(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0114719
(43) 공개일자 2012년10월17일

(51) 국제특허분류(Int. Cl.)
H04N 7/24 (2011.01)
(21) 출원번호 10-2011-0032422
(22) 출원일자 2011년04월08일
심사청구일자 없음

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정용화
대전광역시 유성구 은구비로 31, 열매마을아파트 505동 402호 (지족동)
정서현
서울특별시 동작구 동작대로29길 119, 102동 1506호 (사당동, 극동아파트)
(뒷면에 계속)
(74) 대리인
특허법인충현

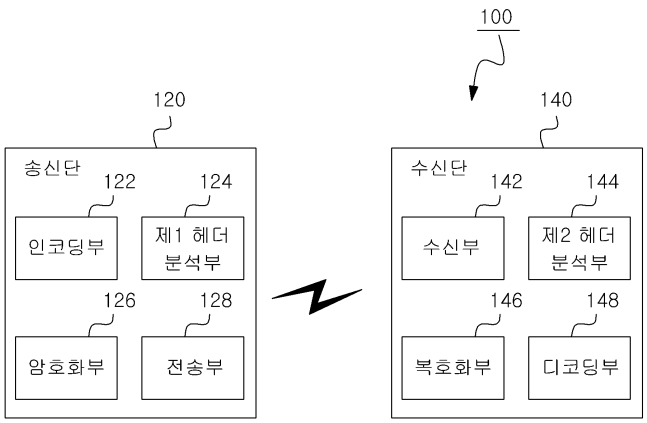
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 **영상의 부분 암호화 및 복호화 시스템 및 방법**

(57) 요 약

본 발명은 영상프레임에 대한 인코딩을 수행하는 인코딩부와, 상기 영상프레임을 구성하는 슬라이스 내 헤더데이터를 분석하는 제1헤더분석부와, 상기 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화하는 암호화부 및 상기 헤더데이터 및 일부 암호화된 슬라이스데이터의 포함하는 슬라이스에 해당하는 영상프레임을 전송하는 전송부;를 포함하는 송신단; 및 상기 송신단으로부터 전송된 상기 영상프레임을 수신하는 수신부와, 수신한 상기 영상프레임의 헤더데이터를 분석하는 제2헤더분석부와, 분석한 헤더데이터를 제외한 슬라이스데이터 중 적어도 적어도 하나의 슬라이스데이터를 인증이 완료된 복호화키에 기초하여 복호화하는 복호화부 및 복호화된 적어도 하나의 슬라이스데이터를 포함하는 슬라이스의 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득하는 디코딩부를 포함하는 수신단;을 포함하되, 상기 수신단은 인증이 완료되지 않은 복호화키를 이용하여 상기 영상프레임에 대한 디코딩을 수행하는 경우, 상기 영상프레임 내 다수의 슬라이스데이터에 에러가 전파되는 것을 특징으로 한다. 이러한 구성에 의해, 본 발명은 영상프레임의 각 슬라이스에 대한 헤더데이터를 분석 후, 상기 헤더데이터 이후의 슬라이스데이터 일부만을 암호화함으로써, 상기 영상프레임에 대한 암호화시간을 감소시킬 수 있다.

대 표 도 - 도1



(72) 발명자

이성주

서울특별시 마포구 월드컵북로22길 20 (성산동)

이은지

경상북도 경산시 정평동 130 현대타운 106-602

이 발명을 지원한 국가연구개발사업

과제고유번호 1345097011

부처명 한국산업기술재단

연구사업명 지역혁신인력양성사업

연구과제명 (2차년도)베터리로동작하는 감시카메라용 비디오 압축 특성을 이용한 정보보호 및 상황인지 연구를 통한 최적화

주관기관 고려대학교 산학협력단

연구기간 2010.05.01 ~ 2011.04.30

특허청구의 범위

청구항 1

영상프레임에 대한 인코딩을 수행하는 인코딩부와, 상기 영상프레임을 구성하는 슬라이스 내 헤더데이터를 분석하는 제1헤더분석부와, 상기 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화하는 암호화부 및 상기 헤더데이터 및 일부 암호화된 슬라이스데이터의 포함하는 슬라이스에 해당하는 영상프레임을 전송하는 전송부;를 포함하는 송신단; 및

