(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년07월28일
(11) 등록번호 10-0848642
(24) 등록일자 2008년07월21일

(51) Int. Cl.
H04N 7/167 (2006.01) *H04N 7/16* (2006.01)
(21) 출원번호 10-2007-0017966
(22) 출원일자 2007년02월22일
심사청구일자 2007년02월22일
(56) 선행기술조사문헌
JP10013828 A*
KR1020060003330 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
이희조

추의진

(뒷면에 계속)

(74) 대리인
유미특허법인

전체 청구항 수 : 총 11 항 심사관 : 김영태

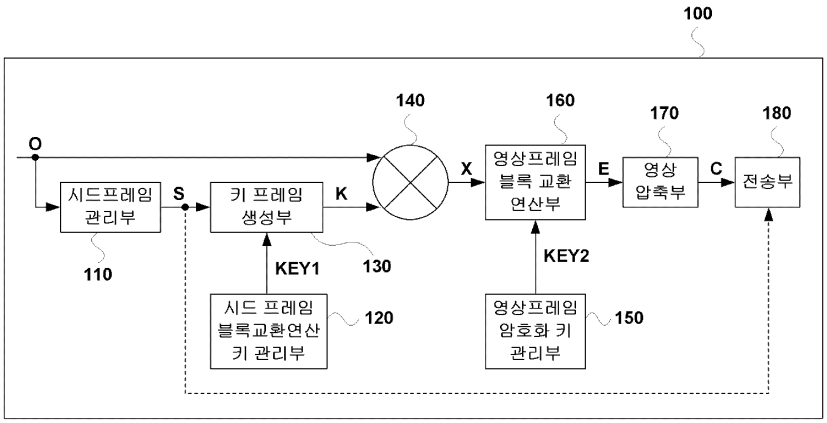
(54) 영상 프레임을 암호화하는 방법과 복원하는 방법

(57) 요 약

영상 프레임을 암호화하는 장치는 키 프레임을 생성하고, 영상 프레임과 키 프레임을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임을 생성하며, 임시 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 암호화된 영상 프레임을 생성한다.

영상 프레임을 복원하는 장치는 암호화된 영상 프레임을 수신하고, 키 프레임을 생성하고, 암호화된 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 임시 영상 프레임을 생성하며, 임시 영상 프레임과 키 프레임을 가지고 배타적 논리합 연산을 수행하여 영상 프레임을 생성한다.

대표도



(72) 발명자 **남기원**

이제현

특허청구의 범위

청구항 1

삭제

청구항 2

영상 프레임을 암호화하는 방법에 있어서,

키 프레임을 생성하는 단계;

상기 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임을 생성하는 단계;

상기 임시 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 암호화된 영상 프레임을 생성하는 단계를 포함하고

상기 키 프레임을 생성하는 단계는

시드 프레임을 생성하는 단계와,

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 3

제2항에 있어서,

상기 시드 프레임을 생성하는 단계는

상기 영상 프레임에서 최소 존재 확률을 가지는 하나 이상의 색상 값으로 상기 시드 프레임을 생성하는 단계를 포함하는 방법.

청구항 4

제3항에 있어서,

상기 키 프레임을 생성하는 단계는

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 반복적으로 변경하여 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 5

제3항에 있어서,

상기 키 프레임을 생성하는 단계는

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 재귀적으로 변경하여 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 6

제2항 내지 제5항 중 어느 한 항에 있어서,

상기 암호화된 영상 프레임의 각 블록 내의 중복된 색상 값을 제거하여 압축된 프레임을 생성하는 단계를 더 포함하는 방법.

청구항 7

삭제

청구항 8

영상 프레임을 암호화하는 방법에 있어서,

키 프레임을 생성하는 단계;

상기 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 임시 영상 프레임을 생성하는 단계; 및

상기 키 프레임과 상기 임시 영상 프레임을 가지고 배타적 논리합 연산을 수행하여 암호화된 영상 프레임을 생성하는 단계를 포함하고

상기 키 프레임을 생성하는 단계는

시드 프레임을 생성하는 단계와,

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 시드 프레임을 생성하는 단계는

상기 영상 프레임에서 최소 존재 확률을 가지는 하나 이상의 색상 값으로 상기 시드 프레임을 생성하는 단계를 포함하는 방법.

청구항 10

삭제

청구항 11

영상 프레임을 복원하는 방법에 있어서,

암호화된 영상 프레임을 수신하는 단계;

키 프레임을 생성하는 단계;

상기 암호화된 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 임시 영상 프레임을 생성하는 단계; 및

상기 임시 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 상기 영상 프레임을 생성하는 단계를 포함하고

상기 키 프레임을 생성하는 단계는,

시드 프레임을 수신하는 단계와,

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 12

제11항에 있어서,

상기 암호화된 영상 프레임을 수신하는 단계는,

압축된 영상 프레임을 수신하는 단계와,

상기 압축된 영상 프레임의 압축을 해제하여 상기 암호화된 영상 프레임을 생성하는 단계를 포함하는 방법.

청구항 13

삭제

청구항 14

영상 프레임을 복원하는 방법에 있어서,

암호화된 영상 프레임을 수신하는 단계;

키 프레임을 생성하는 단계;

상기 암호화된 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임을 생성하는 단계; 및

상기 임시 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 상기 영상 프레임을 생성하는 단계를 포함하고

상기 키 프레임을 생성하는 단계는,

시드 프레임을 수신하는 단계와,

상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성하는 단계를 포함하는 방법.

청구항 15

제14항에 있어서,

상기 암호화된 영상 프레임을 수신하는 단계는,

압축된 영상 프레임을 수신하는 단계와,

상기 압축된 영상 프레임의 압축을 해제하여 상기 암호화된 영상 프레임을 생성하는 단계를 포함하는 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<13> 본 발명은 영상 프레임을 암호화하는 방법과 복원하는 방법에 관한 것이다. 특히, 본 발명은 실시간으로 안전하게 멀티미디어를 전송하기 위하여 영상 프레임을 암호화하는 방법과 복원하는 방법에 관한 것이다.

<14> 멀티미디어는 문자, 음성, 도형, 영상 등으로 이루어진 복합 정보를 보관하거나 전송하기 위하여 사용되는 정보매체로, 디지털화하여 저장하는데 많은 공간을 필요로 하며, 가공이 까다롭고 전송에 많은 대역폭을 소모한다. 또한 멀티미디어는 서로 다른 형태의 정보의 집합체이기 때문에 전체 정보 중 일부로부터 나머지 부분을 유추하는 것이 용이하고, 생성과정 중 매체에 포함되는 정보의 양과 경중을 직관적으로 인식하기 어렵다.

<15> 멀티미디어 전송은 그 처리량의 방대함과 내포된 정보의 양과 중요도를 가늠하거나 정량적으로 측정하기 어렵다는 이유로 문자나 음성에 비해 인가되지 않은 접근이나 훼손으로부터의 안전장치나 보안체계가 갖춰지지 않은 채 통용되고 있다. 이로 인해 개인 정보, 보안 정보 등 기밀 정보의 유출, 가치 상실로 인한 금전적 손실, 사생활 침해와 같은 피해가 발생하였다. 이에 따라 보관 또는 전송중인 멀티미디어의 기밀성 또는 배타성을 인가되지 않은 열람, 변형, 복제에 의한 가치 상실, 왜곡, 누출로부터 보호하기 위하여 보관 또는 전송 과정 중에 암호화하는 것이 중요하다.

