향상에 도움이 된다.

[0107] 깊은 다중 도메인 특징 h_m 은 수학식 11을 이용하여 비밀키 공간으로 매핑한다.

수학식 11

[0108]
$$\overline{X_i} = a + (\frac{b-a}{X_{min} - X_{max}})(X_i - X_{max}), a < b$$

[0109] 여기서, a와 b는 비밀키 공간에서 최소값과 최대값을 나타내고, a와 b는 0.1과 0.5이고, $\overline{X_i}$ 와 X_i는 각각 정규

화 전 i번째 샘플의 특징을 나타내고, X_{min} 와 X_{max} 는 각각 특징의 최소값과 최대값을 나타낸다.

[0110] 제어부(122)는 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 의사 난수 생성기(126)를 생성한다.

[0111] 도 7은 본 발명의 실시예에 따른 카오스 매핑을 기반으로 한 의사 난수 생성기를 생성하는 과정을 나타낸 도면이다.

[0112] 제어부(122)는 EEG 고유값을 입력받고(S100), EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 이용하여 의사 난수열을 발생하는 장치인 의사 난수 생성기(126)를 생성할 수 있다(S110, S120, S130).

[0113] 암호화 초기에는 3개의 Deep Autoencoder를 통해 EEG 신호의 다중 도메인 특징을 얻을 수 있으며, EEG 고유값을 이중 암호화 장치(120)의 키로 정규화하여 초기 인자를 얻는다. EEG 신호 자체에는 무작위성이 있다.

[0114] EEG 고유값을 키의 일부로 사용하면 키의 비밀성을 크게 향상시킬 수 있다.

[0115] 본 발명에서는 PLCM과 LTM을 기반으로 한 이중 카오스 의사 난수 생성기(126)를 제공하며, 반복 횟수는 단일 카오스 생성기와 동일하다. 이 알고리즘에서는 PLCM의 초기값 y(0), 구조 매개변수 P 및 LTM의 구조 매개변수 u인 3개의 EEG 고유값이 키로 사용된다.

[0116] PLCM은 반복을 통해 (0, 1) 범위의 무작위 시퀀스를 얻을 수 있다.

[0117] PLCM 반복의 처음 20개 숫자는 삭제되고, 21번째 값이 유효한 값으로 시작됩니다. 이 값을 LTM의 초기값으로 삼고, LTM의 반복 횟수는 10,000으로 설정한다. LTM의 반복 횟수를 지정하면 PLCM은 한 번 반복하여 다음 LTM의 초기값을 생성한다. 그림 9는 랜덤 시퀀스의 생성 흐름도를 보여준다. PLCM에서 생성된 시퀀스도 랜덤이므로 단일 카오스와 동일한 계산량으로 LTM에 랜덤 간섭을 추가하여 궤도의 예측 불가능성을 보장한다.

[0118] 도 8은 본 발명의 실시예에 따른 이중 카오스 암호화 프로세스를 나타낸 도면이다.

[0119] EEG 고유값 계산부(124)는 초기값의 무작위성을 확보하기 위해 깊은 다중 도메인 특징을 포함하는 EEG(Electroencephalogram) 고유값을 카오스 기반 의사 난수(Pseudo-Random) 생성기의 초기 인자로 추출한다(S200, S210).

[0120] 제어부(122)는 추출한 EEG 고유값을 이용하여 의사 난수 특성을 갖는 카오스 매핑인 PLCM(Piecewise Linear Map)과, Logistic 매핑과 Tent 매핑을 결합한 카오스 매핑인 LTM(Coupled Logistic-Tent map)을 기반으로 하이브리드 의사 난수 생성기를 생성한다(S220).

[0121] 이중 카오스 암호화 처리부(127)는 (0, 1) 범위의 무작위성을 갖는 카오스 시퀀스 Xn을 의사 난수 생성기(126)에 의해 얻어진다. 그러면 암호화에 사용되는 이진 시퀀스 Sn은 다음의 수학식 12와 같은 임계값으로 판단할 수 있다.