상기 송신단으로부터 전송된 상기 영상프레임을 수신하는 수신부와, 수신한 상기 영상프레임의 헤더데이터를 분석하는 제2헤더분석부와, 분석한 헤더데이터를 제외한 슬라이스데이터 중 적어도 적어도 하나의 슬라이스데이터를 인증이 완료된 복호화키에 기초하여 복호화하는 복호화부 및 복호화된 적어도 하나의 슬라이스데이터를 포함하는 슬라이스의 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득하는 디코딩부를 포함하는 수신단;을 포함하되,

상기 수신단은

인증이 완료되지 않은 복호화키를 이용하여 상기 영상프레임에 대한 디코딩을 수행하는 경우, 상기 영상프레임 내 다수의 슬라이스데이터에 에러가 전파되는 것을 특징으로 하는 영상의 부분 암호화 및 복호화 시스템.

청구항 2

제1항에 있어서,

상기 암호화부는

상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 암호화하는 것을 특징으로 하는 영상의 부분 암호화 및 복호화 시스템.

청구항 3

제1항에 있어서,

상기 복호화부는

상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 복호화하는 것을 특징으로 하는 영상의 부분 암호화 및 복호화 시스템.

청구항 4

송신단이 영상프레임의 인코딩을 수행하고, 상기 영상프레임 내 슬라이스의 헤더데이터를 분석하는 제1헤더분석단계;

상기 송신단이 상기 영상프레임의 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화하는 암호화단계;

수신단이 상기 송신단으로부터 암호화된 상기 영상프레임을 수신하고, 수신한 상기 영상프레임의 슬라이스 내 헤더데이터를 분석하는 제2헤더분석단계;

상기 수신단이 상기 영상프레임 중 분석한 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 인증이 완료된 복호화키에 기초하여 복호화하는 복호화단계;

상기 수신단이 복호화된 슬라이스데이터를 포함하는 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득하는 디코딩단계;

를 포함하되,

상기 디코딩단계는

인증이 완료되지 않은 복호화키를 이용하여, 상기 영상프레임에 대한 디코딩을 수행하는 경우, 상기 영상프레임 내 다수의 슬라이스데이터에 에러가 전파되는 것을 특징으로 하는 영상의 부분 암호화 및 복호화 방법.

청구항 5

제1항에 있어서,

상기 암호화단계 또는 상기 복호화단계는

상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 암호화 또는 복호화하는 것을 특징으로 하는 영상의 부분 암호화 및 복호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 영상의 부분 암호화 및 복호화 시스템 및 방법에 관한 것으로, 특히, 영상에 대한 암호화 시간을 감소시키면서, 허용되지 않은 외부인이 접근하는 경우, 정보를 보호할 수 있는 영상의 부분 암호화 및 복호화 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 들어, 기술의 발전에 따라, 대량의 멀티미디어 데이터가 휴대폰과 같은 휴대기기로 전송되어, 남녀노소 누구나 장소에 구애받지 않고, 전송받은 멀티미디어 데이터를 실행하여 다양한 서비스를 제공받고 있다.

[0003] 이처럼 멀티미디어 데이터를 전송받고자 하는 수요가 급증함에 따라, 대용량의 멀티미디어 데이터를 각종 휴대기기로 전송 시, 전송되는 상기 멀티미디어 데이터에 대한 정보보호의 중요성 또한 급증하고 있는 것이 현실이다. 이처럼, 휴대기기로 전송되는 멀티미디어 데이터에 대하여 내부 정보보호를 위해 휴대기기로의 전송 시 암호화를 수행하고 있다.