<16> 대용량의 멀티미디어 자료는 저장 공간의 절약과 전송 효율을 위해 영상의 지역성에 기초하여 압축될 수 있는데, 압축 기법에 따라 독특한 구조적 특성을 가지게 된다.

<17> 화상 대화, 감시 카메라, 중계방송과 같이 일반적으로 실시간에 전송할 필요성이 있는 경우 MPEG4(Moving Picture Experts Group 4) 압축 방식이 사용된다. MPEG4 압축 방식은 영상을 구역 분할하여 구역 내 색상 값의 중복을 제거하는 방법과 근접 시간 내의 영상 간의 중복을 참조명시로 대체하는 방법을 혼합하여 사용한다.

<18> 현재 멀티미디어를 암호화 하는 방식들은 멀티미디어 정보를 압축하기 전 암호화하는 방식과 압축이 완료 된 후 별도의 암호화 단계를 거치는 방법이 사용되고 있다. 압축 후 암호화 기법은 시간 복잡도가 큰 기법을 사용하게

되어 자료가 고품질 대용량화 되어가는 현재의 추세에서 그 효용성이 떨어진다.

<19> 압축 전 암호화하는 방법으로는 나이브 알고리즘(Naive Algorithm)과 선택적 암호화 방식(Selective Algorithm)이 있다.

<20> 나이브 알고리즘에 따르면, 멀티미디어의 구조적 특성을 무시하고 문자 자료를 암호화하는 것처럼 압축되지 않은 멀티미디어 자료 전체를 암호화한다. 나이브 알고리즘에 따르면, 방대한 양의 멀티미디어 자료 전체를 암호화하기 때문에 암호화에 많은 시간과 자원이 소모되는 문제가 발생한다. 또한, 멀티미디어의 구조적인 특성을 깨뜨려 압축률을 떨어뜨린다.

<21> 이에 반하여 선택적 암호화 방식에 따르면, 멀티미디어 고유의 구조적 특성을 고려하여 선택적인 부분만을 암호화함으로써 암호화 효율이 증대되지만, 멀티미디어 전체가 암호화되지 않으므로 멀티미디어의 일부가 노출될 수 있는 문제가 있다.

발명이 이루고자 하는 기술적 과제

<22> 본 발명이 이루고자 하는 기술적 과제는 멀티미디어를 압축하기 이전에 암호화하더라도 시간과 자원을 절약하며 압축률을 크게 저하시키지 않는 암호화 방법을 제공하는 것이다.

발명의 구성 및 작용

<23> 본 발명의 한 실시예에 따라 영상 프레임을 암호화하는 장치는 키 프레임을 생성하고, 상기 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임을 생성하며, 상기 임시 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 암호화된 영상 프레임을 생성한다.

<24> 이때, 영상 프레임을 암호화하는 장치는 시드 프레임을 생성하고, 상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성할 수 있다.

<25> 또한 이때, 영상 프레임을 암호화하는 장치는 상기 영상 프레임에서 최소 존재 확률을 가지는 하나 이상의 색상 값으로 상기 시드 프레임을 구성하는 색상 값을 결정하여 상기 시드 프레임을 생성할 수 있다.

<26> 본 발명의 다른 실시예에 따라 영상 프레임을 암호화하는 장치는 키 프레임을 생성하고, 상기 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 임시 영상 프레임을 생성하며, 상기 키 프레임과 상기 임시 영상 프레임을 가지고 배타적 논리합 연산을 수행하여 암호화된 영상 프레임을 생성한다.

<27> 본 발명의 한 실시예에 따라 영상 프레임을 복원하는 장치는 암호화된 영상 프레임을 수신하고, 키 프레임을 생성하고, 상기 암호화된 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 임시 영상 프레임을 생성하며, 상기 임시 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 상기 영상 프레임을 생성한다.

<28> 이때, 영상 프레임을 복원하는 장치는 시드 프레임을 생성하고, 상기 시드 프레임의 각 블록의 위치를 제2 키에 따라 변경하여 상기 키 프레임을 생성할 수 있다.

<29> 또한 이때, 영상 프레임을 복원하는 장치는 압축된 영상 프레임을 수신하고, 상기 압축된 영상 프레임의 압축을 해제하여 상기 암호화된 영상 프레임을 생성할 수 있다.

<30> 본 발명의 다른 실시예에 따라 영상 프레임을 복원하는 장치는 암호화된 영상 프레임을 수신하고, 키 프레임을 생성하고, 상기 암호화된 영상 프레임과 상기 키 프레임을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임을 생성하며, 상기 임시 영상 프레임의 각 블록의 위치를 제1 키에 따라 변경하여 상기 영상 프레임을 생성한다.

<31> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<32> 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. 또한, 명세서에 기재

된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

<33> 동영상은 여러 장의 정지 영상을 빠르게 전환하여 구현된다. 본 명세서에서는 동화상의 단위 정지 영상 또는 보통의 정지 영상을 프레임이라 한다. 한편, 프레임은 일정한 크기의 정사각형의 조각으로 논리적으로 분리될 수 있는데, 이 정사각형의 조각을 매크로 블록(macro block) 또는 간단히 블록이라 하도록 한다. 즉, 프레임은 복수의 블록으로 구성된다.

<34> 다음은 도 1과 도 2를 참조하여 본 발명의 제1 실시예에 따른 영상 암호화 방법을 설명한다.

<35> 도 1은 본 발명의 제1 실시예에 따른 영상 암호화 장치를 개략적으로 도시한 블록도이다.

<36> 도 1에 도시된 바와 같이, 본 발명의 제1 실시예에 따른 영상 암호화 장치(100)는 시드 프레임 관리부(110), 시드 프레임 블록 교환 연산 키 관리부(120), 키 프레임 생성부(130), 배타적 논리합 연산부(140), 영상 프레임 암호화 키 관리부(150), 영상 프레임 블록 교환 연산부(160), 영상 압축부(170), 및 전송부(180)를 포함한다.

<37> 시드 프레임 관리부(110)는 시드 프레임(S)의 생성, 재사용, 폐기 등의 관리를 수행한다. 시드 프레임 관리부(110)는 영상 프레임(O)를 기초로 시드 프레임(S)를 생성할 수 있다.

<38> 시드 프레임 블록 교환 연산 키 관리부(120)는 키 프레임 생성부(130)가 블록 교환 연산에 사용하는 시드 프레임 블록 교환 연산 키(KEY1)를 생성, 재사용, 폐기하는 등의 관리를 수행한다.

<39> 키 프레임 생성부(130)는 시드 프레임(S)에 대하여 시드 프레임 블록 교환 연산 키(KEY1)를 사용하여 블록 교환 연산을 수행하여 키 프레임(K)을 생성한다.

<40> 배타적 논리합 연산부(140)는 영상 프레임(O)과 키 프레임(K)을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임(X)을 생성한다.