[0122] 이중 카오스 암호화 처리부(127)는 의사 난수 생성기(126)의 출력으로 (0, 1) 범위의 무작위성을 갖는 카오스 시퀀스(Chaotic Sequence) Xn을 얻고, 카오스 시퀀스(Chaotic Sequence) Xn을 하기의 수학식 12에 대입하여 암호화에 사용되는 이진 시퀀스(Binary Sequence) Sn을 얻는다.

[0123] 이중 카오스 암호화 처리부(127)는 I(M, N)으로 표현되는 평문을 픽셀 단위의 행렬(M,N)로 형성하고(S230, S240), 픽셀 단위의 행렬(M,N)dmf 이진 시퀀스(Binary Sequence) In으로 변환한다(S250).

[0124] 이중 카오스 암호화 처리부(127)는 I(M, N)으로 표현되는 평문의 유효 정보를 길이가 n = M × N × 8인 이진 시퀀스(Binary Sequence) In으로 변환하고, 하기의 수학식 11를 이용하여 랜덤 시퀀스 스트림 Sn과 평문 시퀀스 스트림 Xn을 XOR 연산을 통해 암호문 시퀀스 스트림 Zn을 얻는다(S260).

[0125] I(M, N)으로 표현되는 평문의 유효 정보를 암호화 시스템에서 완전히 숨겨야 한다는 목적은 본 발명에서 제안하는 스트림 암호화 기법을 통해 달성할 수 있다.

[0126] 일반 텍스트를 길이가 n = M × N × 8인 이진 시퀀스 In으로 변환한다. 이는 필요한 카오스 시퀀스의

길이이다.

[0127] 암호문 시퀀스 스트림 Zn은 하기의 수학식 13을 이용하여 랜덤 시퀀스 스트림 Sn과 평문 시퀀스 스트림 Xn을 XOR 연산을 통해 얻을 수 있다.

[0128] 전송해야 할 암호문 시퀀스 스트림 Zn은 랜덤 시퀀스 스트림 Sn과 평문 시퀀스 스트림 Xn을 비교하여 얻을 수 있다. 수학식 13은 이중 카오스 기반의 암호화 과정을 보여준다.