[0004] 하지만, 이러한 멀티미디어 데이터는 대부분 대용량이기 때문에, 멀티미디어 데이터의 전송 시, 수행되는 상기 멀티미디어 데이터에 대한 암호화에 있어서, 많은 시간이 소요되는 문제점이 발생했다.

[0005] 이러한 문제점을 해결하기 위해, 다양한 방법들이 연구되고 있는데, 그 중에서도 암호화 및 압축을 병합한 형태의 비디오 암호화-압축방법인 SECMPEG을 이용하여, 멀티미디어 데이터의 암호화 시 오버헤드를 줄여주는 방법이 주로 사용되고 있다. 하지만 이러한 SECMPEG 또한 전송하고자 하는 멀티미디어 데이터를 실시간으로 암호화 시키는 데 있어서, 많은 계산량이 필요하므로 멀티미디어 데이터에 대한 암호화 시간이 길어지는 문제점은 여전히 발생되고 있다.

발명의 내용

해결하려는 과제

[0006] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 영상프레임을 구성하는 각 슬라이스 내 헤더데이터 이후의 일부 슬라이스데이터만을 암호화하여 인증되지 않은 복호화키를 이용하여 복호화를 수행하는 경우, 영상프레임의 전체에 대해 에러가 전파되도록 함으로써, 영상프레임에 대한 암호화 시간을 줄이면서도, 허용되지 않은 외부인의 접근으로부터 상기 영상프레임의 정보 보호를 용이하게 할 수 있는 영상의 부분 암호화 및 복호화 시스템 및 방법을 제공하고자 한다.

과제의 해결 수단

[0007] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 영상의 부분 암호화 및 복호화 시스템은 영상프레임에 대한 인코딩을 수행하는 인코딩부와, 상기 영상프레임을 구성하는 슬라이스 내 헤더데이터를 분석하는 제1헤더분석부와, 상기 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화하는 암호화부 및 상기 헤더데이터 및 일부 암호화된 슬라이스데이터의 포함하는 슬라이스에 해당하는 영상프레임을 전송하는 전송부;를 포함하는 송신단; 및 상기 송신단으로부터 전송된 상기 영상프레임을 수신하는 수신부와, 수신한 상기 영상프레임의 헤더데이터를 분석하는 제2헤더분석부와, 분석한 헤더데이터를 제외한 슬라이스데이터 중 적어도 적어도 하나의 슬라이스데이터를 인증이 완료된 복호화키에 기초하여 복호화하는 복호화부 및 복호화된 적어도 하나의 슬라이스데이터를 포함하는 슬라이스의 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득하는 디코딩부를 포함하는 수신단;을 포함하되, 상기 수신단은 인증이 완료되지 않은 복호화키를 이용하여 상기 영상프레임에 대한 디코딩을 수행하는 경우, 상기 영상프레임 내 다수의 슬라이스데이터에 에러가 전파되는 것을 특징으로 한다.

[0008] 보다 바람직하게는 상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 암호화하는 암호화부를 포함할 수 있다.

[0009] 보다 바람직하게는 상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 복호화하는 복호화부를 포함할 수 있다.

[0010] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 영상의 부분 암호화 및 복호화 방법은 송신단이 영상프레임의 인코딩을 수행하고, 상기 영상프레임 내 슬라이스의 헤더데이터를 분석하는 제1헤더분석단계; 상기 송신단이 상기 영상프레임의 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화하는 암호화단계; 수신단이 상기 송신단으로부터 암호화된 상기 영상프레임을 수신하고, 수신한 상기 영상프레임의 슬라이스 내 헤더데이터를 분석하는 제2헤더분석단계; 상기 수신단이 상기 영상프레임 중 분석한 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 인증이 완료된 복호화키에 기초하여 복호화하는 복호화단계; 상기 수신단이 복호화된 슬라이스데이터를 포함하는 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득하는 디코딩단계; 를 포함하되, 상기 디코딩단계는 인증이 완료되지 않은 복호화키를 이용하여, 상기 영상프레임에 대한 디코딩을 수행하는 경우, 상기 영상프레임 내 다수의 슬라이스데이터에 에러가 전파되는 것을 특징으로 한다.