<41> 영상 프레임 암호화 키 관리부(150)는 영상 프레임 블록 교환 연산부(160)가 블록 교환 연산에 사용하는 영상 프레임 암호화 키(KEY2)를 생성, 재사용, 폐기하는 등의 관리를 수행한다.

<42> 영상 프레임 블록 교환 연산부(160)는 임시 영상 프레임(X)에 대하여 영상 프레임 암호화 키(KEY2)를 사용하여 블록 교환 연산을 수행하여 암호화된 영상 프레임(E)을 생성한다.

<43> 영상 압축부(170)는 암호화된 영상 프레임(E)을 압축하여 압축된 영상 프레임(C)를 생성한다.

<44> 전송부(180)는 압축된 영상 프레임(C)을 채널에 전송한다. 또한, 전송부(180)는 주기적으로 시드 프레임(S) 또는 압축된 시드 프레임(S)을 채널에 전송할 수 있다.

<45> 도 2는 본 발명의 제1 실시예에 따른 영상 암호화 방법을 개략적으로 도시한 흐름도이다.

<46> 먼저, 시드 프레임 관리부(110)는 시드 프레임(S)의 생성, 재사용, 폐기 여부를 결정한다(S110). 이때, 시드 프레임 관리부(110)는 암호화하고자 하는 하나 이상의 영상 프레임(O)을 분석하여 영상 암호화의 시드가 되는 시드 프레임(S)을 생성할 수 있다(S110). 또한 이때, 시드 프레임 관리부(110)는 하나 이상의 영상 프레임(O)을 구성하는 색상 값의 통계적 분포를 분석하여 최소 존재 확률을 가지는 하나 이상의 색상 값으로 시드 프레임(S)을 구성하는 색상 값을 결정할 수 있다. 즉, 시드 프레임 관리부(110)는 암호화하고자 하는 하나 이상의 영상 프레임(O)에 잘 나타나지 않는 색상 값 또는 이와 유사한 색상 값으로 시드 프레임(S)을 생성한다. 예를 들어, 시드 프레임 관리부(110)는 영상 프레임(O)에 잘 나타나지 않는 원색에 가까운 RGB 색상들, 즉 (253,253,0), (253,0,253), (0,253,253) 등으로 시드 프레임(S)를 생성할 수 있다. 이로써 배타적 논리합 연산부(140)의 결과 프레임의 압축률이 저하되는 것을 막을 수 있다. 왜냐 하면, 시드 프레임을 구성하는 색상 값을 암호화하고자 하는 하나 이상의 영상 프레임(O)에 통상적으로 나타나는 색상 값으로 결정하는 경우, 배타적 논리합 연산부(140)의 출력 프레임의 각 블록의 픽셀들은 서로 큰 차이를 갖는 색상 값을 갖게 된다. 즉, 각 블록 내의 값들이 그 유사성을 잃기 때문에 프레임 내의 중복된 색상 값을 제거하는 압축 방식에 따른다면 압축률이 크게 저하된다.

<47> 예를 들어 영상 프레임(O)이 RGB 형식으로 디지털화된 프레임인 경우를 가정한다. 영상 프레임(O)이 $64_{(16)}$과 $C8_{(16)}$ 사이의 색상 값을 주로 포함하고 $FF_{(16)}$를 드물게 포함하고 있다면 시드 프레임 관리부(110)는 $FF_{(16)}$에 가까운 색상 값(예를 들어 $FA_{(16)}$과 $FF_{(16)}$사이의 색상 값)을 시드 프레임(S)의 생성에 이용할 수 있다.

<48> 키 프레임 생성부(130)는 시드 프레임 관리부(110)로부터의 시드 프레임(S)에 대하여 시드 프레임 블록 교환 연산 키(KEY1)를 사용하여 블록 교환 연산을 수행하여 키 프레임(K)을 생성한다(S120). 키 프레임 생성부(130)는 블록 교환 연산을 반복적으로 또는 재귀적으로 수행하여 키 프레임(K)를 생성할 수 있다. 블록 교환 연산은 영상 프레임(O)의 각 블록들의 위치를 일정 규칙에 따라 뒤섞는 연산으로, 뒤섞는 규칙은 시드 프레임 블록 교환 연산 키(KEY1)와 해시함수로부터 도출될 수 있다. 즉, 키 프레임 생성부(130)는 시드 프레임 블록 교환 연산 키(KEY1)와 해시함수를 사용하여 시드 프레임(S)의 블록들의 위치를 뒤섞어 키 프레임(K)을 생성할 수 있다. 그리고, 키 프레임 생성부(130)는 해시 함수의 생성, 규격 지정, 변경, 폐기 등을 수행할 수도 있다. 키 프레임 생성부(130)는 다음의 수학식 1과 같은 규칙에 의하여 시드 프레임(S)에 대한 블록 교환 연산을 수행할 수 있다.

수학식 1

<49> $$TR[i] = KEY1[i]\,\eta\, B[i]$$

<50> 수학식 1에서 i는 블록 교환되는 시드 프레임(S)의 블록 번호이고, B[i]는 블록 교환되는 시드 프레임(S)의 블록이며, KEY1[i]는 B[i]의 위치를 바꾸기 위한 시드 프레임 블록 교환 연산 키(KEY1)의 i번째 엘리먼트를 의미한다. 그리고, TR[i]는 B[i]가 이동될 위치를 나타내며, η는 블록이 이동될 위치를 구하기 위한 해시 함수(hash function)이다.

<51> 도 3은 본 발명의 실시예에 따른 블록 교환 연산을 개략적으로 보여준다.

<52> 도 3에 도시된 바와 같이, 프레임이 블록 교환 연산되면 프레임의 각 블록의 위치가 변경된다.

<53> 키 프레임 생성부(130)는 도 3과 같은 블록 교환 연산을 수행하여 도 4와 같은 키 프레임(K)를 생성한다. 도 4는 본 발명의 실시예에 따른 키 프레임을 보여준다.

<54> 계속하여 도 2를 설명한다.

<55> 배타적 논리합 연산부(140)는 영상 프레임(O)과 키 프레임 생성부(130)로부터의 키 프레임(K)을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임(X)을 생성한다(S130). 수학식 2는 배타적 논리합 연산부(140)가 수행하는 동작을 보여준다.

수학식 2

<56> $$X = O \oplus K$$

<57> 영상 프레임 블록 교환 연산부(160)는 배타적 논리합 연산부(140)로부터의 임시 영상 프레임(X)에 대하여 영상 프레임 암호화 키(KEY2)를 사용하여 블록 교환 연산을 수행하여 암호화된 영상 프레임(E)을 생성한다(S140). 영상 프레임 블록 교환 연산부(160)는 블록 교환 연산을 반복적으로 또는 재귀적으로 수행하여 암호화된 영상 프레임(E)를 생성할 수 있다. 영상 프레임 블록 교환 연산부(160)는 수학식 1과 같이 키 프레임 생성부(130)와 동일 또는 유사한 기능을 수행할 수 있다. 영상 프레임 블록 교환 연산부(160)는 해시 함수의 생성, 규격 지정, 변경, 폐기 등을 수행할 수 있다. 한편, 시드 프레임 블록 교환 연산 키(KEY1)와 영상 프레임 암호화 키(KEY2)는 동일할 수도 있고, 서로 다를 수도 있다. 영상 프레임 블록 교환 연산부(160)가 생성하는 암호화된 영상 프레임(E)의 예가 도 5에 나타난다.