수학식 12

[0129] $$S_n = \begin{cases} 1, & x_n > 0.5 \\ 0, & x_n < 0.5 \end{cases}$$

수학식 13

[0130] $$encryption_processZ_n = S_n \oplus I_n$$

[0131] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

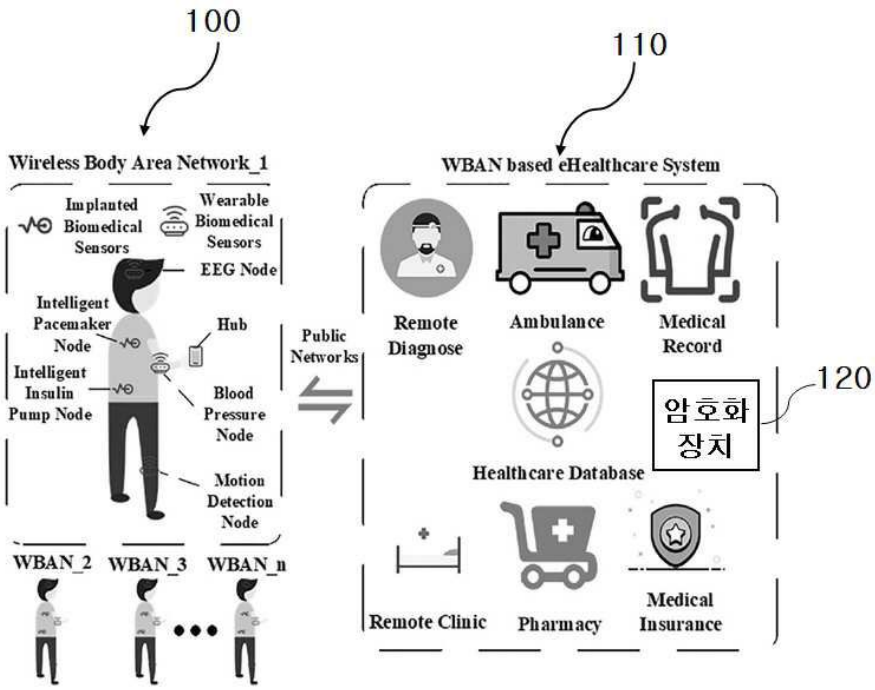
[0132] 100: WBAN

110: E-헬스케어 서비스 시스템

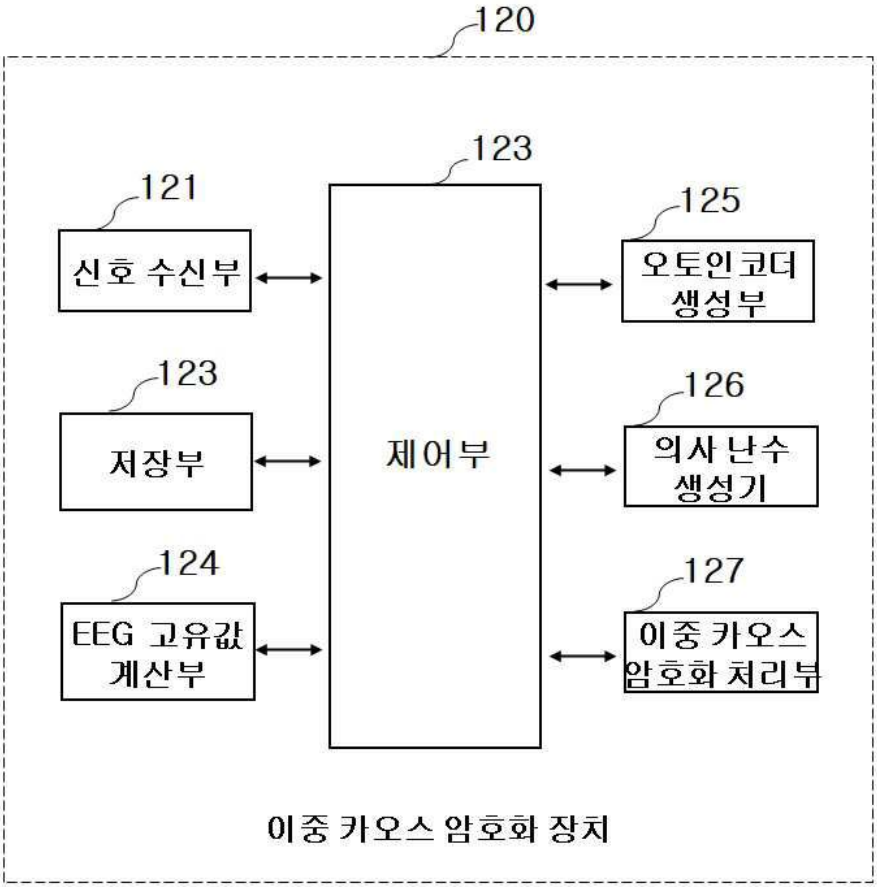
120: 이중 카오스 암호화 장치

도면

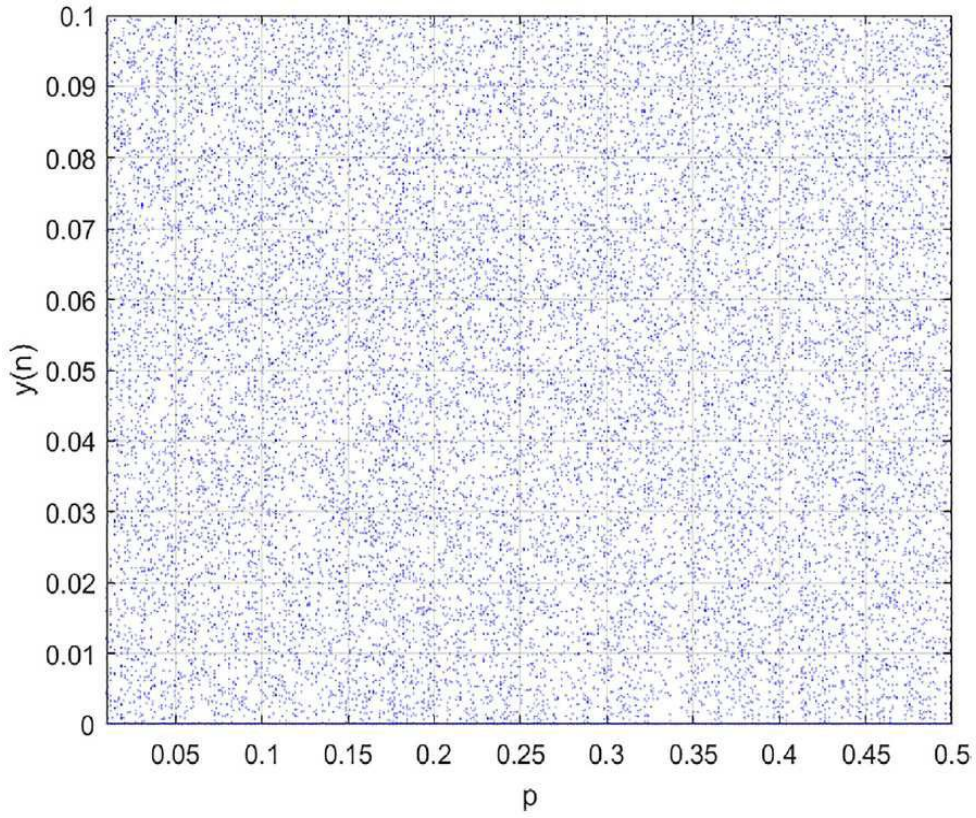
도면1


100
110
Wireless Body Area Network_1
WBAN based eHealthcare System