[0011] 보다 바람직하게는, 상기 영상프레임 내 분석된 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터를 암호화 또는 복호화하는 암호화단계 또는 복호화단계를 포함할 수 있다.

발명의 효과

[0012] 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 영상프레임을 구성하는 각 슬라이스에 대한 헤더데이터를 분석한 후, 상기 헤더데이터 이후의 슬라이스데이터 일부만을 암호화함으로써, 상기 영상프레임에 대한 암호화시간을 감소시키는 효과가 있다.

[0013] 또한, 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 영상프레임을 구성하는 슬라이스 중 영상정보를 포함하는 슬라이스데이터 중 일부 슬라이스데이터만을 암호화하여 암호화 수행시간이 감소됨에 따라, 상기 영상프레임에 대한 실시간 암호화를 수행할 수 있는 효과가 있다.

[0014] 더불어, 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 인증이 완료되지 않은 복호화키를 이용하여 암호화된 영상프레임을 복호화하는 경우, 상기 영상프레임의 전체에 대한 정보보호가 이루어짐에 따라, 인증이 완료된 복호화키를 갖는 허용된 사용자 즉, 수신단이 상기 영상프레임에 대한 복호화를 수행하여, 원본 영상프레임을 획득할 수 있으므로, 데이터 정보보호의 신뢰성을 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시 예에 따른 영상의 부분 암호화 및 복호화 시스템의 블록도이다.

도 2는 본 발명의 다른 실시 예에 따른 영상의 부분 암호화 및 복호화 방법의 순서도이다.

도 3은 영상프레임 내부의 에러 전파과정을 나타낸 도면이다.

도 4(a)는 영상프레임 내 헤더데이터 이후 첫 번째 슬라이스데이터를 암호화한 결과를 나타낸 영상이고, 도 4(b)는 영상프레임 내 헤더데이터 이후 중간 슬라이스데이터부터 일부 슬라이스데이터를 암호화한 결과를 나타낸 영상이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 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 실시 예에 한정되는 것은 아니다.

[0017] 본 발명에 대하여 설명하기에 앞서, 본 발명에서 사용되는 영상프레임에 대하여 먼저 살펴보도록 한다. 상기 영상프레임은 기본적으로 I-프레임, P-프레임, B-프레임으로 구성되며, 이 때, 상기 I-프레임은 다른 P-프레임 또는 B-프레임의 참조없이 정지영상의 압축 표준인 JPEG 방식으로 압축된 프레임을 나타낸다. 또한, P-프레임은 I-프레임 또는 B-프레임의 데이터를 참조하는 모션벡터(Motion Vector)를 가지고 있으므로, 상기 I-프레임에 비해 상대적으로 데이터의 크기가 적은 것이 특징이다. 이와 더불어, 상기 B-프레임은 I-프레임과 P-프레임 간 또는 P-프레임과 P-프레임 간에 움직임의 차를 보간하여 데이터를 구성한다. 이 때, 각 프레임 간 움직임 보상 시, 맞는 블록을 찾지 못하는 경우, 그 블록을 인트라 코드 상태로 압축하고, 해당 매크로블록을 I-블록으로 정의한다.

[0018] 이와 더불어, 각 프레임은 데이터 열의 최소단위인 슬라이스로 구성되어 있으며, 일반적으로 한 개의 슬라이스로 영상의 한 행이 구성되며, 매 행마다 새로운 슬라이스가 구성된다.

[0019] 그 중에서도 상기 I-프레임은 상기 B-프레임 또는 P-프레임보다 더 큰 크기를 갖는 것을 알 수 있는데, 이는 앞서 상술한 바와 같이, 상기 I-프레임이 한 장의 원 영상을 압축한 데이터인 반면, 상기 B-프레임과 P-프레임은 움직임 예측에 의한 차 영상으로 구성이 되어 있기 때문이다.