<58> 도 5는 본 발명의 실시예에 따른 암호화 프레임을 보여준다. 도 5에 도시된 바와 같이, 영상 프레임은 암호화 이후에 인식할 수 없는 영상으로 변환된다.

<59> 영상 압축부(170)는 암호화된 영상 프레임(E)을 소정의 규칙에 따라 압축하여 압축된 프레임을 생성한다(S150). 이때 영상 압축부(170)는 암호화된 영상 프레임(E)의 각 블록 내의 중복된 색상 값을 제거하는 방법인 MPEG4 방식으로 암호화된 영상 프레임(E)을 압축할 수 있다. 영상 압축부(170)는 시드 프레임(S)을 압축하여 압축된 시드 프레임(S)을 생성할 수도 있다.

<60> 전송부(180)는 압축된 영상 프레임(C)을 채널에 전송한다(S160). 또한, 전송부(180)는 주기적으로 시드 프레임(S) 또는 압축된 시드 프레임(S)을 채널에 전송할 수도 있다.

<61> 다음은 도 6과 도 7을 참조하여 본 발명의 제1 실시예에 따른 영상 프레임 복원 방법을 설명한다.

<62> 도 6은 본 발명의 제1 실시예에 따른 영상 프레임 복원 장치를 개략적으로 도시한 블록도이다.

<63> 도 6에 도시된 바와 같이, 본 발명의 제1 실시예에 따른 영상 프레임 복원 장치(200)는 수신부(210), 영상 압축 해제부(220), 시드 프레임 관리부(280), 시드 프레임 블록 교환 연산 키 관리부(230), 키 프레임 생성부(240), 영상 프레임 암호화 키 관리부(250), 영상 프레임 블록 교환 연산부(260), 및 배타적 논리합 연산부(270)를 포함한다.

<64> 시드 프레임 블록 교환 연산 키 관리부(230)및 영상 프레임 암호화 키 관리부(250)는 도 1의 시드 프레임 블록 교환 연산 키 관리부(120) 및 도 1의 영상 프레임 암호화 키 관리부(150)와 동일 또는 유사한 기능을 수행하므로 그 상세한 설명을 생략한다.

<65> 도 7은 본 발명의 제1 실시예에 따른 영상 프레임 복원 방법을 개략적으로 도시한 흐름도이다.

<66> 먼저, 수신부(210)는 압축된 영상 프레임(C)을 수신한다(S210). 또한, 수신부(210)는 주기적으로 시드 프레임(S) 또는 압축된 시드 프레임(S)을 수신할 수 있다.

<67> 시드 프레임 관리부(280)는 수신부(210)로부터 수신하는 시드 프레임(S)의 사용, 재사용, 폐기 등의 관리를 수행한다. 또한, 시드 프레임 관리부(280)는 수신부(210)가 수신하는 압축된 시드 프레임(S)의 압축을 해제할 수도 있다.

<68> 다음으로, 키 프레임 생성부(240)는 시드 프레임 관리부(280)로부터의 시드 프레임(S)에 대하여 시드 프레임 블록 교환 연산 키(KEY1)를 사용하여 블록 교환 연산을 수행하여 키 프레임(K)을 생성한다(S220).

<69> 한편, 영상 압축 해제부(220)는 압축된 영상 프레임(C)의 압축을 해제하여 암호화된 영상 프레임(E)을 생성한다(S230).

<70> 그 후, 영상 프레임 블록 교환 연산부(260)는 영상 압축 해제부(220)로부터의 암호화된 영상 프레임(E)을 가지고 영상 프레임 암호화 키(KEY2)를 사용하여 블록 교환 연산을 수행하여 임시 영상 프레임(X)를 생성한다(S240).

<71> 그리고, 배타적 논리합 연산부(270)는 영상 프레임 블록 교환 연산부(260)로부터의 임시 영상 프레임(X)과 키 프레임 생성부(240)로부터의 키 프레임(K)을 가지고 배타적 논리합 연산을 수행하여 최종 복원된 영상 프레임(O)를 생성한다(S250).

<72> 다음은 도 8과 도 9를 참조하여 본 발명의 제2 실시예에 따른 영상 암호화 방법을 설명한다.

<73> 도 8은 본 발명의 제2 실시예에 따른 영상 암호화 장치를 개략적으로 도시한 블록도이다.

<74> 도 8에 도시된 바와 같이, 본 발명의 제2 실시예에 따른 영상 암호화 장치(300)는 시드 프레임 관리부(310), 시드 프레임 블록 교환 연산 키 관리부(320), 키 프레임 생성부(330), 영상 프레임 암호화 키 관리부(340), 영상 프레임 블록 교환 연산부(350), 배타적 논리합 연산부(360), 영상 압축부(370), 및 전송부(380)를 포함한다.

<75> 시드 프레임 블록 교환 연산 키 관리부(320)및 영상 프레임 암호화 키 관리부(340)는 도 1의 시드 프레임 블록 교환 연산 키 관리부(120) 및 도 1의 영상 프레임 암호화 키 관리부(150)와 동일 또는 유사한 기능을 수행하므로 그 상세한 설명을 생략한다.

<76> 도 9는 본 발명의 제2 실시예에 따른 영상 암호화 방법을 개략적으로 도시한 흐름도이다.

<77> 먼저, 시드 프레임 관리부(310)는 시드 프레임(S)의 생성, 재사용, 폐기 등의 관리를 수행한다(S310). 이때, 시드 프레임 관리부(310)는 암호화하고자 하는 하나 이상의 영상 프레임(O)를 기초로 시드 프레임(S)를 생성할 수 있다.

<78> 다음으로, 키 프레임 생성부(330)는 시드 프레임 관리부(310)로부터의 시드 프레임(S)에 대하여 시드 프레임 블록 교환 연산 키(KEY1)를 사용하여 블록 교환 연산을 수행하여 키 프레임(K)을 생성한다(S320).

<79> 한편, 영상 프레임 블록 교환 연산부(350)는 영상 프레임(O)에 대하여 영상 프레임 암호화 키(KEY2)를 사용하여 블록 교환 연산을 수행하여 임시 영상 프레임(X)를 생성한다(S330).

<80> 배타적 논리합 연산부(360)는 영상 프레임 블록 교환 연산부(350)로부터의 임시 영상 프레임(X)와 키 프레임 생성부(330)로부터의 키 프레임(K)을 가지고 배타적 논리합 연산을 수행하여 암호화된 영상 프레임(E)을 생성한다(S340).

<81> 영상 압축부(370)는 암호화된 영상 프레임(E)을 압축하여 압축된 영상 프레임(C)를 생성한다(S350).

<82> 전송부(380)는 압축된 영상 프레임(C)을 채널에 전송한다(S360). 또한, 전송부(380)는 주기적으로 시드 프레임(S) 또는 압축된 시드 프레임(S)을 채널에 전송할 수 있다.

<83> 다음은 도 10과 도 11을 참조하여 본 발명의 제2 실시예에 따른 영상 프레임 복원 방법을 설명한다.