Implanted Biomedical Sensors
Wearable Biomedical Sensors
EEG Node
Intelligent Pacemaker Node
Hub
Intelligent Insulin Pump Node
Blood Pressure Node
Motion Detection Node
Public Networks
Remote Diagnose
Ambulance
Medical Record
120
암호화 장치
Healthcare Database
Remote Clinic
Pharmacy
Medical Insurance
WBAN_2
WBAN_3
WBAN_n

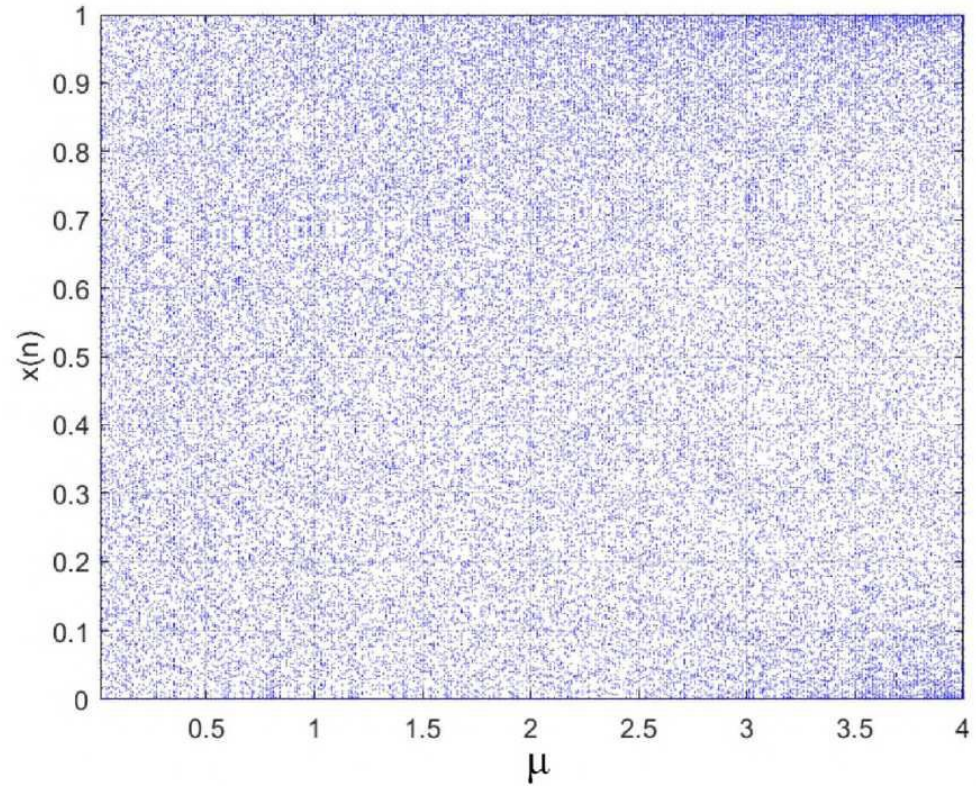
도면2


120
123
121
신호 수신부
125
오토인코더 생성부
123
저장부
제어부
126
의사 난수 생성기
124
EEG 고유값 계산부
127
이중 카오스 암호화 처리부
이중 카오스 암호화 장치

