(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0104728
(43) 공개일자 2019년09월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04B 13/00* (2006.01)
(52) CPC특허분류
H04L 9/001 (2013.01)
H04B 13/005 (2013.01)
(21) 출원번호 10-2018-0025196
(22) 출원일자 2018년03월02일
심사청구일자 2018년03월02일
기술이전 희망 : 기술양도

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 아카데미로 119 (송도동)
(72) 발명자
전광길
인천광역시 연수구 경원대로119번길 21, 114동 904호(동춘동, 풍림2차아파트)
(74) 대리인
특허법인충정

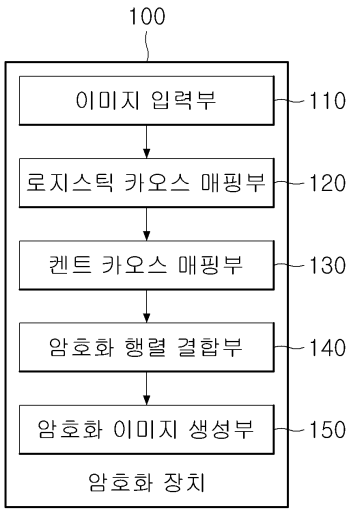
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **신체 영역 네트워크에서 카오스에 기반한 암호화 장치 및 방법**

(57) 요 약

신체 영역 네트워크에서 카오스에 기반한 암호화 장치 및 방법은 원본 이미지에 로지스틱 카오스 매핑(Logistic Chaotic Mapping)과 켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 서브 카오스 행렬이 각각 생성되고, 카오스 암호화된 행렬을 얻기 위해서 2개의 서브 카오스 행렬을 결합하며, 초기 데이터 행렬 및 카오스 암호화된 행렬을 XOR 연산을 수행하여 암호화된 이미지를 획득한다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

원본 이미지 I(i, j)를 읽어 원본 이미지 데이터 행렬 T를 형성하는 이미지 입력부;

로지스틱 카오스 매핑(Logistic Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sl를 구성하는 로지스틱 카오스 매핑부;

켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sk를 구성하는 켄트 카오스 매핑부;

상기 서브 카오스 행렬 Sl과 상기 서브 카오스 행렬 Sk를 결합하여 카오스 암호화된 2차원 카오스 행렬 Ec를 형성하는 암호화 행렬 결합부; 및

상기 원본 이미지 데이터 행렬 T와 상기 2차원 카오스 행렬 Ec를 XOR 연산하여 암호화된 이미지 행렬 E를 생성하는 암호화 이미지 생성부를 포함하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

청구항 2

제1항에 있어서,

상기 로지스틱 카오스 매핑부는 상기 로지스틱 카오스 매핑에서 하기의 수학식 1에 의해 X_0와 μ의 초기 파라미터 값을 설정하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

[수학식 1]

$$x_n = \mu * x_{n-1}(1 - x_{n-1})$$

여기서, μ는 비선형 강도 제어를 위한 매개 변수이고, Xn은 n번째 반복 이후의 상태 변수의 값을 나타낸다. μ ∈ [3.5699456, 4], Xn ∈ [0, 1] 및 n ∈ N 일 때, 카오스 상태임.

청구항 3

제1항에 있어서,

상기 켄트 카오스 매핑부는 상기 켄트 카오스 매핑에서 하기의 수학식 2에 의해 Y_0와 a의 초기 파라미터 값을 설정하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

[수학식 2]

$$y_n = \begin{cases} \frac{y_n}{a}, & 0 < x \le a \\ \frac{1-y_n}{1-a}, & a < x \le 1 \end{cases}$$

여기서, a는 제어 매개 변수이다. 0.4 < a < 0.5 및 Yn ∈ [0, 1] 일 때, 이상적인 카오스 상태임.

청구항 4

제2항에 있어서,

상기 로지스틱 카오스 매핑부는 반복루프(iteration) X_0의 초기값과 매개 변수 μ를 설정하고, 카오스 상태가 되어 $n_1 = M \times N_1$ and $N_1 = N\text{-}ceil(N/2)$을 가진 1차원 카오스 시퀀스 $x = \{x_1, x_2, \ldots, x_{n1}\}$를 생성하고. 1차원 카오틱 시퀀스 X의 행과 열의 수가 재조정되는 것을 특징으로

하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

청구항 5

제1항에 있어서,

상기 켄트 카오스 매핑부는 반복루프(iteration) Y_0의 a의 초기 파라미터 값을 설정하고, 암호화 장치는 카오스 상태가 되어 $n_2 = M \times N_2$ and N_2=N-ceil(N/2)을 가진 1차원 카오스 시퀀스 Y={Y_1, Y_2..., Yn_2}를 생성하고, 1차원 카오틱 시퀀스 Y의 행과 열의 수가 재조정되는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

청구항 6

제1항에 있어서,

상기 암호화 행렬 결합부는 상기 서브 카오스 행렬 Sl과 상기 서브 카오스 행렬 Sk를 결합하여 카오스 암호화된 2차원 카오스 행렬 Ec를 하기의 수학식 3과 같이 나타내는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치.

[수학식 3]

$$E_{C_{M\times N}} = \{Sl_{M\times N_1};\ Sk_{M\times N_2}\}$$

청구항 7

원본 이미지 I(i, j)를 읽어 원본 이미지 데이터 행렬 T를 형성하는 단계;

로지스틱 카오스 매핑(Logistic Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sl를 구성하는 단계;

켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sk를 구성하는 단계;

상기 서브 카오스 행렬 Sl과 상기 서브 카오스 행렬 Sk를 결합하여 카오스 암호화된 2차원 카오스 행렬 Ec를 형성하는 단계; 및

상기 원본 이미지 데이터 행렬 T와 상기 2차원 카오스 행렬 Ec를 XOR 연산하여 암호화된 이미지 행렬 E를 생성하는 단계를 포함하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 방법.

청구항 8

제7항에 있어서,

상기 서브 카오스 행렬(Sub-Chaotic Matrix) Sl를 구성하는 단계는,

상기 로지스틱 카오스 매핑에서 하기의 수학식 1에 의해 X_0와 μ의 초기 파라미터 값을 설정하는 단계; 및

반복루프(iteration) X_0의 초기값과 매개 변수 μ를 설정하고, 카오스 상태가 되어 $n_1 = M \times N_1$ and $N_1 = N\text{-}ceil(N/2)$을 가진 1차원 카오스 시퀀스 $x = \{x_1, x_2, \ldots, x_{n1}\}$를 생성하고. 1차원 카오틱 시퀀스 X의 행과 열의 수가 재조정되는 단계를 포함하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 방법.

[수학식 1]

$$x_n = \mu * x_{n-1}(1 - x_{n-1})$$

여기서, μ는 비선형 강도 제어를 위한 매개 변수이고, Xn은 n번째 반복 이후의 상태 변수의 값을 나타낸다. μ ∈ [3.5699456, 4], Xn ∈ [0, 1] 및 n ∈ N 일 때, 카오스 상태임.