<84> 도 10은 본 발명의 제2 실시예에 따른 영상 프레임 복원 장치를 개략적으로 도시한 블록도이다.

<85> 도 10에 도시된 바와 같이, 본 발명의 제2 실시예에 따른 영상 프레임 복원 장치(400)는 수신부(410), 영상 압축 해제부(420), 시드 프레임 관리부(480), 시드 프레임 블록 교환 연산 키 관리부(430), 키 프레임 생성부(440), 배타적 논리합 연산부(450), 영상 프레임 암호화 키 관리부(460), 및 영상 프레임 블록 교환 연산부(470)을 포함한다.

<86> 시드 프레임 블록 교환 연산 키 관리부(430)및 영상 프레임 암호화 키 관리부(460)는 도 1의 시드 프레임 블록 교환 연산 키 관리부(120) 및 도 1의 영상 프레임 암호화 키 관리부(150)와 동일 또는 유사한 기능을 수행하므로 그 상세한 설명을 생략한다.

<87> 도 11은 본 발명의 제2 실시예에 따른 영상 프레임 복원 방법을 개략적으로 도시한 흐름도이다.

<88> 먼저, 수신부(410)는 압축된 영상 프레임(C)을 수신한다(S410). 또한, 수신부(410)는 주기적으로 시드 프레임(S) 또는 압축된 시드 프레임(S)을 수신할 수 있다.

<89> 시드 프레임 관리부(480)는 수신부(410)로부터 수신하는 시드 프레임(S)의 사용, 재사용, 폐기 등의 관리를 수행한다. 또한, 시드 프레임 관리부(480)는 수신부(410)가 수신하는 압축된 시드 프레임(S)의 압축을 해제할 수도 있다.

<90> 다음으로, 키 프레임 생성부(440)는 시드 프레임 관리부(410)로부터의 시드 프레임(S)에 대하여 시드 프레임 블록 교환 연산 키(KEY1)를 사용하여 블록 교환 연산을 수행하여 키 프레임(K)을 생성한다(S420).

<91> 한편, 영상 압축 해제부(420)는 압축된 영상 프레임(C)의 압축을 해제하여 암호화된 영상 프레임(E)을 생성한다(S430).

<92> 그 후, 배타적 논리합 연산부(450)는 영상 압축 해제부(420)로부터의 암호화된 영상 프레임(E)과 키 프레임 생성부(440)로부터의 키 프레임(K)을 가지고 배타적 논리합 연산을 수행하여 임시 영상 프레임(X)를 생성한다(S440).

<93> 그리고, 영상 프레임 블록 교환 연산부(470)는 배타적 논리합 연산부(450)로부터의 임시 영상 프레임(X)을 가지고 영상 프레임 암호화 키(KEY2)를 사용하여 블록 교환 연산을 수행하여 최종 복원된 영상 프레임(O)를 생성한다(S450).

<94> 도 12는 다양한 암호화 방식에 따른 압축률을 보여준다.

<95> 도 12에서, Normal은 암호화를 수행하지 않은 경우를 나타내고, AES는 Advanced Encryption Standard를 나타내며, XOR는 배타적 논리합 연산을 통한 암호화를 의미한다. 그리고, "Scramble with XOR"는 배타적 논리합 연산과 스크램블을 결합한 암호화를 나타내고, SRMT(Secure Real-time Media Transmission)는 본 발명의 실시예에 따른 암호화를 나타낸다.

<96> 도 12에 도시된 바와 같이, 본 발명의 실시예에 따른 암호화 알고리즘은 다른 암호화 알고리즘에 비하여 더 나은 압축률을 보여준다.

<97> 본 발명의 실시예는 이상에서 설명한 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.

<98> 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.

발명의 효과

<99> 본 발명의 실시예에 따르면, 움직임의 많고 적음 등 멀티미디어의 특성에 상관없이 효율적으로 멀티미디어를 암호화할 수 있다.

<100> 또한, 본 발명의 실시예에 따르면, 영상 암호화 장치는 영상의 압축에 사용되는 구조적인 특성을 고려하여 영상 프레임을 암호화하므로, 암호화를 위한 시간과 자원이 절약되고 압축률이 크게 저하되지 않는다. 이에 따라 영상 암호화 방법은 멀티미디어의 실시간 전송에 이용될 수 있다.

<101> 뿐만 아니라, 본 발명의 실시예에 따르면, 영상 암호화 장치는 하나 이상의 영상 프레임에서 최소 존재 확률을 가지는 색상 값으로 시드 프레임을 구성하는 색상 값을 결정함으로써 압축률의 저하를 더욱 방지한다.

도면의 간단한 설명

<1> 도 1은 본 발명의 제1 실시예에 따른 영상 암호화 장치를 개략적으로 도시한 블록도이다.

<2> 도 2는 본 발명의 제1 실시예에 따른 영상 암호화 방법을 개략적으로 도시한 흐름도이다.

<3> 도 3은 본 발명의 실시예에 따른 블록 교환 연산을 개략적으로 보여준다.

<4> 도 4는 본 발명의 실시예에 따른 키 프레임을 보여준다.

<5> 도 5는 본 발명의 실시예에 따른 암호화 프레임을 보여준다.

<6> 도 6은 본 발명의 제1 실시예에 따른 영상 프레임 복원 장치를 개략적으로 도시한 블록도이다.

<7> 도 7은 본 발명의 제1 실시예에 따른 영상 프레임 복원 방법을 개략적으로 도시한 흐름도이다.

<8> 도 8은 본 발명의 제2 실시예에 따른 영상 암호화 장치를 개략적으로 도시한 블록도이다.

<9> 도 9는 본 발명의 제2 실시예에 따른 영상 암호화 방법을 개략적으로 도시한 흐름도이다.

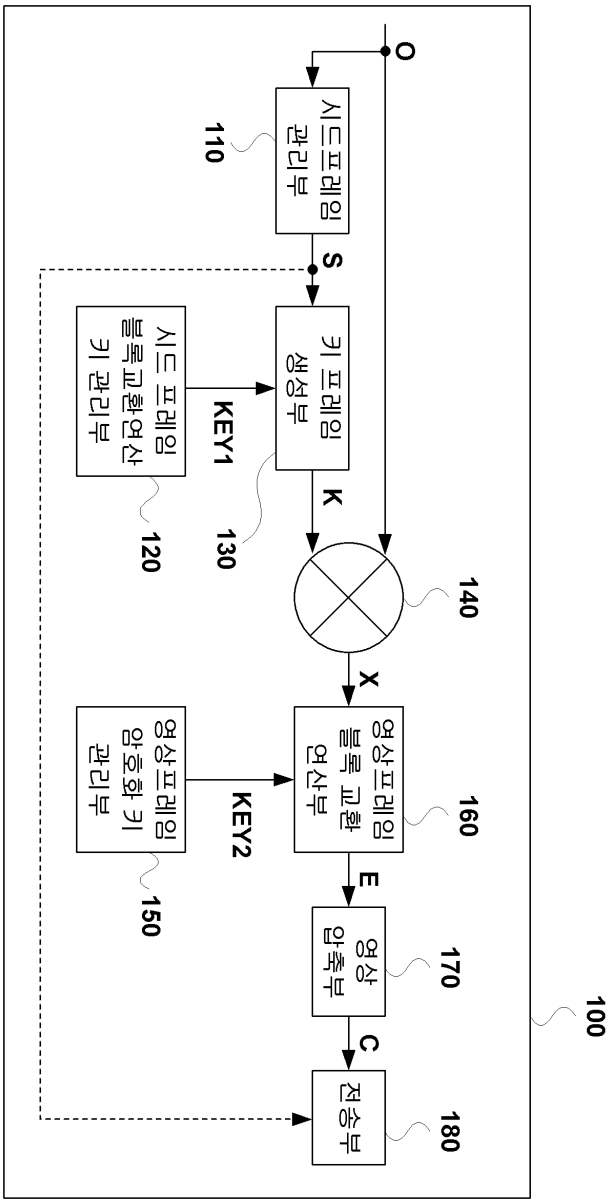
<10> 도 10은 본 발명의 제2 실시예에 따른 영상 프레임 복원 장치를 개략적으로 도시한 블록도이다.