[0020] 그러므로, 본 발명에서는 영상프레임을 구성하는 각 프레임 중 가장 많은 크기를 갖는 I-프레임에 대한 부분 암호화를 수행함으로써, 보다 효율적인 영상프레임의 암호화를 수행할 수 있도록 한다.

[0021] 이하, 도 1을 참조하여, 본 발명에 따른 I-프레임을 구성하는 슬라이스의 부분 암호화 및 복호화에 대하여 자세히 설명하도록 한다.

[0022] 도 1은 본 발명의 일 실시 예에 따른 영상의 부분 암호화 및 복호화 시스템의 블록도이다.

[0023] 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 영상의 부분 암호화 및 복호화 시스템(100)은 MPEG 비디오 스트림과 같은 영상프레임을 암호화하여 전송하는 송신단(120)과, 암호화된 영상프레임을 입력받아 복호화함으로써, 원본 영상프레임을 획득하는 수신단(140)을 포함한다.

[0024] 송신단(120)은 인코딩부(122), 제1헤더분석부(124), 암호화부(126) 및 전송부(128)를 포함한다.

[0025] *인코딩부(122)는 암호화하고자 하는 영상프레임에 대하여 인코딩을 수행하고, 이에 따라 압축데이터를 생성한다. 이때, 상기 인코딩부(122)에서는 MPEG2 인코더를 사용하여, 상기 영상프레임을 인코딩할 수 있다.

[0026] 제1헤더분석부(124)는 상기 인코딩부(122)를 통해 인코딩된 압축데이터를 포함하는 영상프레임은 데이터 열의 최소단위인 슬라이스로 각각 이루어짐에 따라, 상기 영상프레임의 슬라이스 내 헤더데이터를 분석함으로써, 상기 영상프레임의 각 슬라이스 중 영상정보를 포함하는 헤더데이터 및 영상정보를 포함하는 슬라이스데이터를 확인한다.

[0027] 예를 들어, 상기 제1헤더분석부(124)는 상기 슬라이스 중 '00 00 01 0X'의 헥사코드로 이루어진 압축데이터를 헤더데이터로 판단하고, 이에 따라 상기 슬라이스 내 헤더데이터와 슬라이스데이터를 구분할 수 있도록 한다.

[0028] 암호화부(126)는 상기 제1헤더분석부(124)가 상기 슬라이스 중 분석한 헤더데이터 이후의 압축데이터에 대하여 영상정보를 포함하는 슬라이스데이터로 판단하고, 상기 슬라이스데이터에 대하여 암호화를 수행한다. 이 때, 상

기 암호화부(126)는 상기 헤더데이터 이후 첫 압축데이터 즉, 전체 슬라이스데이터 중 첫 번째 슬라이스데이터부터 이후 16 Byte에 해당하는 슬라이스데이터까지만 암호화를 수행하도록 한다. 이처럼, 상기 암호화부(126)가 전체 슬라이스데이터 중 처음 16 Byte의 슬라이스데이터에 대해서만 암호화를 수행하는 것은 16Byte의 슬라이스데이터가 AES암호화를 수행하기 위한 기본 데이터 크기이기 때문이다.

[0029] 따라서, 상기 암호화부(126)는 상기 슬라이스 내 모든 슬라이스데이터에 대하여 암호화를 수행하는 것이 아니라, 헤더데이터 이후의 일부 슬라이스데이터에 대해서만 부분적으로 암호화를 수행하는 것이다.

[0030] 이때, 상기 상기 암호화부(126)는 AES(Advanced Encryption Standard)암호화를 이용하여 상기 슬라이스데이터를 암호화할 수 있다.

[0031] 전송부(128)는 상기 암호화부(126)를 통해 암호화된 슬라이스데이터 및 헤더데이터를 포함하는 상기 슬라이스를 수신단(140)으로 전송한다.

[0032] 수신단(140)은 수신부(142), 제2헤더분석부(144), 복호화부(146) 및 디코딩부(148)를 포함한다.