청구항 9

제7항에 있어서,

상기 서브 카오스 행렬(Sub-Chaotic Matrix) Sk를 구성하는 단계는,

상기 켄트 카오스 매핑에서 하기의 수학식 2에 의해 Y_0와 a의 초기 파라미터 값을 설정하는 단계; 및

반복루프(iteration) Y_0의 a의 초기 파라미터 값을 설정하고, 암호화 장치는 카오스 상태가 되어 $n_2 = M \times N_2$ and N_2=N-ceil(N/2)을 가진 1차원 카오스 시퀀스 Y={Y_1, Y_2..., Yn_2}를 생성하고, 1차원 카오틱 시퀀스 Y의 행과 열의 수가 재조정되는 단계를 포함하는 것을 특징으로 하는 신체 영역 네트워크에서 카오스에 기반한 암호화 방법.

[수학식 2]

$$y_n = \begin{cases} \frac{y_n}{a}, & 0 < x \le a \\ \frac{1-y_n}{1-a}, & a < x \le 1 \end{cases}$$

여기서, a는 제어 매개 변수이다. 0.4 < a < 0.5 및 Yn ∈ [0, 1] 일 때, 이상적인 카오스 상태임.

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화 방법에 관한 것으로서, 특히 원본 이미지에 로지스틱 카오스 매핑(Logistic Chaotic Mapping)과 켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 서브 카오스 행렬이 각각 생성되고, 카오스 암호화된 행렬을 얻기 위해서 2개의 서브 카오스 행렬을 결합하며, 초기 데이터 행렬 및 카오스 암호화된 행렬을 XOR 연산을 수행하여 암호화된 이미지를 획득하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 신체 부위 네트워크(BAN)에서는 개인의 생리 데이터가 매우 민감하기 때문에 센서 노드의 데이터 암호화가 매우 중요하다.

[0003] 그러나 과거의 암호화 방법은 키 공간이 작기 때문에 공격에 취약하다.

[0004] 네트워크의 필요성과 고혈압 및 당뇨병과 같은 만성 질환의 보급과 함께 인체 주변의 무선 네트워크와 관련된 애플리케이션이 큰 관심을 끌기 때문에 센서와 노드를 연결하는 웨어러블 시스템인 BAN(body area network)이 등장했다.

[0005] 도 1에 도시된 바와 같이 인체 내부, 주변 또는 그 주위에 배치될 수 있다.

[0006] BAN은 원격 생체 진단, 응급 치료 및 건강 정보 서비스를 지원하는 인간의 활력 징후를 얻을 수 있다.

[0007] 사용자의 경우 생체 신호 정보는 매우 비공개이며 권한있는 기관에서만 액세스할 수 있다. 보안은 BAN에서 필수적이다. BAN은 신원 인증, 개인 정보 보호 및 정보 완전성을 지원한다. 기존의 암호화 기술은 많은 영역에 적용된다.

[0008] BAN은 사전에 키가 배포된 방법, 암호화 및 암호 해독 알고리즘 등 많은 암호화 방법이 연구되어 적용되었다.

[0009] 그러나 BAN 노드의 출처가 제한되어 있기 때문에 키 사전 배포 체계, 키 배포 센터, RSA 공개 키 인프라 및 타원 기능 공개 키 인프라는 BAN 응용 프로그램에 적합하지 않다. 첫 번째 방법으로 암호화 및 암호 해독 알고리즘은 많은 수의 연산을 필요로 하므로 전력 소비가 급격히 증가하며, 극단적인 저전력 BAN 노드의 요구 사항을 고려할 때 BAN 시스템에 적합하지 않다.

[0010] 두 번째 방법은 BAN 채널의 특성을 키로 사용하여 물리 계층의 통신 측면 간에 대칭 키를 임의로 생성 할 수 있다.

[0011] 두 번째 방법은 수신된 무선 채널 신호 강도를 계산한 값에 따라 수신기에 키를 생성한다. 도청자와 수신자의 거리가 일정하지 않기 때문에 신호 강도값이 달라져 도청자가 데이터를 해독할 수 없다.

[0012] 그러나 이러한 두 번째 방법은 송신기가 도청자 및 수신기와 같은 거리를 가질 때 실패 할 수 있는 문제점이 있다.

[0013] 세 번째 방법은 생체 신호 정보에 따라 키를 생성한다. 일반적인 센서 네트워크 노드와 달리 BAN 노드의 매개변수는 인간의 생리적 신호이며 다른 개인에 따라 다른 기능을 나타낸다. 동일한 개인의 경우에도 값은 시간이 지남에 따라 천천히 변한다.

[0014] 생리적 파라미터를 사용하는 키 생성 접근법이 BAN 시스템에 적당하지만, 일부 파라미터의 고유값이 시간에 따라 명백한 변화없이 유사하며 암호화 강도가 약한 문제점이 있다.

[0015] 전술한 종래의 암호화 방법은 약한 암호화 강도의 단점을 가지고 있기 때문에 낮은 저항과 감도의 단점이 있다.

선행기술문헌

특허문헌

[0016] (특허문헌 0001) 한국 등록특허번호 제10-1502930호("발명의 명칭: 비대칭 카오스 암호화")

발명의 내용

해결하려는 과제

[0017] 이와 같은 문제점을 해결하기 위하여, 본 발명은 원본 이미지에 로지스틱 카오스 매핑(Logistic Chaotic Mapping)과 켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 서브 카오스 행렬이 각각 생성되고, 카오스 암호화된 행렬을 얻기 위해서 2개의 서브 카오스 행렬을 결합하며, 초기 데이터 행렬 및 카오스 암호화된 행렬을 XOR 연산을 수행하여 암호화된 이미지를 획득하는 신체 영역 네트워크에서 카오스에 기반한 암호화 장치 및 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0018] 상기 목적을 달성하기 위한 본 발명의 특징에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 장치는,

[0019] 원본 이미지 I(i, j)를 읽어 원본 이미지 데이터 행렬 T를 형성하는 이미지 입력부;

[0020] 로지스틱 카오스 매핑(Logistic Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sl를 구성하는 로지스틱 카오스 매핑부;

[0021] 켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sk를 구성하는 켄트 카오스 매핑부;

[0022] 상기 서브 카오스 행렬 Sl과 상기 서브 카오스 행렬 Sk를 결합하여 카오스 암호화된 2차원 카오스 행렬 Ec를 형성하는 암호화 행렬 결합부; 및

[0023] 상기 원본 이미지 데이터 행렬 T와 상기 2차원 카오스 행렬 Ec를 XOR 연산하여 암호화된 이미지 행렬 E를 생성하는 암호화 이미지 생성부를 포함하는 것을 특징으로 한다.

[0024] 본 발명의 특징에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 방법은,

[0025] 원본 이미지 I(i, j)를 읽어 원본 이미지 데이터 행렬 T를 형성하는 단계;

[0026] 로지스틱 카오스 매핑(Logistic Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sl를 구성하는 단계;

[0027] 켄트 카오스 매핑(Kent Chaotic Mapping)으로 생성된 1차원 카오스 시퀀스에 따른 부분행렬인 서브 카오스 행렬(Sub-Chaotic Matrix) Sk를 구성하는 단계;

[0028] 상기 서브 카오스 행렬 Sl과 상기 서브 카오스 행렬 Sk를 결합하여 카오스 암호화된 2차원 카오스 행렬 Ec를 형

성하는 단계; 및

[0029] 상기 원본 이미지 데이터 행렬 T와 상기 2차원 카오스 행렬 Ec를 XOR 연산하여 암호화된 이미지 행렬 E를 생성하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0030] 전술한 구성에 의하여, 본 발명은 Logistic 카오스 매핑과 Kent 카오스 매핑의 결합이 카오스 시스템의 암호화의 보안을 향상시키고 높은 저항과 감도를 갖는 시스템을 제공하는 효과가 있다.

