(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0093739
(43) 공개일자 2013년08월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 21/60* (2013.01)
(21) 출원번호 10-2011-0142669
(22) 출원일자 2011년12월26일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
박장현
서울특별시 서초구 서초중앙로29길 28, 반포미도아파트 303동 1408호 (반포동)
최성훈
서울특별시 마포구 동교로13길 30-3, 2호 (서교동)
(뒷면에 계속)
(74) 대리인
한양특허법인

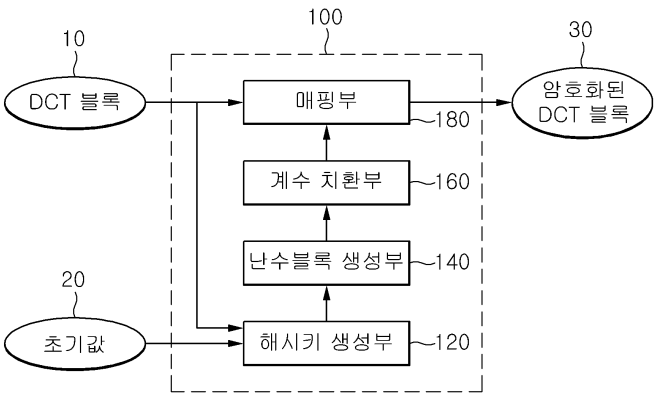
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치 및 방법**

(57) 요 약

본 발명은 디지털 콘텐츠에 대한 저작권 보호와 기밀성 유지를 위해 암호화에 사용되는 키 값과 데이터 암호화의 과정에 복수의 카오스 사상을 이용함으로써 디지털 콘텐츠에 대한 보안과 실시간 네트워크 환경에 용이하게 적용할 수 있는 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치 및 방법에 관한 것이다. 이를 위해, 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치는, 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상(Tent Map)을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성하는 해시키 생성부; 해시키 생성부에 의해 생성된 해시키 값으로부터 초기 의사난수 블록을 생성하는 난수 블록 생성부; 난수 블록 생성부에 의해 생성된 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 계수 치환부; 및 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수와 최종 의사난수 블록의 계수에 대한 매핑을 수행하여 디지털 콘텐츠 스트림에 대해 암호화된 DCT 블록을 출력하는 매핑부를 포함한다.

대 표 도 - 도1



(72) 발명자

장인수

인천광역시 서구 경서동 215-2 37블록 7루트 지원 드림파크 1동 401호

김창범

서울특별시 노원구 동일로227길 25, 주공11단지 1104동 906호 (상계동)

김덕환

서울특별시 양천구 목동로 230, 103동 1004호 (목동, 목동아이파크)

윤병춘

인천광역시 남구 인하로 100, 인하대학교 하이테크 센터 813호 (용현동)

이 발명을 지원한 국가연구개발사업

과제고유번호	10035169
부처명	지식경제부
연구사업명	인력양성사업
연구과제명	시스템반도체 융복합형 설계인재 양성사업
주관기관	한국전자통신연구원
연구기간	2006.03.01 ~ 2011.12.31

특허청구의 범위

청구항 1

디지털 콘텐츠 스트림에 대한 DCT(Discrete Cosine Transform) 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상(Tent Map)을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성하는 해시키 생성부;

상기 해시키 생성부에 의해 생성된 해시키 값으로부터 초기 의사난수 블록을 생성하는 난수 블록 생성부;

상기 난수 블록 생성부에 의해 생성된 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 계수 치환부; 및

상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수와 상기 최종 의사난수 블록의 계수에 대한 매핑을 수행하여 디지털 콘텐츠 스트림에 대해 암호화된 DCT 블록을 출력하는 매핑부를 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 2

청구항 1에 있어서,

상기 해시키 생성부는,

상기 해시 체인에 대해 비트 정규화된 입력값으로 사용하기 위해 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 선택하고, 선택된 계수들을 복수의 그룹으로 분할하는 계수 그룹 생성부를 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 3

청구항 2에 있어서,

상기 해시키 생성부는,

상기 해시 체인에 0 내지 1 사이의 실수값을 초기값으로 입력하고, 상기 계수 그룹 생성부에 의해 분할된 복수의 그룹의 각 그룹에 대하여 0 내지 1 사이의 실수값으로 정규화한 값을 입력하여 해시키 값을 생성하는 해시 체인부를 더 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 4

청구항 1에 있어서,

상기 난수 블록 생성부는 상기 해시키 생성부에 의해 생성된 해시키 값을 초기값으로 갖는 로지스틱 사상(Logistic Map)을 이용하여 초기 의사난수 블록을 생성하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 5

청구항 1에 있어서,

상기 계수 치환부는 상기 난수 블록 생성부에 의해 생성된 초기 의사난수 블록의 계수들을 헤논 사상(Henon Map)을 이용하여 치환함으로써 최종 의사난수 블록을 생성하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 6

청구항 1에 있어서,

상기 매핑부는 상기 디지털 콘텐츠 스트림에 대한 DCT 블록과 상기 최종 의사난수 블록으로부터 XOR 연산의 매핑을 이용하여 상기 암호화된 DCT 블록을 출력하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치.