[0033] 수신부(142)는 상기 송신단(120)의 전송부(128)로부터 전송된 슬라이스데이터 및 헤더데이터를 포함하는 상기 슬라이스를 수신한다.

[0034] 제2헤더분석부(144)는 상기 수신부(142)가 수신한 상기 슬라이스 중 헤더데이터를 분석한다. 이러한 상기 제2헤더분석부(144)는 상기 제1헤더분석부(124)와 마찬가지로, 수신한 상기 슬라이스 중 '00 00 01 0X'의 헥사코드로 이루어진 압축데이터에 대해서 헤더데이터로 판단하고, 상기 슬라이스 내 상기 헤더데이터 이후의 압축데이터를 슬라이스데이터로 판단한다.

[0035] 복호화부(146)는 상기 슬라이스 중 상기 제2헤더분석부(144)가 분석한 헤더데이터를 제외한 슬라이스데이터에 대해 복호화키를 이용하여 복호화를 수행한다. 이러한 상기 복호화부(146)는 상기 제2헤더분석부(144)가 분석한 헤더데이터 이후의 첫 번째 슬라이스데이터부터 이후 16 Byte에 해당하는 슬라이스데이터까지 복호화를 수행할 수 있다.

[0036] 디코딩부(148)는 상기 복호화부(146)를 통해 복호화된 슬라이스데이터에 대한 디코딩을 수행하여, 암호화 수행 전 원본 영상프레임을 획득한다.

[0037] 하지만, 상기 복호화부(146)가 미리 설정되어 인증이 완료된 복호화키가 아닌 그 외의 다른 복호화키를 이용하여 복호화를 수행하거나, 또는 복호화키없이 복호화를 수행한 후, 디코딩을 수행하는 경우, 암호화된 일부 슬라이스데이터로 인하여, 암호화되지 않은 나머지 슬라이스데이터까지 에러가 전파되어 영상에 대한 정보보호가 이루어진다.

[0038] 이하, 도 2를 참조하여, 본 발명의 다른 실시 예에 따른 영상의 부분 암호화 및 복호화 방법에 대하여 자세히 살펴보도록 한다.

[0039] 도 2는 본 발명의 다른 실시 예에 따른 영상의 부분 암호화 및 복호화 방법의 순서도이다.

[0040] 도 2에 도시된 바와 같이, 본 발명의 영상의 부분 암호화 및 복호화 방법은 먼저, 송신단(120)의 인코딩부(122)가 암호화하고자 하는 영상프레임에 대한 인코딩을 수행하여 압축데이터를 생성하면, 상기 송신단(120)의 제1헤더분석부(124)가 압축데이터로 이루어진 상기 영상프레임의 각 슬라이스별로 상기 슬라이스에 포함된 헤더데이터를 분석한다(S210).

[0041] 예를 들어, 상기 제1헤더분석부(124)가 상기 슬라이스의 압축데이터 중 '00 00 01 0X'의 헥사코드로 이루어진 압축데이터를 헤더데이터로 판단하고, 이에 따라 상기 슬라이스 내 헤더정보를 갖는 헤더데이터와 영상정보를 갖는 슬라이스데이터를 용이하게 구분할 수 있도록 한다.

[0042] 이어서, 상기 송신단(120)의 암호화부(126)가 상기 영상프레임 내 상기 헤더데이터를 제외한 나머지 슬라이스데이터 중 일부 슬라이스데이터를 암호화한다(S220). 이 때, 상기 암호화부(126)는 상기 슬라이스 내 상기 헤더데이터와 연속하는 적어도 하나의 슬라이스데이터 즉, 상기 슬라이스 내 상기 헤더데이터 이후 첫 번째 슬라이스데이터부터 이후 16 Byte에 해당하는 슬라이스데이터까지 일부 슬라이스데이터를 암호화하는 것이 바람직하다. 또한, 상기 암호화부(126)가 상기 슬라이스데이터의 암호화를 위해 AES암호화를 수행함에 따라, 상기 AES암호화 수행 시 필요한 최소 데이터 크기인 16 Bytes 크기의 슬라이스데이터를 암호화하는 것이 바람직하다.