[0031] 본 발명은 키 공간이 크고 키 감도가 높고 공격 저항 능력이 뛰어나며 BAN 시스템의 프라이버시 보호에 적합한 효과가 있다.

도면의 간단한 설명

[0032] 도 1은 종래의 신체 부위 네트워크의 구성을 개념적으로 나타낸 도면이다.

도 2는 본 발명의 실시예에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 장치의 구성을 나타낸 도면이다.

도 3은 본 발명의 실시예에 따른로지스틱(Logistic) 매핑의 일례를 나타낸 도면이다.

도 4는 본 발명의 실시예에 따른 켄트(Kent) 매핑의 시계열을 나타낸 도면이다.

도 5는 본 발명의 실시예에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 방법을 나타낸 도면이다.

도 6은 본 발명의 실시예에 따른 원본 회색 이미지에 대한 실험 결과를 나타낸 도면이다.

도 7은 본 발명의 실시예에 따른 원본 컬러 이미지에 대한 실험 결과를 나타낸 도면이다.

도 8은 본 발명의 실시예에 따른 원본 회색 이미지와 암호화된 회색 이미지의 서로 다른 방향의 상관 관계를 나타낸 도면이다.

도 9는 본 발명의 실시예에 따른 그레이 이미지의 키 민감도 테스트 결과를 나타낸 도면이다.

도 10은 본 발명의 실시예에 따른 컬러 이미지의 키 민감도 테스트 결과를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0033] 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.

[0034] 본 발명은 결합된 카오스에 기반한 새로운 암호화 알고리즘을 제안한다. 먼저 Logistic 카오스 매핑과 Kent 카오스 매핑을 도입하여 두 개의 부분 행렬을 만든 다음 결합된 행렬을 생성하여 원본 데이터와 XOR 연산을 수행하여 암호화한다.

[0035] 실험 결과는 제안된 알고리즘이 키 공간이 크고 키 감도가 높고 공격 저항 능력이 뛰어나며 BAN 시스템의 프라이버시 보호에 적합함을 알 수 있다.

[0036] 카오스 시스템의 결합된 사용은 암호화의 보안을 향상시킬 수 있다. 본 발명에서는 Logistic 카오스 매핑과 Kent의 카오스 매핑을 이용한 알고리즘을 제안하고, 데이터의 암호화를 위한 2차원 카오스 매트릭스를 생성하는 새로운 방법을 제안한다.

[0037] 이러한 방법은 큰 키 공간, 높은 키 감도 및 우수한 공격 저항 능력을 얻을 수 있다.

[0038] 도 1은 본 발명의 실시예에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 장치의 구성을 나타낸 도면이다.

[0039] 본 발명의 실시예에 따른 신체 영역 네트워크에서 카오스에 기반한 암호화 장치(100)는 이미지 입력부(110), 로지스틱 카오스 매핑부(120), 켄트 카오스 매핑부(130), 암호화 행렬 결합부(140) 및 암호화 이미지 생성부(150)를 포함한다.

[0040] 카오스와 암호학 사이에는 자연스러운 연결과 구조적 유사성이 있다. 카오스에서의 초기값의 민감도는 궤도와 직접적으로 관련되어 카오스된 궤도의 혼합 특성을 유도한다. 이러한 민감도는 암호 시스템의 확산 특성에 해당

하며, 카오스 신호의 무작위 유사 특성은 암호 시스템에서 카오스 특성에 해당한다.

[0041] 암호화 시스템의 설계 과정에서 카오스 매핑은 디지털 이산 혼돈 시퀀스의 생성에 필수적이다. 카오스 현상은 특정 비선형 시스템으로 나타낼 수 있지만, 비선형 시스템이 카오스 현상을 일으키는지 여부는 제어 매개 변수의 값에 따라 다르다.

[0042] 카오스 시스템의 수학적 모델을 구성하는 과정에서, 카오스 시스템은 상이한 카오스 현상 및 매개 변수에 따라 카오스 상태를 달성하도록 적응된다.

[0043] 카오스 매핑은 비선형 카오스 방정식이며 혼란스러운 이미지 암호화 알고리즘에 광범위하게 사용되는 가장 일반적인 카오스 모델 중 하나이다.

[0044] 켄트(Kent) 매핑은 성능이 우수한 널리 사용되는 카오스 시스템이다. 따라서, 본 발명의 암호화 방법은 로지스틱 매핑과 켄트 매핑을 적용하여 카오스 시퀀스를 생성한다. 기간 이중화 분기(Period Doubling Bifurcation)는 카오스를 만드는 일반적인 방법이다. 로지스틱 매핑은 제어 매개 변수가 증가하는 비선형 시스템을 나타내어 주기적 배가 현상을 생성하고 카오스 상태를 달성하며, 다음의 [수학식 1]과 같이 나타낸다.

수학식 1

[0045] $$x_n = \mu * x_{n-1}(1 - x_{n-1})$$

[0046] 여기서, μ는 비선형 강도 제어를 위한 매개 변수이고, Xn은 n번째 반복 이후의 상태 변수의 값을 나타낸다. μ ∈ [3.5699456, 4], Xn ∈ [0, 1] 및 n ∈ N 일 때, 암호화 장치(100)는 카오스 상태에 있다. 도 3은 로지스틱(Logistic) 매핑을 보여준다. 켄트(Kent) 매핑은 초기 조건에 대해 높은 민감도를 가진다. 그 궤적은 단기간에 예측할 수 있지만 장기간에 걸쳐 예측할 수 없다. 켄트 매핑은 다음의 [수학식 2]와 같다.

수학식 2

[0047] $$y_n = \begin{cases} \frac{y_n}{a}, & 0 < x \le a \\ \frac{1-y_n}{1-a}, & a < x \le 1 \end{cases}$$

[0048] 여기서, a는 제어 매개 변수이다. 0.4 < a < 0.5 및 Yn ∈ [0, 1] 일 때, 암호화 장치(100)는 상대적으로 이상적인 카오스 상태에 있다. 도 4는 켄트(Kent) 매핑의 시계열을 설명하고 있다.

[0049] BAN 시스템에서는 많은 양의 데이터가 이미지로 저장된다. 따라서, 본 발명에서는 암호화 알고리즘을 기술하고 테스트하기 위해 이미지 형식을 사용한다.

[0050] M×N 크기의 원본 이미지 I에서, I(i, j)는 (i, j)에 위치하는 픽셀 데이터를 나타내며 원본 이미지 데이터 행렬 T를 형성한다. 본 발명에서 제안된 신체 영역 네트워크에서 카오스에 기반한 암호화 방법은 도 5에 도시되어 있다.

[0051] 본 발명의 신체 영역 네트워크에서 카오스에 기반한 암호화 방법은 다음과 같은 단계를 거친다.