<11> 도 11은 본 발명의 제2 실시예에 따른 영상 프레임 복원 방법을 개략적으로 도시한 흐름도이다.

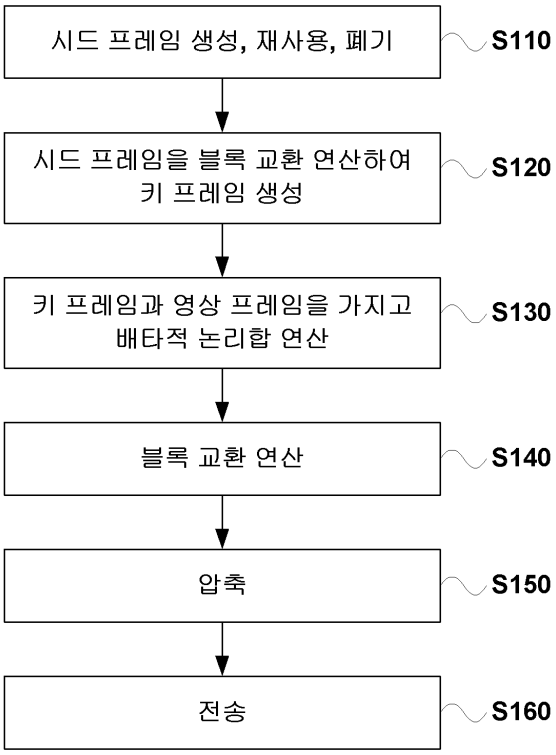
<12> 도 12는 다양한 암호화 방식에 따른 압축률을 보여준다.

도면

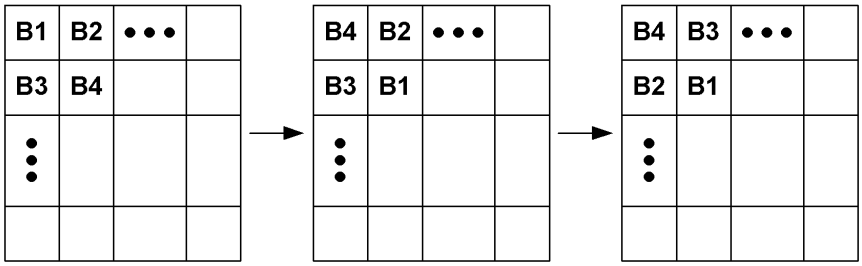
도면1


O
시드프레임 관리부
110
S
키 프레임 생성부
시드 프레임 블록교환연산 키 관리부
KEY1
120
130
K
140
X
영상프레임 블록 교환 연산부
영상프레임 암호화 키 관리부
KEY2
150
160
E
영상 압축부
170
C
전송부
180
100

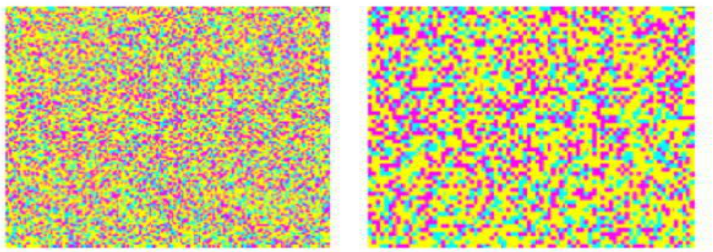
도면2


시드 프레임 생성, 재사용, 폐기
S110
시드 프레임을 블록 교환 연산하여 키 프레임 생성
S120
키 프레임과 영상 프레임을 가지고 배타적 논리합 연산
S130
블록 교환 연산
S140
압축
S150
전송
S160