청구항 7

디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성하는 단계;

상기 해시키 값으로부터 초기 의사난수 블록을 생성하는 단계;

상기 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 단계; 및

상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수와 상기 최종 의사난수 블록의 계수에 대한 매핑을 수행하여 상기 디지털 콘텐츠 스트림에 대해 암호화된 DCT 블록을 출력하는 단계를 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

청구항 8

청구항 7에 있어서,

상기 해시키 값을 생성하는 단계는,

상기 해시 체인에 대해 비트 정규화된 입력값으로 사용하기 위해 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 선택하고, 선택된 계수들을 복수의 그룹으로 분할하는 단계를 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

청구항 9

청구항 8에 있어서,

상기 해시키 값을 생성하는 단계는,

상기 해시 체인에 0 내지 1 사이의 실수값을 초기값으로 입력하고, 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 기초로 분할된 복수의 그룹의 각 그룹에 대하여 0 내지 1 사이의 실수값으로 정규화한 값을 입력하여 해시키 값을 생성하는 단계를 더 포함하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

청구항 10

청구항 7에 있어서,

상기 초기 의사난수 블록을 생성하는 단계는, 상기 해시키 값을 생성하는 단계에서 생성된 해시키 값을 초기값으로 갖는 로지스틱 사상을 이용하여 초기 의사난수 블록을 생성하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

청구항 11

청구항 7에 있어서,

상기 최종 의사난수 블록을 생성하는 단계는, 상기 초기 의사난수 블록을 생성하는 단계에서 생성된 초기 의사난수 블록의 계수들을 헤논 사상을 이용하여 치환함으로써 최종 의사난수 블록을 생성하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

청구항 12

청구항 7에 있어서,

상기 디지털 콘텐츠 스트림에 대한 암호화된 DCT 블록을 출력하는 단계는, 상기 디지털 콘텐츠 스트림에 대한 DCT 블록과 상기 최종 의사난수 블록으로부터 XOR 연산의 매핑을 이용하여 상기 암호화된 DCT 블록을 출력하는 것을 특징으로 하는, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치 및 방법에 관한 것으로, 보다 상세하게는 디지털 콘텐츠에 대한 저작권 보호와 기밀성 유지를 위해 암호화에 사용되는 키 값과 데이터 암호화의 과정에 복수의 카오스 사상을 이용함으로써 디지털 콘텐츠에 대한 보안과 실시간 네트워크 환경에 용이하게 적용할 수 있는 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 디지털 콘텐츠에 대한 기밀성을 유지하기 위해 멀티미디어 데이터는 본래의 데이터를 추측할 수 없는 형식으로 암호화되어야 하고, 인증된 사용자에게만 복호화의 권한이 주어져야 한다. 이를 위해, 직접적인 동영상 암호화 방법으로써 텍스트 데이터를 보호할 목적으로 사용되는 전통적 암호화 방법인 AES(Advance Encryption Standard)를 인코딩된 디지털 콘텐츠 스트림 전체에 적용하여 데이터를 암호화하는 naive algorithm이 제안되었다. 하지만 통상적으로 영상 데이터의 크기는 텍스트 데이터의 크기에 비해 매우 크기 때문에 AES 또는 DES(Data Encryption Standard)와 같은 텍스트 암호화 알고리즘을 영상 데이터의 암호화에 직접적으로 적용할 경우 실시간 처리에 적합하지 못할 뿐만 아니라, 암호화 처리 후의 동영상 데이터의 크기 및 시간 오버헤드의 측면에서 좋지 못한 성능을 나타내는 문제가 있다.

[0003] 한편, 디지털 콘텐츠의 보호를 위한 동영상 및 정지영상의 암호화하는 기법으로써, Shiguo Lian의 논문 'Efficient image or video encryption based on spatiotemporal chaos system'(Chaos, Solitons & Fractal, June. 2009, pp. 2509-2519)에서는 시공간 카오스 시스템 기반의 영상 암호 알고리즘을 제안하고 있다. 상기 논문에 개시된 카오스 사상을 이용한 암호화 기법은 디지털 콘텐츠 스트림에 대한 DCT 블록에서 선택된 매개변수를 암호화하는데, 2D CML(Coupled Map Lattice)를 목적에 맞게 변형하여 사용하여 의사난수 수열을 생성함으로써 디지털 콘텐츠에 대한 암호화를 수행하고 있다. 그러나, 상기와 같은 카오스 사상을 이용한 종래의 암호화 기법은 의사난수 수열을 생성하기 위한 초기 격자로써 128bit의 임의의 키 값을 사용하기 때문에 키 공간에 대한 난수 특성이 미흡할 수 있다는 문제가 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은, 복수의 카오스 사상을 이용하여 디지털 콘텐츠 스트림에 대한 암호화를 수행함으로써, 디지털 콘텐츠를 보호하기 위해 난수 특성이 우수하고, 보안성과 안정성이 뛰어난 암호화 기술을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0005] 상기한 목적을 달성하기 위한 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치는, 디지털 콘텐츠 스트림에 대한 DCT(Discrete Cosine Transform) 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상(Tent Map)을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성하는 해시키 생성부; 상기 해시키 생성부에 의해 생성된 해시키 값으로부터 초기 의사난수 블록을 생성하는 난수 블록 생성부; 상기 난수 블록 생성부에 의해 생성된 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 계수 치환부; 및 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수와 상기 최종 의사난수 블록의 계수에 대한 매핑을 수행하여 디지털 콘텐츠 스트림에 대해 암호화된 DCT 블록을 출력하는 매핑부를 포함하는 것을 특징으로 한다.