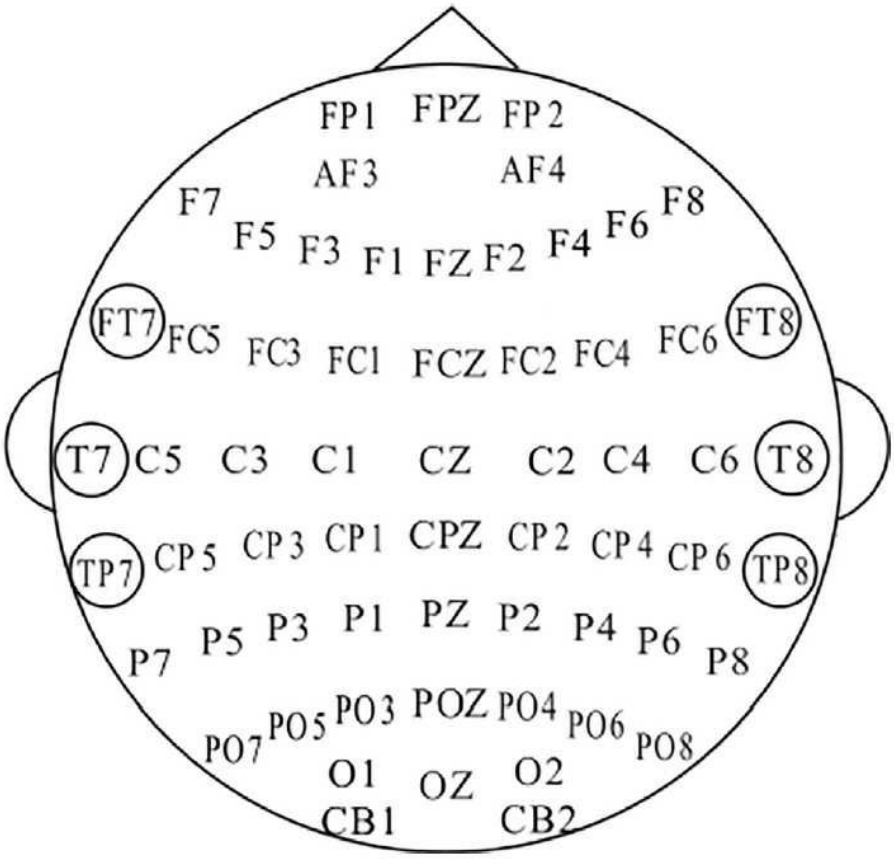
도면3


0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
y(n)
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
p