[0052] 이미지 입력부(110)는 원본 이미지 I(i, j)를 읽어 원본 이미지 데이터 행렬 T를 형성한다(S100).

[0053] 로지스틱 카오스 매핑부(120)는 로지스틱 카오스 매핑(Logistic Chaotic Mapping)(수학식 1)에서 X_0와 μ의 초기 파라미터 값을 설정하고(S102), 생성된 1차원 카오스 시퀀스에 따라 서브 카오스 행렬(Sub-Chaotic Matrix) S1를 구성한다(S104).

[0054] 로지스틱 카오스 매핑부(120)는 반복루프(iteration) X_0의 초기값과 매개 변수 μ를 설정하고, 암호화 장치(100)는 카오스 상태가 되어 $n_1 = M \times N_1$ and $N_1 = N\text{-}ceil(N/2)$을 가진 1차원 카오스 시퀀스 $x = \{x_1, x_2, \ldots, x_{n1}\}$를 생성한다. 그런 다음 1차원 카오틱 시퀀스 X의 행과 열의 수가 재조정된다.

[0055] $x=\{x_1, x_2,\ldots, x_{n1}\}$의 값은 순서대로 얻어지고 2차원 행렬 Sl의 열에 순차적으로 채워진다. 마지막으로, 크기 $M\times N_1$의 2 차원 서브 카오스 행렬 S l이 생성된다.

[0056] 켄트 카오스 매핑부(130)는 켄트(Kent) 카오스 매핑(수학식 2)에서 Y_0와 a의 초기 파라미터 값을 설정하고(S106), 생성된 1차원 카오스 시퀀스에 따라 서브 카오스 행렬 Sk를 구성한다(S108).

[0057] 크기 $n_2=M\times N_2$ (여기서, $N_2 = N - N_1$)의 서브 카오스 행렬 Sk의 구성 과정은 서브 카오스 행렬 Sl의 구성 과정과 동일하다.

[0058] 켄트 카오스 매핑부(130)는 반복루프(iteration) Y_0의 a의 초기 파라미터 값을 설정하고, 암호화 장치(100)는 카오스 상태가 되어 $n_2=M\times N_2$ and N_2=N-ceil(N/2)을 가진 1차원 카오스 시퀀스 Y={Y_1, Y_2..., Yn_2}를 생성한다. 그런 다음 1차원 카오틱 시퀀스 Y의 행과 열의 수가 재조정된다.

[0059] Y={Y_1, Y_2..., Yn_2}의 값은 순서대로 얻어지고 2차원 행렬 Sk의 열에 순차적으로 채워진다. 마지막으로, 크기 $M\times N_2$의 2 차원 서브 카오스 행렬 Sk이 생성된다.

[0060] 암호화 행렬 결합부(140)는 카오스 암호화된 행렬 Ec를 얻기 위해서 서브-카오스 행렬 Sl 및 Sk를 결합한다(S110).

[0061] 로지스틱(Logistic) 카오스 매핑과 켄트(Kent) 카오스 매핑은 정교하게 연구되었지만, 단독으로 사용될 때 키 공간이 작고 보안성이 떨어지며 시스템 정확도가 제한적이다. 암호화 행렬 결합부(140)는 2차원 카오스 행렬을 생성하기 위해서 로지스틱 카오스 매핑과 켄트 카오스 매핑을 결합한다. 결합 표현식은 다음의 [수학식 3]과 같다.

수학식 3

[0062] $$E_{C_{M\times N}} = \{Sl_{M\times N_1};\ Sk_{M\times N_2}\}$$

[0063] 암호화 이미지 생성부(150)는 최종 암호화된 이미지 E를 얻기 위해서 원본 이미지 데이터 행렬 T와 최종 암호화 행렬 Ec를 XOR 연산을 수행하여 암호화된 이미지 행렬 E를 생성한다(S112, S114).

[0064] 해독 알고리즘은 암호화 알고리즘의 역 과정이다.

[0066] (1) 시각적 결과 분석

[0067] 레퍼런스 평가 기준에 따라 원본 이미지와 암호화된 이미지를 비교한다. 실험에서 로지스틱 카오스 매핑의 초기 파라미터 값은 X_0 = 0.36, u = 3.970이다. 켄트 카오스 맵핑에서 Y_0의 초기 매개 변수 값은 [수학식 1]에서 보여지는 k 반복루프를 수행한 후의 결과이다. 여기서, 로지스틱 카오스 매핑을 위해 k = 500이다. 켄트 카오스 매핑의 a 초기 매개 변수값은 0.414이다.

[0068] 암호화된 그레이 이미지와 픽셀 히스토그램은 도 6에 나와 있다. 암호화된 컬러 이미지와 픽셀 히스토그램은 도 7에 나와 있다. 히스토그램은 그레이 레벨의 분포 특성을 나타낸다.

[0069] 도 6 및 도 7에 도시된 바와 같이, 원본 회색 이미지 및 컬러 이미지에 대한 히스토그램의 분포가 불균일하며, 암호화된 그레이 이미지 및 컬러 이미지에 대한 히스토그램의 분포가 균일하여 암호화된 이미지의 양호한 스크램블링 특성을 나타내고, 평문 이미지의 정보를 효과적으로 은폐하는 것을 알 수 있다.

[0070] 도 6은 원본 회색 이미지에 대한 실험 결과를 나타낸 것이다. 도 6의 (a)는 원본 회색 이미지이고, 도 6의 (b)는 암호화된 그레이 이미지이고, 도 6의 (c)는 원본 회색 이미지의 히스토그램이고, 도 6의 (d)는 암호화된 그레이 이미지의 히스토그램이다.

[0071] 도 7은 원본 컬러 이미지에 대한 실험 결과를 나타낸 것이다. 도 7의 (a)는 원본 컬러 이미지이고, 도 7의 (b)

는 암호화된 컬러 이미지이고, 도 7의 (c)는 원본 컬러 이미지의 R 성분의 히스토그램이고, 도 7의 (d)는 원본 컬러 이미지의 G 성분의 히스토그램이고, 도 7의 (e)는 원본 컬러 이미지의 B 성분의 히스토그램이고, 도 7의 (f)는 암호화된 컬러 이미지의 R 성분의 히스토그램이고, 도 7의 (g)는 암호화된 컬러 이미지의 G 성분의 히스토그램이고, 도 7의 (h)는 암호화된 컬러 이미지의 B 성분의 히스토그램이다.

[0073] (2) 양적 결과 분석

[0074] 원본 이미지의 많은 인접한 픽셀은 동일하거나 유사한 그레이 레벨을 가지기 때문에 인접 픽셀의 상관 관계를 통해 본 발명의 암호화 방법에 대한 효과를 관찰한다. 수평, 수직 및 대각선 방향의 인접한 픽셀의 상관 관계는 다음과 같이 정의된다.