[0043] 이와 같이, 슬라이스 내 일부 암호화된 슬라이스데이터를 포함하는 영상프레임을 상기 송신단(120)의 전송부

(128)가 수신단(140)으로 전송한다(S230).

[0044] 이후, 상기 송신단(120)으로부터 일정거리 이상 떨어진 곳에 위치하는 수신단(140)의 수신부(142)가 상기 송신단(120)으로부터 전송된 상기 영상프레임을 수신하면, 상기 수신단(140)의 제2헤더분석부(144)가 수신한 상기 영상프레임으로부터 헤더데이터를 분석한다(S240).

[0045] 이러한, 상기 제2헤더분석부(144)가 상기 송신단(120)의 상기 제1헤더분석부(124)와 마찬가지로, 수신한 상기 영상프레임의 슬라이스 중 '00 00 01 0X'의 헥사코드로 이루어진 압축데이터를 헤더데이터로 분석함에 따라 상기 슬라이스 내 헤더데이터와 슬라이스데이터가 용이하게 구분될 수 있다.

[0046] 이후, 상기 수신단(140)의 복호화부(146)가 상기 슬라이스 내 헤더데이터를 제외한 나머지 슬라이스데이터 중 일부 슬라이스데이터에 대하여 미리 설정되어 인증이 완료된 복호화키를 이용해 복호화한다(S250). 이 때, 상기 복호화부(146)는 상기 슬라이스의 헤더데이터 이후의 데이터 즉, 상기 슬라이스데이터 중 첫 번째 슬라이스데이터부터 이후 16 Byte 크기에 해당하는 슬라이스데이터까지를 복호화하는 것이 바람직하다.

[0047] 이어서, 상기 S250의 복호화 과정 시 이용된 복호화키가 미리 설정되어 인증된 복호화키인지 여부를 확인한다(S260).

[0048] 만약, 상기 S250의 복호화 과정 시, 기설정되어 인증이 완료된 복호화키를 이용하여 복호화를 수행한 경우, 복호화된 영상프레임에 대해 디코딩 과정을 수행하여 암호화가 일어나기 전 원본상태의 영상프레임을 획득한다(S270).

[0049] 하지만 이와 달리, 상기 S250의 복호화 과정 시, 인증된 복호화키가 아닌 그외의 다른 복호화키를 사용하여 복호화를 수행한 경우, 복호화된 영상프레임에 대하여 디코딩 과정을 수행하더라도 암호화 전 원본상태를 갖는 영상프레임이 아닌 내부 정보보호가 이루어진 영상프레임이 획득된다(S280). 이는 슬라이스 내 일부 슬라이스데이터만이 암호화된 경우, 디코딩 과정에서 해당 슬라이스 내 암호화 되지 않은 모든 슬라이스데이터로 에러가 전파됨에 따라, 영상프레임의 내부 정보가 보호될 수 있다.

[0050] 이하, 도 3을 참조하여, 본 발명의 슬라이스데이터 내 에러전파과정에 대하여 자세히 살펴보도록 한다.

[0051] 도 3은 영상프레임 내부의 에러 전파과정을 나타낸 도면이다.

[0052] 도 3(a)에 도시된 바와 같이, 하나의 영상프레임은 매 행마다 서로 다른 복수 개의 슬라이스 형태로 나누어지는데, 이 때 각 슬라이스는 다시 헤더정보를 포함하는 슬라이스헤더와, 영상정보를 포함하는 슬라이스데이터로 이루어진다.

[0053] 이와 같은 각 슬라이스에 대하여, 상기 슬라이스 내부에 포함된 헤더데이터를 분석한 후, 분석된 헤더데이터 이후 첫 번째 슬라이스데이터부터 16 Byte에 해당하는 슬라이스데이터까지 일부 슬라이스데이터에 대한 암호화를 수행한다. 본 발명에서는 상기 슬라이스데이터를 암호화하기 위해, AES암호화방법을 사용하였으나, 상기 AES암호화방법 외에도 다양한 암호화방법을 통해서도 이루어지는 것은 당연하다.