[0006] 이때, 해시키 생성부는 상기 해시 체인에 대해 비트 정규화된 입력값으로 사용하기 위해 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 선택하고, 선택된 계수들을 복수의 그룹으로 분할하는 계수 그룹 생성부를 포함할 수 있다.

[0007] 이때, 해시키 생성부는 상기 해시 체인에 0 내지 1 사이의 실수값을 초기값으로 입력하고, 상기 계수 그룹 생성부에 의해 분할된 복수의 그룹의 각 그룹에 대하여 0 내지 1 사이의 실수값으로 정규화한 값을 입력하여 해시키 값을 생성하는 해시 체인부를 포함할 수 있다.

[0008] 이때, 난수 블록 생성부는 상기 해시키 생성부에 의해 생성된 해시키 값을 초기값으로 갖는 로지스틱 사상(Logistic Map)을 이용하여 초기 의사난수 블록을 생성할 수 있다.

[0009] 이때, 계수 치환부는 상기 난수 블록 생성부에 의해 생성된 초기 의사난수 블록의 계수들을 헤논 사상(Henon Map)을 이용하여 치환함으로써 최종 의사난수 블록을 생성할 수 있다.

[0010] 이때, 매핑부는 상기 디지털 콘텐츠 스트림에 대한 DCT 블록과 상기 최종 의사난수 블록으로부터 XOR 연산의 매핑을 이용하여 상기 암호화된 DCT 블록을 출력할 수 있다.

[0011] 또한, 상기한 목적을 달성하기 위한 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법은, 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성하는 단계; 상기 해시키 값으로부터 초기 의사난수 블록을 생성하는 단계; 상기 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 단계; 및 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수와 상기 최종 의사난수 블록의 계수에 대한 매핑을 수행하여 상기 디지털 콘텐츠 스트림에 대해 암호화된 DCT 블록을 출력하는 단계를 포함하는 것을 특징으로 한다.

[0012] 이때, 해시키 값을 생성하는 단계는, 상기 해시 체인에 대해 비트 정규화된 입력값으로 사용하기 위해 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 선택하고, 선택된 계수들을 복수의 그룹으로 분할하는 단계를 포함할 수 있다.

[0013] 이때, 해시키 값을 생성하는 단계는, 상기 해시 체인에 0 내지 1 사이의 실수값을 초기값으로 입력하고, 상기 디지털 콘텐츠 스트림에 대한 DCT 블록의 계수들을 기초로 분할된 복수의 그룹의 각 그룹에 대하여 0 내지 1 사이의 실수값으로 정규화한 값을 입력하여 해시키 값을 생성하는 단계를 포함할 수 있다.

[0014] 이때, 초기 의사난수 블록을 생성하는 단계에서, 상기 해시키 값을 생성하는 단계에서 생성된 해시키 값을 초기값으로 갖는 로지스틱 사상을 이용하여 초기 의사난수 블록을 생성할 수 있다.

[0015] 이때, 최종 의사난수 블록을 생성하는 단계에서, 상기 초기 의사난수 블록을 생성하는 단계에서 생성된 초기 의사난수 블록의 계수들을 혼돈 사상을 이용하여 치환함으로써 최종 의사난수 블록을 생성할 수 있다.

[0016] 이때, 디지털 콘텐츠 스트림에 대한 암호화된 DCT 블록을 출력하는 단계에서, 상기 디지털 콘텐츠 스트림에 대한 DCT 블록과 상기 최종 의사난수 블록으로부터 XOR 연산의 매핑을 이용하여 상기 암호화된 DCT 블록을 출력할 수 있다.

발명의 효과

[0017] 본 발명에 따르면, 멀티미디어 기술과 유무선 통신기술에 발달에 따라 디지털 저작권과 기밀성 유지가 중요시되는 디지털 콘텐츠에 대하여 카오스 사상(Chaos map)을 이용한 암호화 방법을 적용함으로써 암호화 시스템의 안전성을 향상시킬 수 있을 뿐만 아니라, 개방형 네트워크 환경에서 실시간성 및 콘텐츠의 보안성을 확보할 수 있는 효과가 있다.

[0018] 또한, 본 발명에 따르면, MPEG2 동영상 인코딩 과정 내에 암호화 알고리즘을 결합함으로써 암호화에 따른 시간적 손실과 데이터 크기 손실에 대해 효과적으로 대응할 수 있는 효과가 있다.

[0019] 또한 본 발명에 따르면, 난수 특성이 우수한 카오스 사상을 조합하여 암호화를 위한 초기 값을 생성함으로써, 이를 기반으로 1차원 및 2차원 카오스 사상의 연쇄작용에 따른 암호화의 안전성을 확보할 수 있는 효과가 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치의 구성을 나타내는 도면이다.

도 2는 도 1에 도시된 해시키 생성부의 구성을 나타내는 도면이다.