수학식 4

[0075]
$$\gamma = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

수학식 5

[0076]
$$D(x) = \frac{1}{MN}\sum_{i=1}^{MN}(x_i - E(x))^2$$

수학식 6

[0077]
$$E(x) = \frac{1}{MN}\sum_{i=1}^{MN}x_i$$

수학식 7

[0078]
$$\mathrm{cov}(x, y) = \frac{1}{MN}\sum_{i=1}^{MN}(x_i - E(x))(y_i - E(y))$$

[0079] 여기서, x 및 y는 각각 인접한 두 픽셀의 회색값을 나타내며, M 및 N은 이미지에 대한 행 및 열의 수이고, MN은 총 픽셀 수를 나타낸다. 본 발명은 원본 이미지와 암호화된 이미지의 모든 방향에서 1000 내지 3000개의 픽셀 쌍을 무작위로 선택하여 픽셀 상관 관계의 산점도를 나타낸다.

[0080] 도 8은 원본 회색 이미지와 암호화된 회색 이미지의 서로 다른 방향의 상관 관계를 나타낸 것이다. 도 8의 (a)는 원본 회색 이미지의 수평 방향의 상관 산란 플롯(Correlation Scatter Plot)이고, 도 8의 (b)는 원본 회색 이미지의 수직 방향의 상관 산란 플롯이고, 도 8의 (c)는 원본 회색 이미지의 대각선 방향의 상관 산란 플롯이고, 도 8의 (d)는 암호화된 회색 이미지의 수평 방향의 상관 산란 플롯이고, 도 8의 (e)는 암호화된 그레이 이미지의 수직 방향의 상관 산란 플롯이고, 도 8의 (f)는 암호화된 회색 이미지의 대각선 방향의 상관 산란 플롯이다.

[0081] 도 8의 (d), (e) 및 (f)에 도시된 바와 같이, 암호문 이미지에 따른 상관 산란 플롯과 비교하여 평문 이미지에

따른 상관 산란 플롯보다 집중되어 암호화 방법이 평문으로부터 암호문으로의 변환을 달성한다.

[0082] 가로, 세로 및 대각선 방향의 원본 이미지와 암호화된 이미지의 상관 관계는 각각 [표 1]과 [표 2]에 나열되어 있습니다.

[0083] [표 1]은 원본 그레이 이미지와 암호화된 그레이 이미지의 상관 관계를 나타낸다.

표 1

[0084]

Correlation	Horizontal	Vertical	Diagonal
Original image	0.9679	0.9761	0.9722
Encrypted image	0.0272	−0.0114	−0.0484

[0085] [표 2]는 원본 컬러 이미지와 암호화된 컬러 이미지의 상관 관계를 나타낸다.

표 2

[0086]

Correlation	Original color image			Encrypted color image		
	R	G	B	R	G	B
Horizontal	0.9605	0.9654	0.9375	0.0326	0.0765	0.0622
Vertical	0.9716	0.9731	0.9414	0.0027	−0.0019	0.0003
Diagonal	0.9777	0.9654	0.9354	−0.0874	−0.0515	−0.0493

[0087] 모든 방향에서 원본 이미지의 상관값은 0.9이상으로 인접 화소의 그레이 레벨이 유사하고 암호화 이미지의 상관값이 0에 가깝기 때문에 인접 화소의 그레이 레벨이 서로 다르므로 공격에 대한 저항력이 향상된다. 일반적으로 암호화된 이미지와 원본 이미지의 고정 소수점 비율이 작으면 두 이미지의 차이가 더 커지고 스크램블링 효과가 높아진다. 픽셀 변화율(NPCR)의 수는 다음의 [수학식 8]과 [수학식 9]와 같이 나타낸다.

수학식 8

[0088]
$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,\ j)}{MN} \times 100\%$$

수학식 9

[0089]
$$D(i,\ j) = \begin{cases} 0,\ C_1(i,\ j) = C_2(i,\ j) \\ 1,\ C_1(i,\ j) \neq C_2(i,\ j) \end{cases}$$

[0090] 여기서, $C_1(i,\ j)$와 $C_2(i,\ j)$는 각각 픽셀(i, j)에서의 평문과 암호문의 그레이값을 나타내며, D(i, j)는 픽셀(i, j)에서의 평문과 암호문 간의 변화를 나타낸다. 또한, 암호문의 정보 엔트로피는 암호문의 평균 불확실성을 측정하는데 사용되며, 암호문에 그레이값이 나타날 확률이 같을 때 이미지의 정보 엔트로피는 최대 값 8까지이며 이상적 랜덤 이미지 특징이 달성된다.

[0091] 이미지의 정보 엔트로피는 다음의 [수학식 10]과 같이 나타낸다.

수학식 10

$$H(M) = -\sum_{i=1}^{256} P(m(i))\log_2 P(m(i))$$

[0092]

[0093] 여기서, P(m(i))는 그레이값 i의 발생 확률을 나타낸다. 암호문 엔트로피의 값이 이상값 8에 가까울 때 암호화된 이미지는 강한 평균 불확실성과 통계적 공격 및 엔트로피 공격에 대한 높은 내성을 갖는다.

[0094] [표 3]과 [표 4]에서, 본 발명에서 제안된 암호화 방법을 결합된 카오스에 기반한 다른 암호화 알고리즘과 비교한다.

[0095] [표 3]은 원본 회색 이미지의 알고리즘의 성능 비교이고, [표 4]는 원본 컬러 이미지의 알고리즘의 성능 비교이다.

[0096] [표 3]에서 레퍼런스[20]은 NPCR 값을 제공하지 않는다. 이러한 모든 방법 중에서 본 발명의 암호화 방법(알고리즘)은 최대 NPCR 값을 얻는다. 레퍼런스[15]의 알고리즘에서 얻은 H 값은 본 발명의 암호화 방법보다 약간 크지만 본 발명의 암호화 방법이 일반적으로 일반 텍스트에 대한 스크램블링 효과와 감도가 뛰어나 차분 공격에 강한 저항력을 갖는다.

표 3

Indicator	*NPCR*	*H*
Proposed algorithm	0.9991	7.9964
Reference [15]	0.9962	7.9992
Reference [20]	–	7.9822
Reference [21]	0.9985	7.9904

[0097]

표 4

Indicator	*NPCR*			*H*		
	R	G	B	R	G	B
Proposed algorithm	0.9991	0.9991	0.9991	7.9974	7.9969	7.9884
Reference [22]	0.9960	0.9961	0.9962	7.9901	7.9912	7.9921
Reference [23]	0.9960	0.9960	0.9959	7.9972	0.9968	7.9971
Reference [24]	0.9968	0.9968	0.9968	7.9992	7.9992	7.9971

[0098]

[0100] (3) 보안 키의 공간 분석

[0101] 키 공간의 구성과 크기는 암호화 알고리즘의 보안을 결정한다. 본 발명의 암호화 방법(알고리즘)에서는 로지스틱 매핑의 초기값 X_0과 파라미터 μ, 켄트 매핑의 초기값 Y_0와 파라미터 a와 반복 횟수가 암호화 알고리즘의 키

가 된다.

[0102] 각 매개 변수가 소수 자릿수 15개의 2배 정도 숫자로 표현되는 경우 각 매개 변수에 사용할 수 있는 값의 수는 10^{15}이며, 이는 보안키의 공간이 $(10^{15})^4=10^{60}$ 보다 작고, 로지스틱 카오스 시스템과 켄트 카오스 시스템을 기반으로 한 암호화 알고리즘보다 훨씬 클 수 있음을 의미한다.