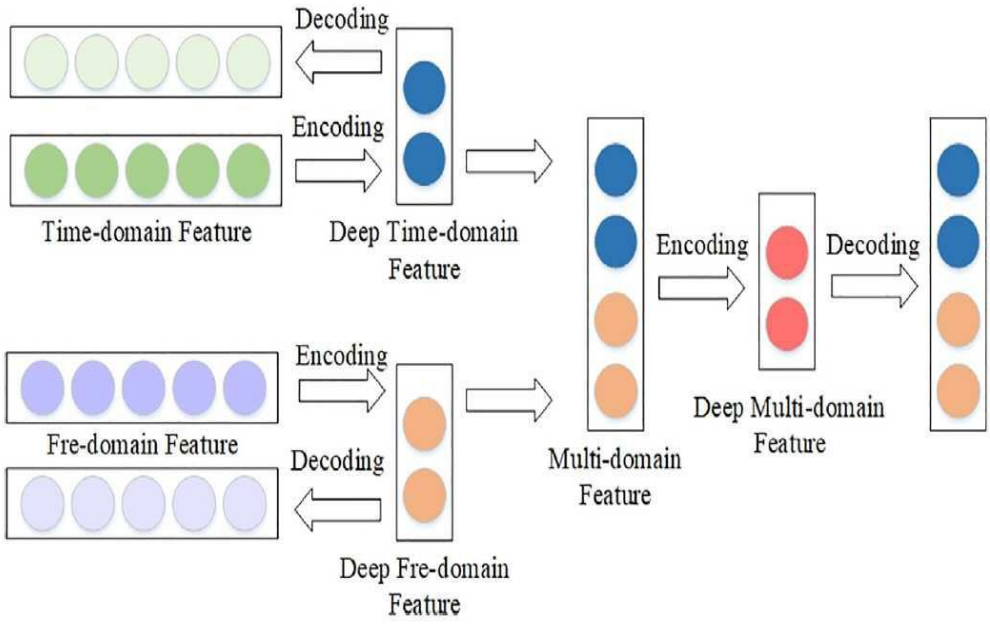
도면4


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
x(n)
0.5
1
1.5
2
2.5
3
3.5
4
μ

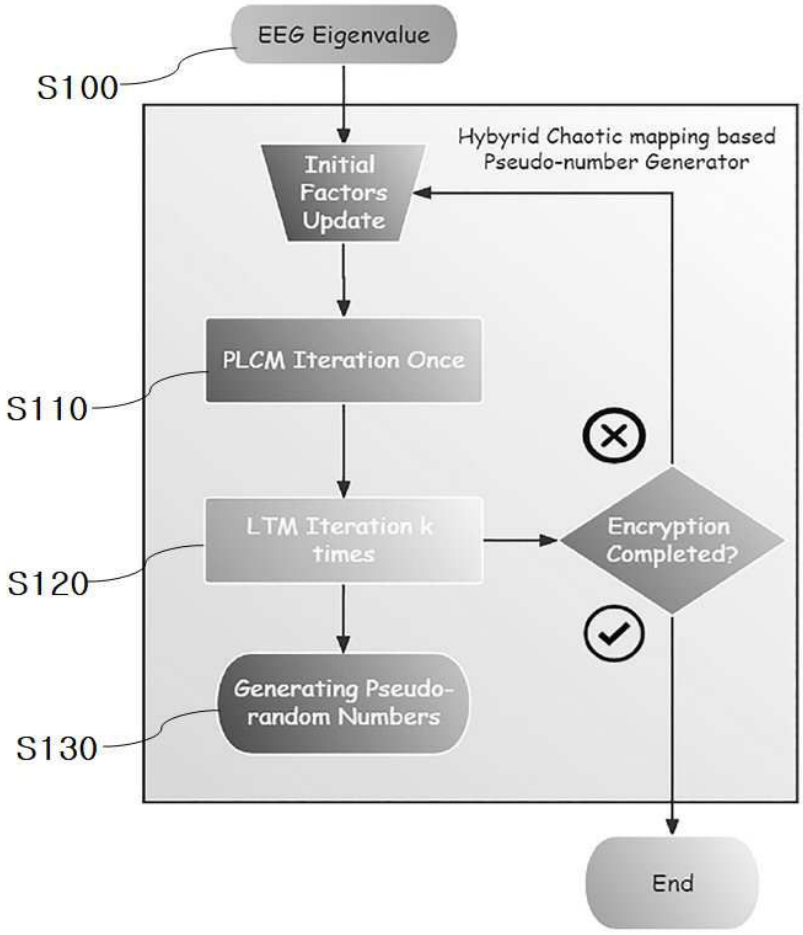
도면5


FP1
FPZ
FP2
AF3
AF4
F7
F5
F3
F1
FZ
F2
F4
F6
F8
FT7
FC5
FC3
FC1
FCZ
FC2
FC4
FC6
FT8
T7
C5
C3
C1
CZ
C2
C4
C6
T8
TP7
CP5
CP3
CP1
CPZ
CP2
CP4
CP6
TP8
P7
P5
P3
P1
PZ
P2
P4
P6
P8
PO7
PO5
PO3
POZ
PO4
PO6
PO8
O1
OZ
O2
CB1
CB2