도면3

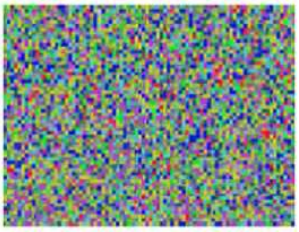

B1 B2 • • •
B3 B4
B4 B2 • • •
B3 B1
B4 B3 • • •
B2 B1

도면4



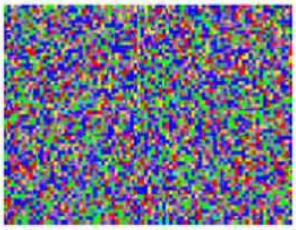
도면5

(a) Lab



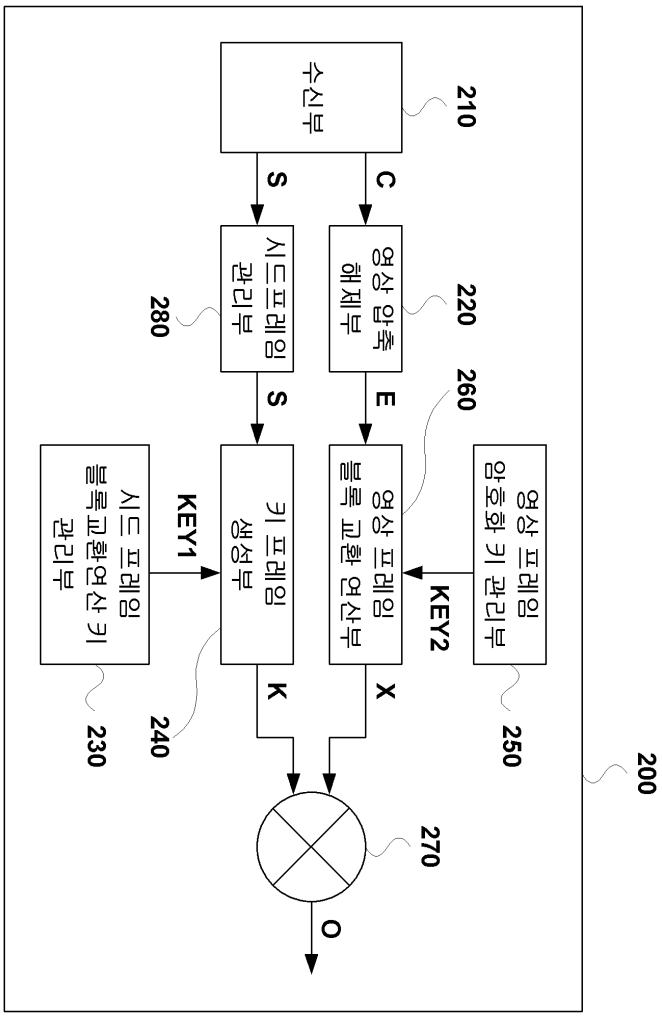
(b) Encrypted lab

(c) Dancer

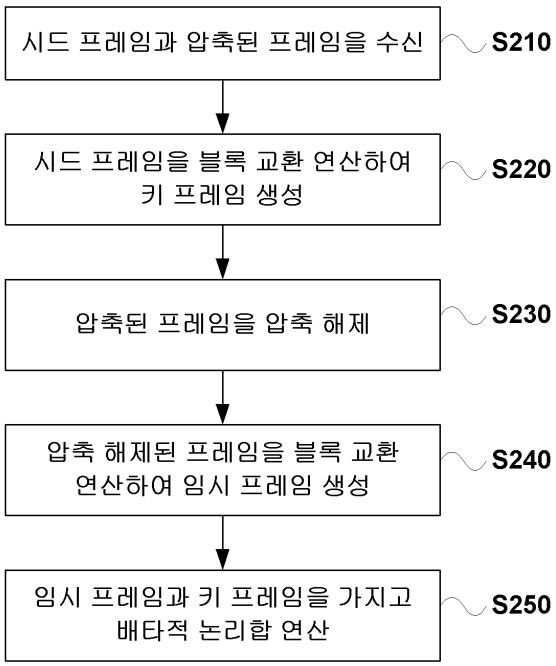


(d) Encrypted dancer

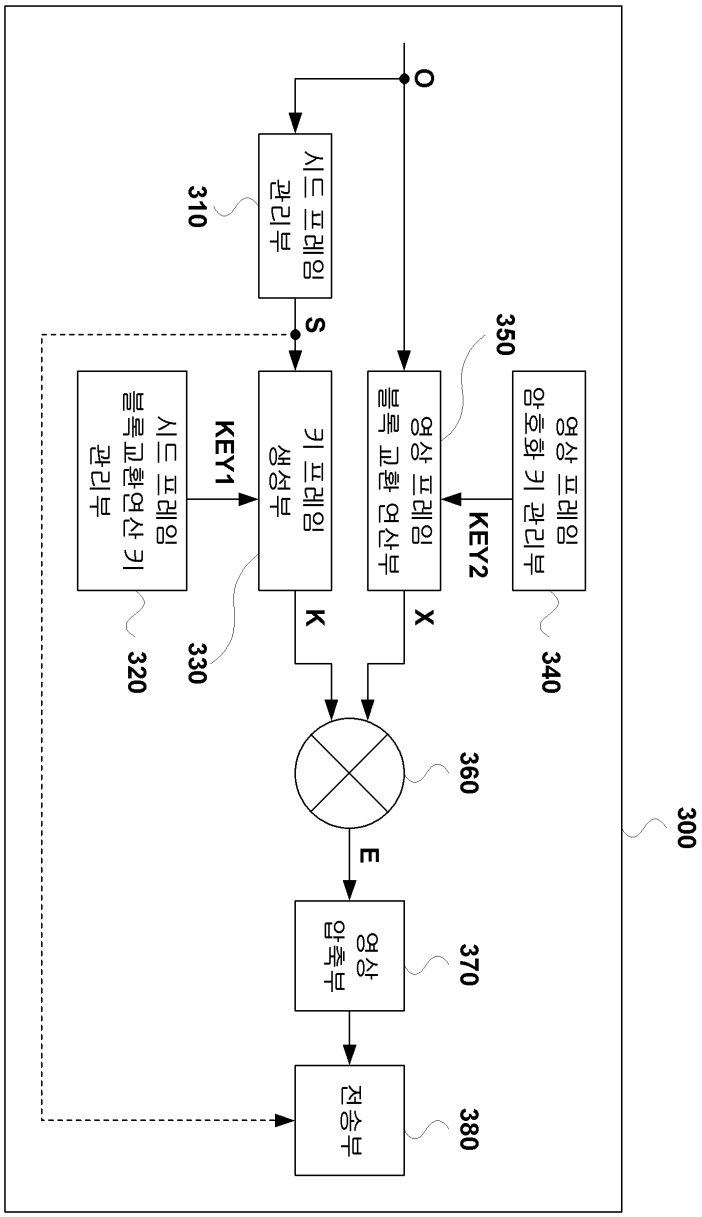
도면6


수신부
210
C
S
영상 압축 해제부
220
시드프레임 관리부
280
260
E
S
영상 프레임 블록 교환 연산부
KEY2
키 프레임 생성부
KEY1
영상 프레임 암호화 키 관리부
250
시드 프레임 블록교환연산 키 관리부
230
240
K
X
270
O
200

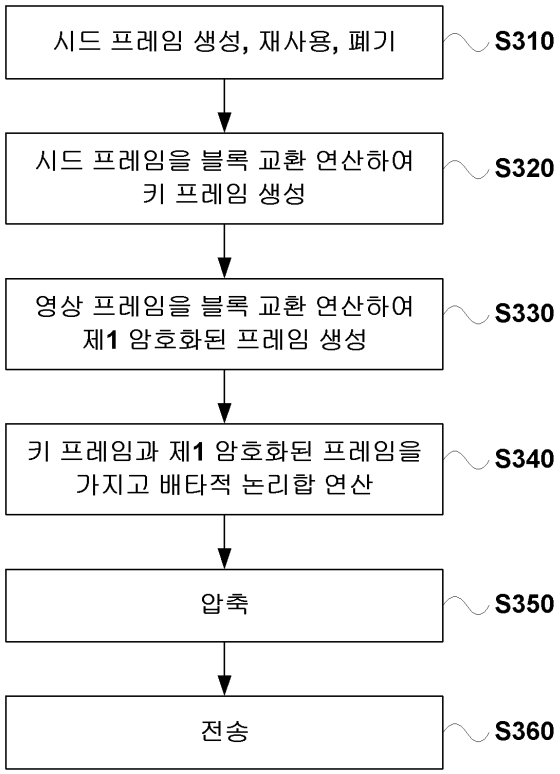
도면7


시드 프레임과 압축된 프레임을 수신
S210
시드 프레임을 블록 교환 연산하여 키 프레임 생성
S220
압축된 프레임을 압축 해제
S230
압축 해제된 프레임을 블록 교환 연산하여 임시 프레임 생성
S240
임시 프레임과 키 프레임을 가지고 배타적 논리합 연산
S250