도 3은 도 2에 도시된 계수 그룹 생성부에서 해시 체인의 입력으로 사용하기 위한 DCT 블록의 계수들을 선택하고 그룹화하는 동작을 설명하기 위한 도면이다.

도 4는 도 2에 도시된 해시 체인부에서 해시 체인을 이용하여 해시키 값을 생성하는 동작을 설명하기 위한 도면이다.

도 5는 도 1에 도시된 난수블록 생성부에서 초기 난수블록을 생성하는 동작을 설명하기 위한 도면이다.

도 6은 도 1에 도시된 매핑부에서 암호화된 DCT 블록을 출력하는 동작을 설명하기 위한 도면이다.

도 7 및 도 8은 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법을 설명하

기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0022] 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 시스템은 동영상 인코더 내에서 구현될 수 있는데, 동영상 스트림의 암호화에 사용되는 2^{128} 크기의 공간을 갖는 키 값은 텐트 사상(Tent Map)을 기본블록으로 갖는 해시 체인에 의해 배포된다. 해시 체인에 의해 생성된 128bit 키는 8개의 16bit 보조키(Sub-key)로 분할되고, 1차원 카오스 사상인 로지스틱 사상(Logistic Map)의 초기 값으로 사용되어 8x8 크기의 초기 의사난수 블록이 생성되며, 생성된 초기 의사난수 블록은 2차원 카오스 사상인 헤논 사상(Henon Map)을 기반으로 블록 내 의사난수들의 위치에 대한 치환 과정이 수행됨으로써, 최종 의사난수 블록이 생성된다. 최종적으로 생성된 의사난수 블록은 동영상의 본래 DCT 블록과 XOR 연산을 통해 원본 신호에 대한 암호화 과정이 이루어지게 된다.

[0023] 도 1은 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치의 구성을 나타내는 도면이다.

[0024] 도 1을 참조하면, 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치(100)는, 디지털 콘텐츠 스트림에 대한 DCT 블록(10)으로부터 해시키(Hash-key)를 생성하는 해시키 생성부(120), 상기 해시키로부터 초기 의사난수 블록을 생성하는 난수블록 생성부(140), 상기 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성하는 계수 치환부(160) 및 상기 최종 의사난수 블록과 디지털 콘텐츠 스트림에 대한 DCT 블록간의 XOR 매핑을 통해 암호화된 DCT 블록(30)을 출력하는 매핑부(180)로 구성된다.

[0025] 해시키 생성부(120)는, 인코더 내부에서 디지털 콘텐츠 스트림에 대한 이산 코사인 변환(DCT: Discrete Cosine Transform) 과정에 의해 생성된 8x8 DCT 블록의 계수들에 대하여 비트 정규화된 값을 텐트 사상을 기본블록으로 갖는 해시 체인에 입력하여 해시키 값을 생성한다.

[0026] 해시키 생성부(120)는, 도 2를 참조하면, 디지털 콘텐츠 스트림에 대한 8x8 DCT 블록(10)을 입력받아 해시 체인의 입력값으로 이용하기 위한 계수들을 선택하고, 선택된 계수들을 복수의 그룹으로 분할하는 계수 그룹 생성부(122)와, 상기 계수 그룹 생성부(122)에 의해 분할된 계수들의 그룹과 초기값(20)을 텐트 사상을 기본블록으로 하는 해시 체인의 입력값으로 하여 해시키 값을 생성하는 해시 체인부(124)로 구성된다.

[0027] 계수 그룹 생성부(122)는 본 발명의 암호화 과정에 제공되는 해시키 값을 생성하기 위해 입력 데이터 선택의 전처리 과정을 수행한다. 도 3에 도시된 바와 같이, 인코더 내부에서 수행되는 DCT 과정에 따른 디지털 콘텐츠 스트림에 대한 8x8 DCT 블록(10)의 DC와 AC의 계수들은, 이후 해시 체인의 입력으로 사용되기 위해 연쇄적으로 선택되고, G_1(12), G_2(14), G_3(16) 및 G_4(18)의 4개의 그룹으로 분할된다.

[0028] 해시 체인부(124)는 상기 계수 그룹 생성부(122)에 의해 분할된 각 그룹을, 도 4에 도시된 바와 같이, 텐트 사상을 기본블록으로 갖는 해시 체인의 입력값으로 사용하여 해시키 값을 생성한다. 이때, 해시 체인부(124)는 상기 계수 그룹 생성부(122)에 의해 분할된 G_1(12), G_2(14), G_3(16) 및 G_4(18)의 4개의 그룹을 0 내지 1 사이의 실수값으로 비트 정규화하여, 각각 32bit 형식의 G_1'(12a), G_2'(14a), G_3'(16a) 및 G_4'(18a)의 4개의 그룹을 생성하고, 이를 해시 체인의 입력값으로 사용한다. 또한, 해시 체인부(124)는 해시 체인의 초기값 X_i(i = 0,1,2,3)인 X_0(22), X_1(24), X_2(26) 및 X_3(28)로써, 의사난수 발생기(PRNG: Pseudo Random Number Generator)(미도시)에 의해 생성된 0 내지 1 사이의 구간에 존재하는 값을 사용한다. 해시 체인부(124)의 해시 체인은 X_0(22), X_1(24), X_2(26) 및 X_3(28)의 초기값과 G_1'(12a), G_2'(14a), G_3'(16a) 및 G_4'(18a)의 입력값에 대하여, 각 기준블

록의 텐트 사상을 반복적으로 연쇄하여 수행함으로써, 다음의 수학식 1 및 2를 통해 기준블록의 입력인 α값과 x_{ij}값을 갱신한다.