[0103] 따라서, 본 발명에서 제안된 암호화 알고리즘은 충분한 키 공간을 가지며 철저한 방법의 공격에 저항할 수 있다.

[0104] 암호문 이미지의 키 민감도가 테스트된다. 로지스틱 매핑의 초기값 X_0을 0.3600000000001로 설정하고 다른 매개 변수는 변경하지 않는다.

[0105] 그레이 이미지 및 컬러 이미지의 결과가 도 9 및 도 10에 도시되어 있다.

[0106] 도 9는 그레이 이미지의 키 민감도 테스트 결과를 나타낸 것이다. 도 9의 (a)는 암호화된 그레이 이미지이고, 도 9의 (b)는 올바르게 해독된 그레이 이미지이고, 도 9의 (c)는 초기값 X_0의 작은 변화로 복호화된 그레이 이미지이다.

[0107] 도 10은 컬러 이미지의 키 민감도 테스트 결과를 나타낸 것이다. 도 9의 (a)는 암호화된 컬러 이미지이고, 도 9의 (b)는 올바르게 해독된 컬러 이미지이고, 도 9의 (c)는 초기값 X_0의 작은 변화로 복호화된 컬러 이미지이다.

[0108] 실험 결과에 따르면 X_0의 초기값이 사소한 변화인 10^{-14}인 경우 원본 이미지를 복구할 수 없다. 다른 초기값의 테스트 결과는 유사하다. 이 실험은 제안된 암호화 알고리즘이 키 민감도가 높고 공격에 대한 내성이 뛰어나며 BAN에 적용할 수 있는 알고리즘 보안이 강함을 보여준다.

[0109] 이러한 암호화 알고리즘은 의료 이미징 시스템과 같은 다른 시스템에서도 사용할 수 있다. 자기 공명 영상 시스템에서 전송 중 신호 암호화는 보안 및 개인 정보 보호를 제공하는 데 매우 중요하다.

[0110] 프라이버시 보호를 고려한 BAN 시스템에서는 보안이 중요하다. 본 발명의 암호화 방법에서는 BAN 시스템의 프라이버시 보호를 지원하기 위해 카오스에 기반한 암호화 알고리즘을 제안한다.

[0111] 제안된 알고리즘은 유한 정밀도 연산과 암호화 알고리즘의 보안 사이의 모순을 조정한다.

[0112] 제안된 알고리즘에서 두 가지 다른 카오스 매핑(Logistic 및 Kent 매핑)을 사용하여 하위 카오스 행렬을 생성한다.

[0113] 첫째는 Logistic과 Kent 매핑의 생성된 1차원 카오스 시퀀스에 따른 서브 카오스 행렬이 각각 생성된다. 이러한 두 가지 하위 카오스 매트릭스는 카오스 암호화 행렬을 얻기 위해 결합된다.

[0114] 마지막으로, 원래의 이미지 데이터 행렬 및 카오스 암호화된 행렬에 대해 XOR 연산을 수행하여 암호화된 이미지를 얻는다.

[0115] Lenna 이미지의 암호화는 시각적 관찰, 정량 분석 및 키 공간 분석의 측면에서 테스트된다. 실험은 본 발명의 제안된 알고리즘이 특히 상관 분석 및 매개 변수 분석에서 중요한 이점을 가지고 있음을 보여준다. 좋은 스크램블링 특성, 큰 키 공간, 높은 키 감도 및 뛰어난 공격 저항 능력으로 이미지 정보를 효과적으로 숨길 수 있으며 BAN 시스템의 개인 정보 보호와 관련된 애플리케이션에 적합하다.

[0116] 본 발명은 2차원 카오스 행렬은 Logistic과 Kent 카오스 매핑을 결합하여 생성되며, 이는 매우 간단하고 효과적이다.

[0117] 또한, 본 발명의 암호화 알고리즘을 의료 영상 암호화와 같은 다른 응용 분야로 확장할 수 있다.

[0118] 이상에서 본 발명의 실시예는 장치 및/또는 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하기 위한 프로그램, 그 프로그램이 기록된 기록 매체 등을 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