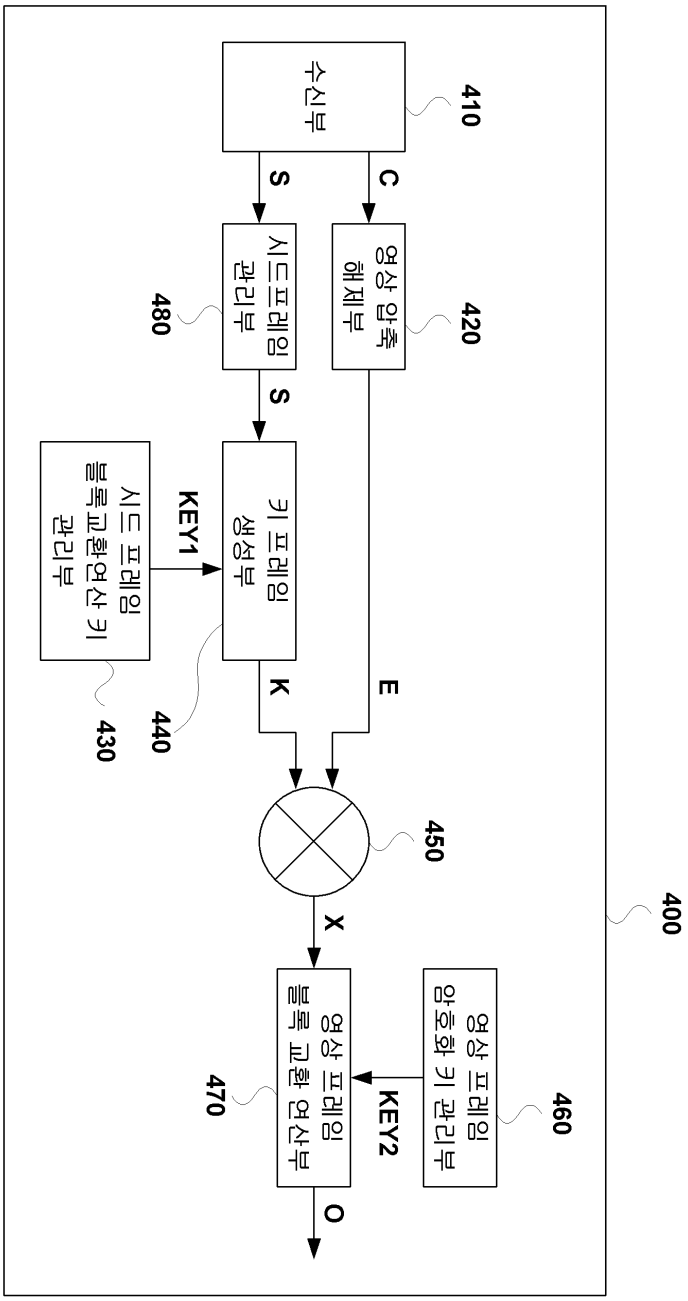
도면8


O
시드 프레임 관리부
310
S
키 프레임 생성부
KEY1
시드 프레임 블록교환연산 키 관리부
320
330
영상 프레임 블록 교환 연산부
350
KEY2
영상 프레임 암호화 키 관리부
340
K
X
360
E
영상 압축부
370
전송부
380
300

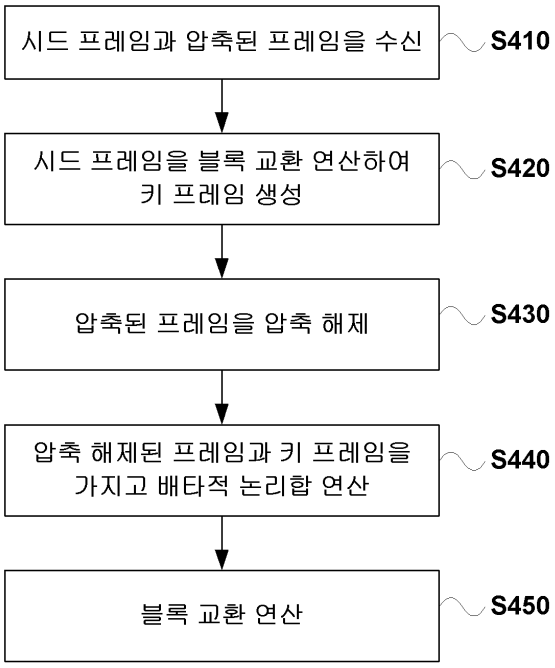
도면9


시드 프레임 생성, 재사용, 폐기
S310
시드 프레임을 블록 교환 연산하여 키 프레임 생성
S320
영상 프레임을 블록 교환 연산하여 제1 암호화된 프레임 생성
S330
키 프레임과 제1 암호화된 프레임을 가지고 배타적 논리합 연산
S340
압축
S350
전송
S360

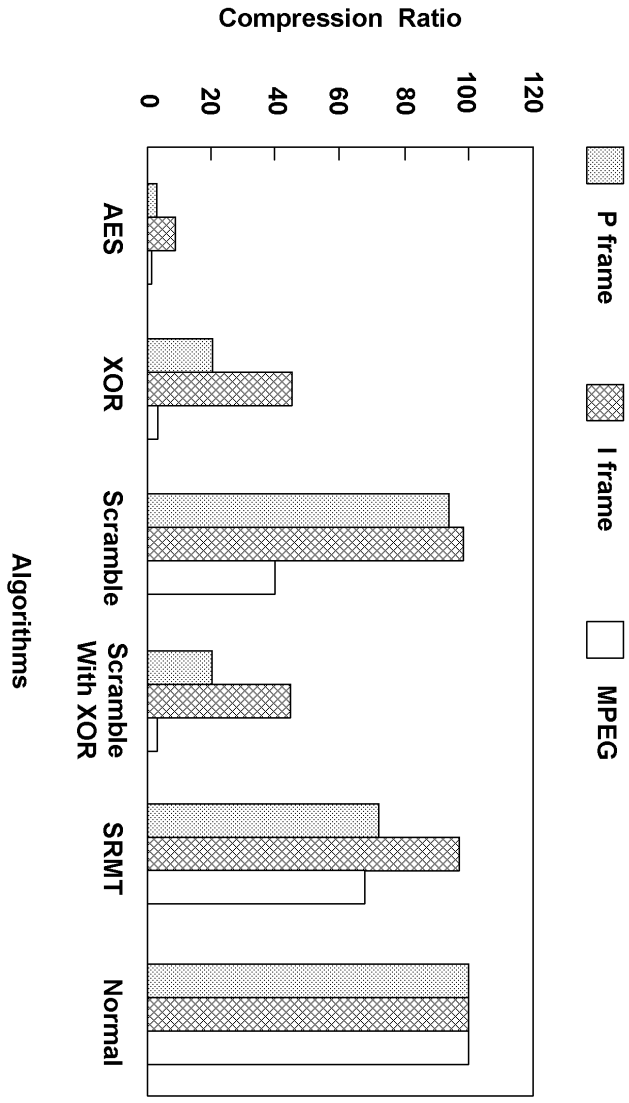
도면10


수신부
410
S
C
시드프레임 관리부
480
영상 압축 해제부
420
S
시드 프레임 블록교환연산 키 관리부
KEY1
키 프레임 생성부
430
440
K
E
450
X
영상 프레임 블록 교환 연산부
470
KEY2
영상 프레임 암호화 키 관리부
460
O
400

도면11


시드 프레임과 압축된 프레임을 수신
S410
시드 프레임을 블록 교환 연산하여 키 프레임 생성
S420
압축된 프레임을 압축 해제
S430
압축 해제된 프레임과 키 프레임을 가지고 배타적 논리합 연산
S440
블록 교환 연산
S450

도면12


Compression Ratio
0
20
40
60
80
100
120
AES
XOR
Scramble
Scramble With XOR
SRMT
Normal
Algorithms
P frame
I frame
MPEG