수학식 1

[0029] $$\alpha = (x_{0j} + X_j) \bmod 1; i = 0; j = 0,1,2,3$$

수학식 2

[0030] $$\alpha = (x_{(i+1)j} + x_{i(j+1)}) \bmod 1; i = 0,1,2; j = 0,1,2,3$$

[0031] 그리고, 해시 체인의 모든 기준블록에서의 처리 과정 후, 해시 체인의 최종 출력값 x_{04}, x_{14}, x_{24} 및 x_{34}는 각각 $0.(b_0b_1b_2b_3\cdots b_{28}b_{29}b_{30}b_{31})$, $b_i \in \{0,1\}$의 2진 형태로 32bit씩 추출된다. 최종 출력값 x_{04}, x_{14}, x_{24} 및 x_{34}로부터 추출된 4개의 32bit의 2진 수열은 각각 h_0, h_1, h_2, h_3으로 정의되고, 그로부터 $h=(h_0, h_1, h_2, h_3)$인 128bit 해시키(40) 값이 생성된다.

[0032] 난수블록 생성부(140)는 해시키 생성부(120)에 의해 생성된 해시키 값으로부터 초기 의사난수 블록을 생성한다. 이때, 난수블록 생성부(140)는 해시키 생성부(120)에 의해 생성된 128bit 해시키 값을 로지스틱 사상(Logistic Map)의 초기값으로 사용하여 8x8 크기의 초기 의사난수 블록을 생성한다.

[0033] 먼저, 난수블록 생성부(140)는 128bit 해시키 $h=(h_0, h_1, h_2, h_3)$를 이용하여, 다음의 수학식 3에 의해 보조키(Sub-key)를 생성한다.

수학식 3

[0034] $$K_i = \frac{h_{16i}h_{16i+1}h_{16i+2}\cdots h_{16i+15}}{2^{16}}; i = 01,2,\cdots,7$$

[0035] 보조키 K_i(i=0,1,2,7)는 암호화에 사용되는 의사난수 블록을 생성하는데 사용된다. 이때, 다음의 수학식 4 및 5에 의해, 도 5에 도시된 바와 같이 격자 초기값 $R_i(r_{i0}, r_{i1}, r_{i2}, \cdots, r_{i7})$을 갖는 8x8의 초기 의사난수 블록이 생성된다. 여기서, 수학식 5의 로지스틱 사상은 혼돈 시스템을 수식적으로 표현하여 분석하는 방법으로 널리 사용되고 있으므로, 이에 대한 자세한 설명은 생략하기로 한다.

수학식 4

[0036] $$r_{ij} = f^{i_0+j}(K_i); j = 0,1,2,\cdots,7$$

수학식 5

[0037] $$f(x) = \mu x(1-x)$$

[0038] 계수 치환부(160)는 난수블록 생성부(140)에 의해 생성된 초기 의사난수 블록의 계수들을 치환하여 최종 의사난수 블록을 생성한다. 이때, 계수 치환부(160)는 난수블록 생성부(140)에 의해 생성된 초기 의사난수 블록의 계수들의 위치를 헤논 사상(Henon Map)을 이용하여 치환함으로써 최종 의사난수 블록을 생성한다.

[0039] 계수 치환부(160)는 난수블록 생성부(140)에 의해 생성된 초기 의사난수 블록의 계수들의 위치에 대하여 다음의 수학식 6 및 7로 표현되는 헤논 사상을 통해, 도 6에 도시된 바와 같은 최종 의사난수 블록(162)을 생성한다. 여기서, 수학식 6 및 7의 헤논 사상은 혼돈 시스템을 수식적으로 표현하여 분석하는 방법으로 널리 사용되고 있으므로, 이에 대한 자세한 설명은 생략하기로 한다.

수학식 6

[0040] $$x_{n+1} = y_n + 1 - ax_n^2$$

수학식 7

[0041] $$y_{n+1} = bx_n$$

[0042] 매핑부(180)는, 도 6에 도시된 바와 같이, 인코더 내부에서 디지털 콘텐츠 스트림에 대한 이산 코사인 변환 과정에 의해 생성된 8x8 DCT 블록(10a)의 각 계수와 그에 대응되는 최종 의사난수 블록(162)의 각 계수에 대하여, 다음의 수학식 8을 따르는 XOR 연산을 수행하는 매핑 과정을 통해 디지털 콘텐츠 스트림에 대한 암호화된 DCT 블록을 출력한다.

수학식 8

[0043] $$c_{ij} = q_{ij} \oplus r_{ij}; i, j = 0,1,2,\ldots,7$$

[0044] 이때, 계수 치환부(160)에 의해 생성된 최종 의사난수 블록(162)은 0 내지 1 사이의 실수값을 갖기 때문에 XOR 매핑에 앞서, $0.(b_0b_1b_2b_3\ldots b_{12}b_{13}b_{14}b_{15})$, $b_i \in \{0,1\}$ 형태의 부호가 있는 16bit 정수 형태로 변환 과정이 선행된다. 한편, 암호화된 디지털 콘텐츠 스트림에 대한 DCT 블록에 대한 복호화 과정은, 다음의 수학식 9에 의해, 암호화된 계수들에 대하여 XOR 연산이 대칭적으로 수행된다.