[0119] 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

[0120] 100: 암호화 장치

110: 이미지 입력부

120: 로지스틱 카오스 매핑부

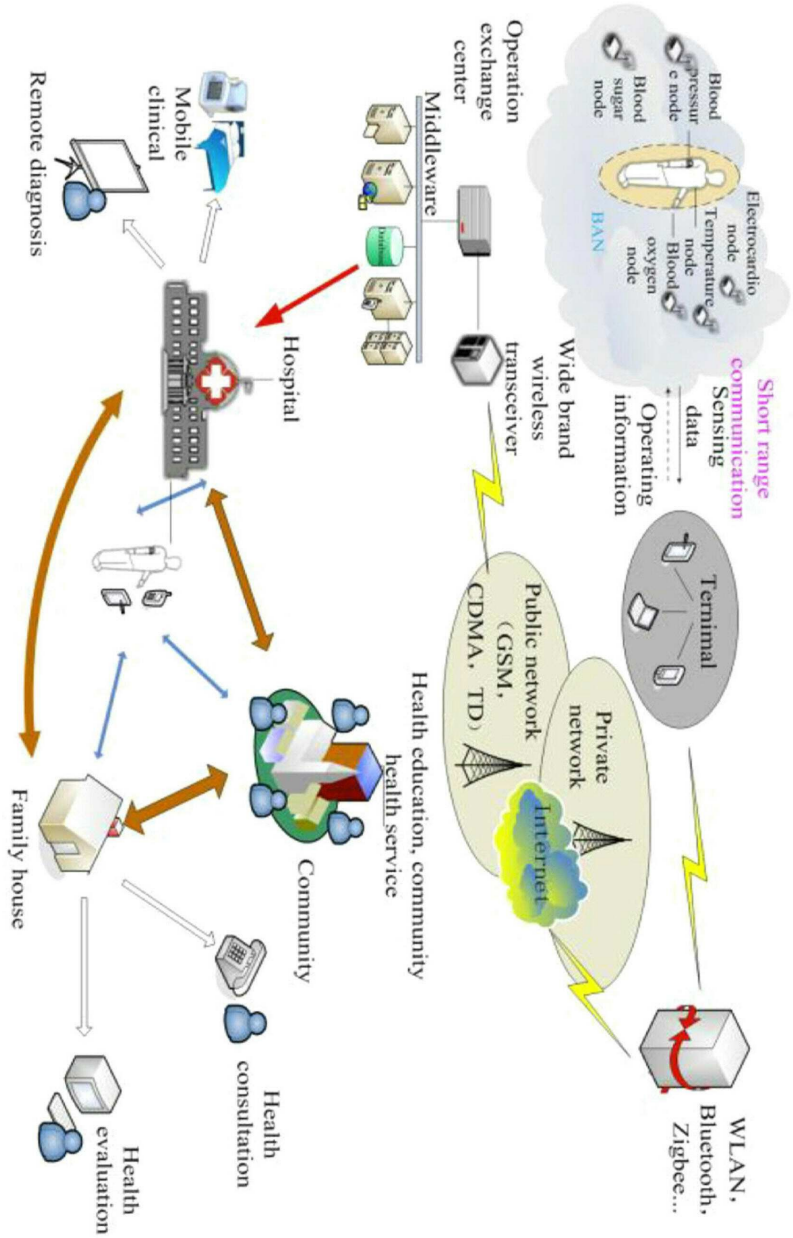
130: 켄트 카오스 매핑부

140: 암호화 행렬 결합부

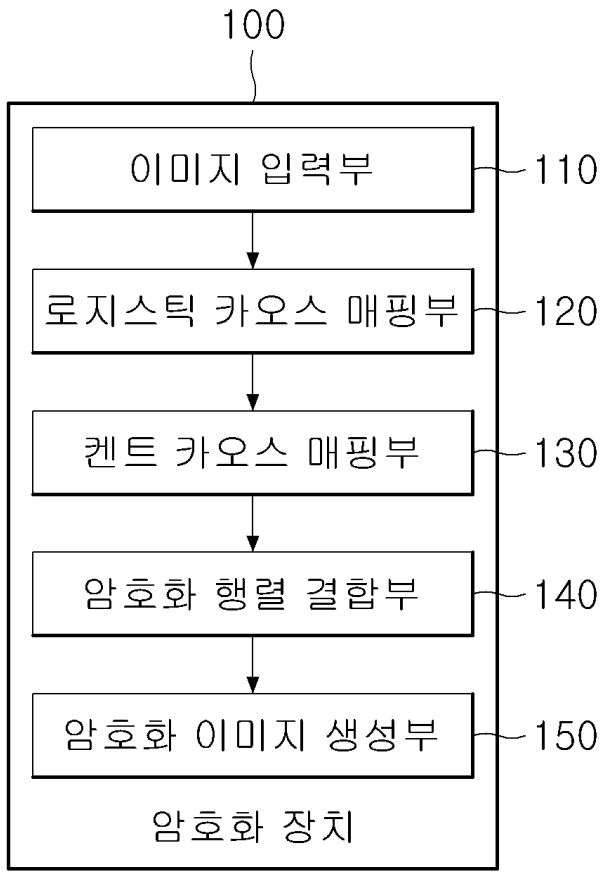
150: 암호화 이미지 생성부

도면

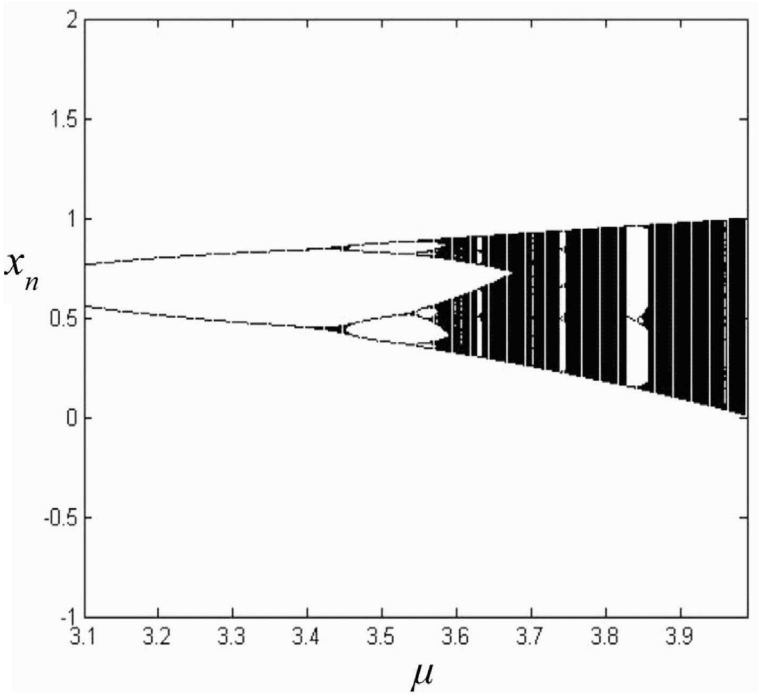
도면1



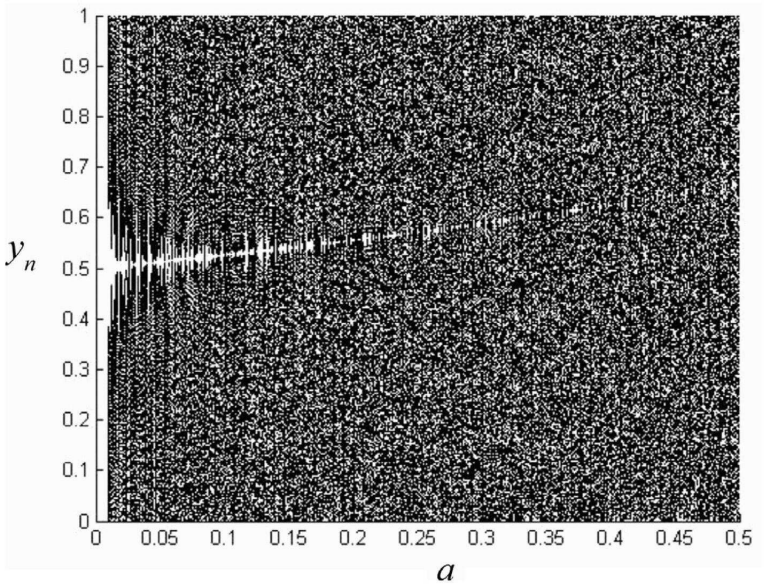
도면2


100
이미지 입력부
110
로지스틱 카오스 매핑부
120
켄트 카오스 매핑부
130
암호화 행렬 결합부
140
암호화 이미지 생성부
150
암호화 장치