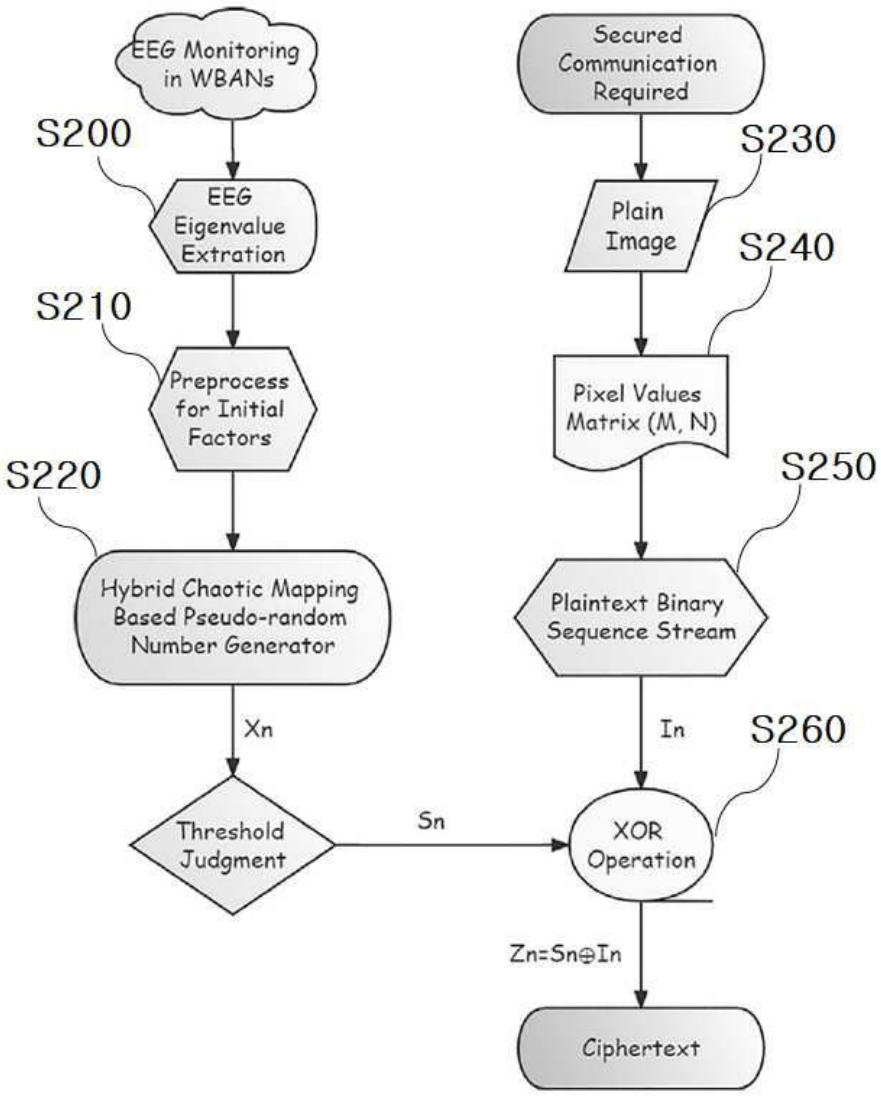
도면6


Decoding
Encoding
Time-domain Feature
Deep Time-domain Feature
Encoding
Decoding
Encoding
Fre-domain Feature
Decoding
Deep Fre-domain Feature
Multi-domain Feature
Deep Multi-domain Feature

도면7


EEG Eigenvalue
S100
Hybyrid Chaotic mapping based Pseudo-number Generator
Initial Factors Update
PLCM Iteration Once
S110
LTM Iteration k times
S120
Encryption Completed?
Generating Pseudo-random Numbers
S130
End

도면8


EEG Monitoring in WBANs
S200
EEG Eigenvalue Extration
S210
Preprocess for Initial Factors
S220
Hybrid Chaotic Mapping Based Pseudo-random Number Generator
Xn
Threshold Judgment
Sn
Secured Communication Required
S230
Plain Image
S240
Pixel Values Matrix (M, N)
S250
Plaintext Binary Sequence Stream
In
S260
XOR Operation
Zn=Sn⊕In
Ciphertext