수학식 9

[0045] $$q_{ij} = c_{ij} \oplus r_{ij}; i, j = 0,1,2,\ldots,7$$

[0046] 암호화 과정에서의 오버헤드를 줄이기 위해, 본 발명에서는 매핑부(180)에 의한 XOR 매핑 과정을 DCT 블록(10a) 전체에 대하여 수행하는 것이 아닌 DCT 블록(10a)에서 실질적으로 많은 정보를 갖는 7~8개의 유효계수들에 대해서만 선택적으로 수행하거나, 또는 I-프레임에 대한 DCT 블록들로 한정해서 암호화를 수행함으로써, 최종적으로

암호화된 디지털 콘텐츠 스트림을 출력할 수 있도록 구성될 수 있다.

[0047] 이하에서는 도 7 및 도 8을 참조하여, 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법에 대하여 설명하도록 한다. 앞서, 도 1 내지 6을 참조한 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 장치의 동작에 대한 설명과 일부 중복되는 부분은 생략하여 설명하기로 한다.

[0048] 도 7은 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법을 설명하기 위한 흐름도이다.

[0049] 도 7을 참조하면, 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법은, 먼저 인코더 내부에서 이산 코사인 변환 과정에 의해 생성된 디지털 콘텐츠 스트림에 대한 8x8 DCT 블록과 해시키 생성부(120)의 해시 체인에 대한 초기값을 입력받는다(S100).

[0050] 그리고, 해시키 생성부(120)는 상기 디지털 콘텐츠 스트림에 대한 8x8 DCT 블록의 계수들에 대해 비트 정규화된 값을 텐트 사상을 기본블록으로 하는 해시 체인에 입력하여 128bit의 해시키를 생성한다(S200).

[0051] 그 다음으로, 난수블록 생성부(140)는 해시키 생성부(120)에 의해 생성된 해시키 값을 로지스틱 사상의 초기값으로 사용하여 초기 의사난수 블록을 생성한다(S300).

[0052] 그리고, 계수 치환부(160)는 난수블록 생성부(140)에 의해 생성된 초기 의사난수 블록의 계수들의 위치를 혜논 사상을 이용하여 치환함으로써 최종 의사난수 블록을 생성한다(S400).

[0053] 그 다음으로, 매핑부(180)는 디지털 콘텐츠 스트림에 대한 DCT 블록의 각 계수와 그에 대응되는 최종 의사난수 블록의 각 계수에 대하여 XOR 연산의 매핑을 수행하고(S500), 최종적으로 암호화된 디지털 콘텐츠 스트림에 대한 DCT 블록을 출력한다(600).

[0054] 도 8은 도 7에 도시된 S200 단계를 보다 구체적으로 설명하기 위한 흐름도이다.

[0055] 도 8을 참조하면, 본 발명에 따른 카오스 사상을 기반으로 디지털 콘텐츠를 보호하기 위한 암호화 방법에서 128bit의 해시키를 생성하기 위한 S200 단계는, 먼저 해시키 생성부(120)의 계수 그룹 생성부(122)가 디지털 콘텐츠 스트림에 대한 DCT 블록(10)을 입력받아 해시 체인의 입력값으로 이용하기 위한 계수들을 선택하고, 선택된 계수들을 각각 32bit의 4개의 그룹으로 분할한다(S210).

[0056] 그 다음으로, 해시 체인부(124)는 상기 S210 단계에서 분할된 4개의 그룹에 대하여 0 내지 1 사이의 실수값으로 비트 정규화하고(S220), DCT 블록의 계수들에 기초한 비트 정규화된 값을 텐트 사상을 기본블록으로 갖는 해시 체인으로 입력한다(S230). 이때, 상기 해시 체인의 초기값으로써 PRNG에 의해 생성된 0 내지 1 사이의 구간에 존재하는 값을 사용한다.

[0057] 그리고, 해시 체인부(124)는 해시 체인의 출력값에 대하여 각각 $0.(b_0b_1b_2b_3\cdots b_{28}b_{29}b_{30}b_{31})$, $b_i \in \{0,1\}$의 2진 형태를 갖는 4개의 32bit 수열을 추출하고(S240), 추출된 4개의 32bit의 2진 수열로부터 128bit의 해시키를 생성한다(S250).