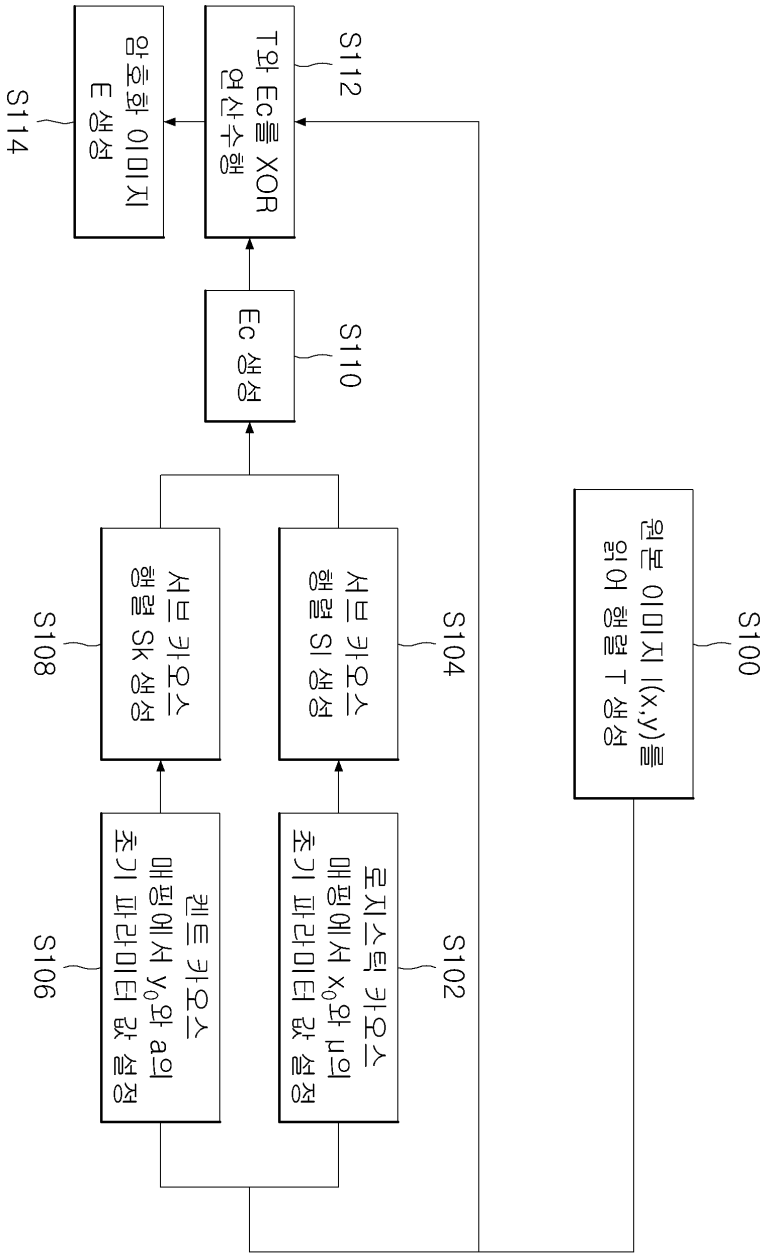
도면3


2
1.5
1
0.5
0
-0.5
-1
x_n
3.1
3.2
3.3
3.4
3.5
3.6
3.7
3.8
3.9
μ

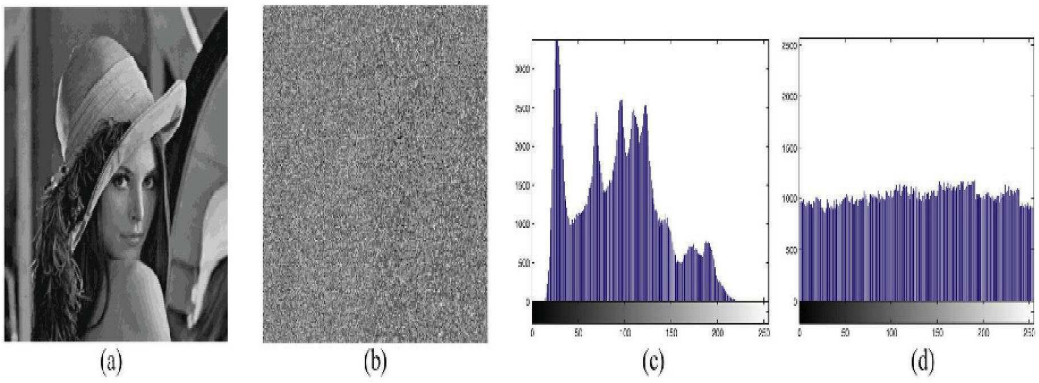
도면4



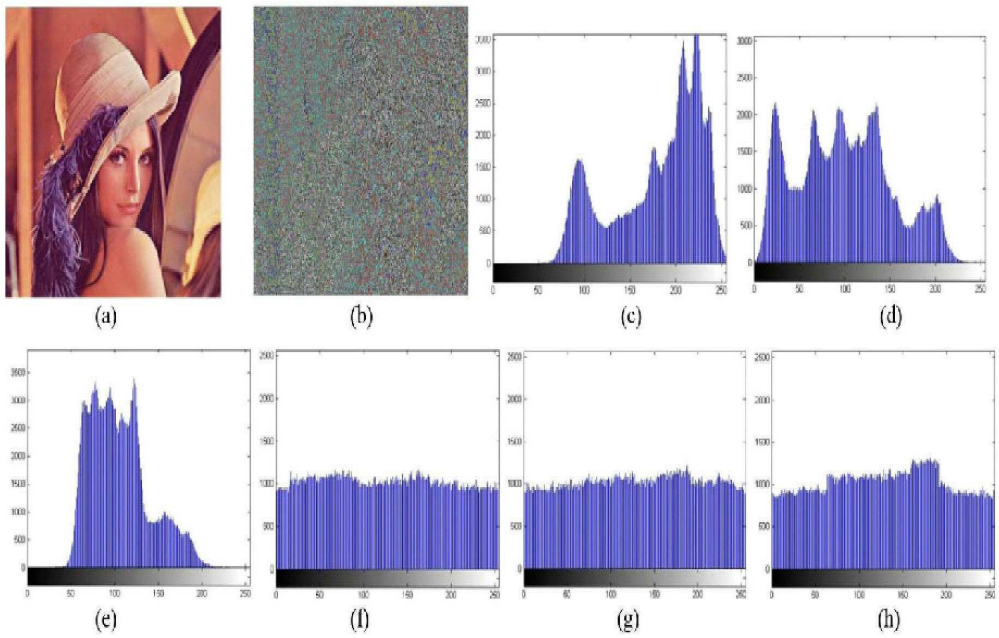
도면5


원본 이미지 I(x,y)를 읽어 행렬 T 생성
S100
로지스틱 카오스 매핑에서 x_0와 μ의 초기 파라미터 값 설정
S102
서브 카오스 행렬 SI 생성
S104
켄트 카오스 매핑에서 y_0와 a의 초기 파라미터 값 설정
S106
서브 카오스 행렬 SK 생성
S108
Ec 생성
S110
T와 Ec를 XOR 연산수행
S112
암호화 이미지 E 생성
S114

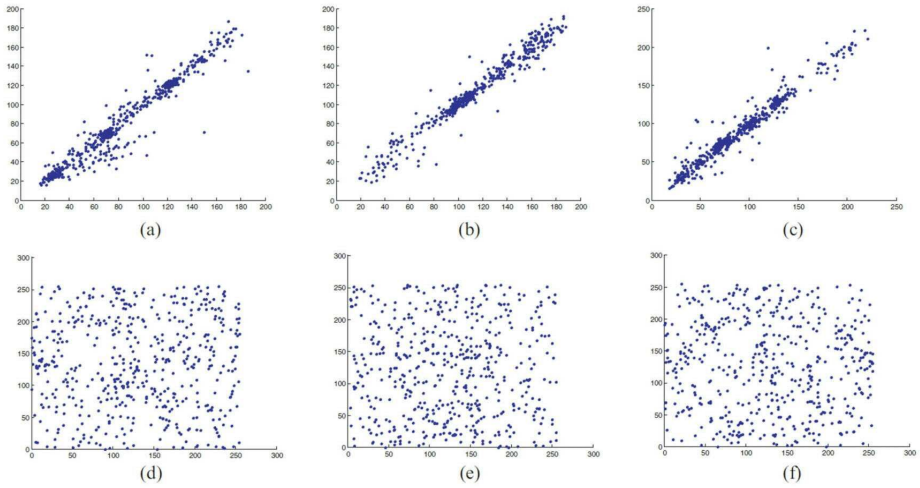
도면6


(a)
(b)
(c)
(d)

도면7



도면8



도면9



도면10



(a) (b) (c)