[0058] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0059] 100: 암호화 장치

120: 해시키 생성부

122: 계수 그룹 생성부

124: 해시 체인부

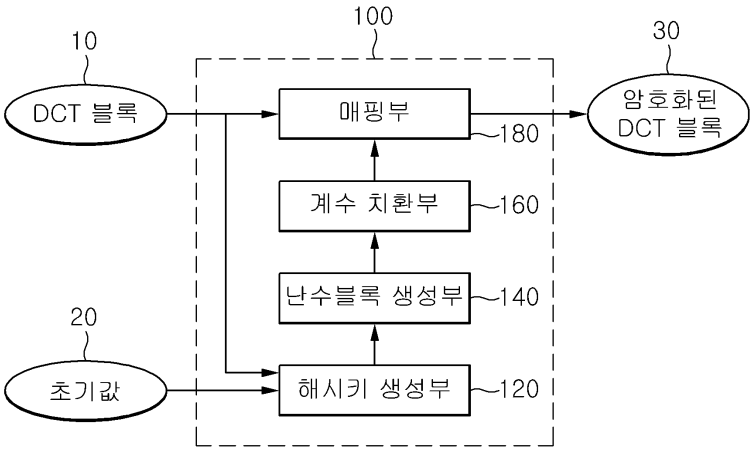
140: 난수블록 생성부

160: 계수 치환부

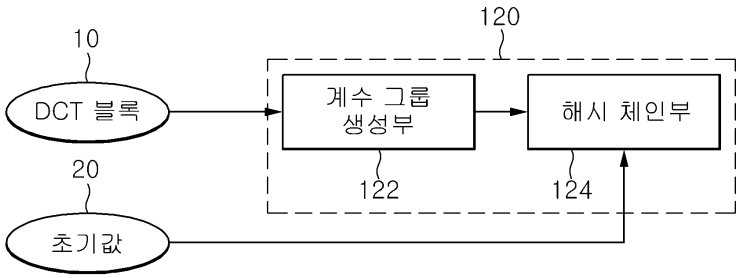
180: 매핑부

도면

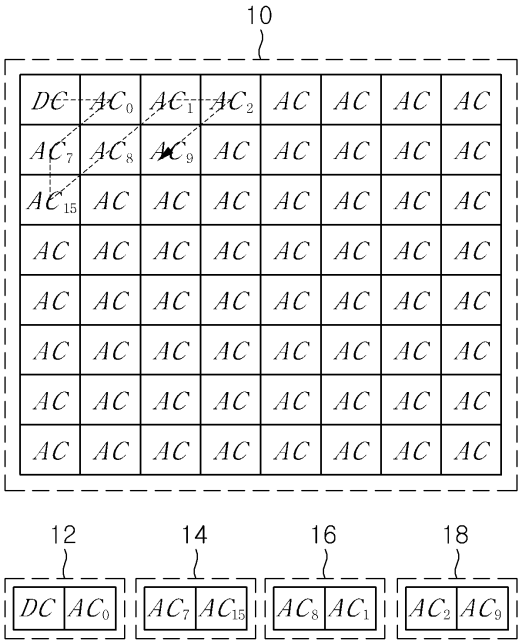
도면1



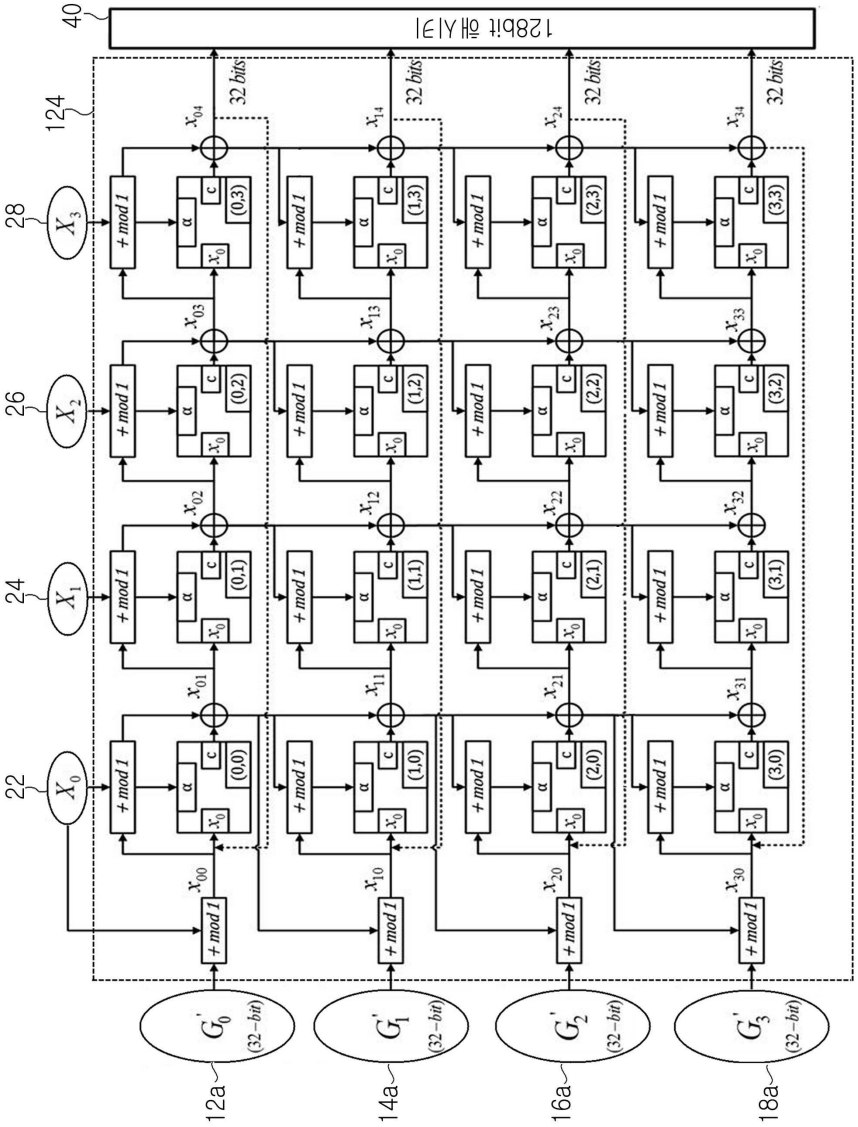
도면2



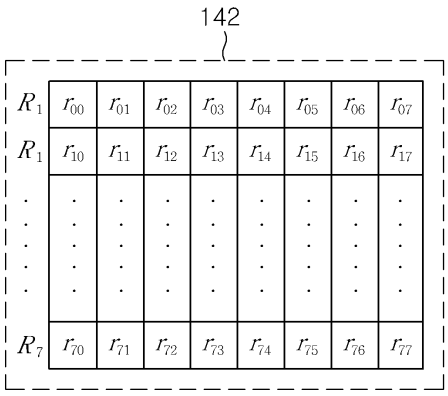
도면3


10
DC
AC0
AC1
AC2
AC7
AC8
AC9
AC15
AC
12
14
16
18
DC
AC0
AC7
AC15
AC8
AC1
AC2
AC9

도면4

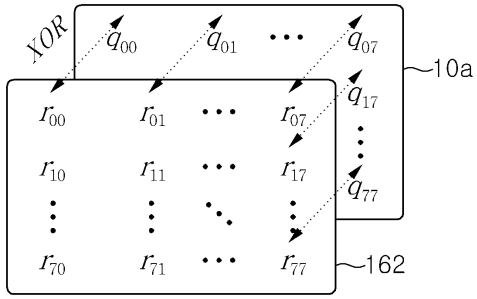


도면5

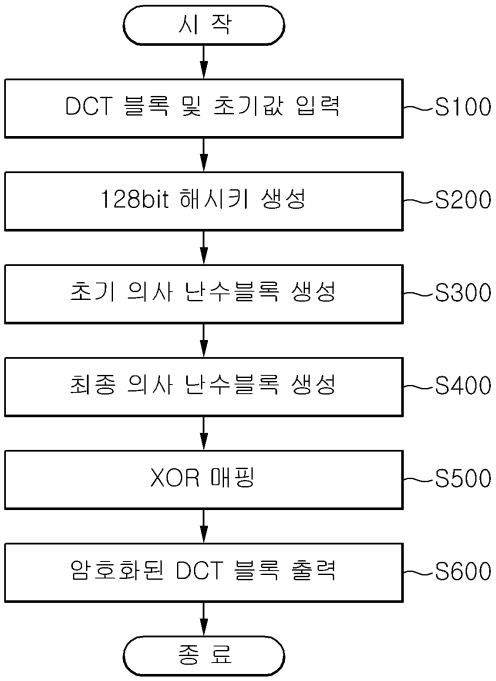


R_1	r_{00}	r_{01}	r_{02}	r_{03}	r_{04}	r_{05}	r_{06}	r_{07}
R_1	r_{10}	r_{11}	r_{12}	r_{13}	r_{14}	r_{15}	r_{16}	r_{17}
. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .
R_7	r_{70}	r_{71}	r_{72}	r_{73}	r_{74}	r_{75}	r_{76}	r_{77}

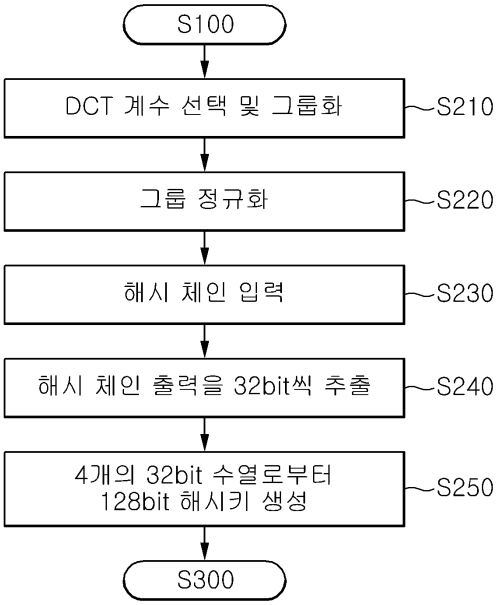
도면6


XOR
q_{00}
q_{01}
q_{07}
q_{17}
q_{77}
10a
r_{00}
r_{01}
r_{07}
r_{10}
r_{11}
r_{17}
r_{70}
r_{71}
r_{77}
162

도면7


시 작
DCT 블록 및 초기값 입력
S100
128bit 해시키 생성
S200
초기 의사 난수블록 생성
S300
최종 의사 난수블록 생성
S400
XOR 매핑
S500
암호화된 DCT 블록 출력
S600
종 료

도면8


S100
DCT 계수 선택 및 그룹화
S210
그룹 정규화
S220
해시 체인 입력
S230
해시 체인 출력을 32bit씩 추출
S240
4개의 32bit 수열로부터
128bit 해시키 생성
S250
S300