[0054] 이처럼, 상기 헤더데이터와 연속하는 슬라이스데이터 즉, 상기 헤더데이터 이후 흑색으로 표시된 첫 번째 슬라이스데이터부터 16 Byte에 해당하는 슬라이스데이터까지 암호화하는 경우, 수신단에서 상기 슬라이스의 디코딩 시, 도3(b)에 도시된 바와 같이, 해당 슬라이스의 내부에 포함되는 모든 슬라이스데이터에 에러가 전파된다.

[0055] 이하에서는 도 4를 참조하여, 상술한 도 3의 슬라이스데이터의 에러전파과정을 실제 이미지영상에 적용한 실험에 대하여 설명하고자 한다.

[0056] 도 4(a)는 영상프레임 내 헤더데이터 이후의 첫 번째 슬라이스데이터로부터 일부 슬라이스 데이터를 암호화한 결과를 나타낸 영상이고, 도 4(b)는 영상프레임 내 헤더데이터 이후의 중간 슬라이스데이터부터 일부 슬라이스데이터를 암호화한 결과를 나타낸 영상이다.

[0057] 도 4(a)에 도시된 바와 같이, 영상프레임의 슬라이스 내 분석한 헤더데이터와 연속하는 첫 번째 슬라이스데이터로부터 16 Byte의 슬라이스데이터만을 암호화한 것으로, 이러한 슬라이스데이터를 복호화하여 디코딩한 경우, 영상의 처음부분부터 영상의 정보보호가 이루어지는 것을 알 수 있다.

[0058] 하지만 이와 달리, 도 4(b)에 도시된 바와 같이, 영상프레임의 슬라이스 내 헤더데이터를 분석한 후, 상기 헤더데이터와 연속하는 슬라이스데이터 즉, 상기 헤더데이터 이후 첫 번째 슬라이스데이터가 아닌 중간 슬라이스데이터부터 이후 16 Byte에 해당하는 슬라이스데이터만을 암호화한 경우, 영상이 중간 이후부터 데이터의 정보보

호가 이루어지는 것을 알 수 있다.

[0059] 이러한 결과를 통해 알 수 있듯이, 영상프레임의 슬라이스 내 헤더데이터 이후의 첫 번째 슬라이스데이터부터 일부 슬라이스데이터를 암호화하는 경우, 영상 전체에 대한 정보보호가 용이하게 이루어지는 것을 알 수 있다.

[0060] 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 영상프레임을 구성하는 각 슬라이스에 대한 헤더데이터를 분석한 후, 상기 헤더데이터 이후의 슬라이스데이터 일부만을 암호화함으로써, 상기 영상프레임에 대한 암호화시간을 감소시키는 효과가 있다.

[0061] 또한, 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 영상프레임을 구성하는 슬라이스 중 영상정보를 포함하는 슬라이스데이터 중 일부 슬라이스데이터만을 암호화하여 암호화 수행시간이 감소됨에 따라, 상기 영상프레임에 대한 실시간 암호화를 수행할 수 있는 효과가 있다.

[0062] 더불어, 본 발명의 영상의 부분 암호화 및 복호화 시스템 및 방법은 인증이 완료되지 않은 복호화키를 이용하여 암호화된 영상프레임을 복호화하는 경우, 상기 영상프레임의 전체에 대한 정보보호가 이루어짐에 따라, 인증이 완료된 복호화키를 갖는 허용된 사용자 즉, 수신단이 상기 영상프레임에 대한 복호화를 수행하여, 원본 영상프레임을 획득할 수 있으므로, 데이터 정보보호의 신뢰성을 향상시킬 수 있는 효과가 있다.

[0063] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

[0064] 120: 송신단 122: 인코딩부

124: 제1헤더분석부 126: 암호화부

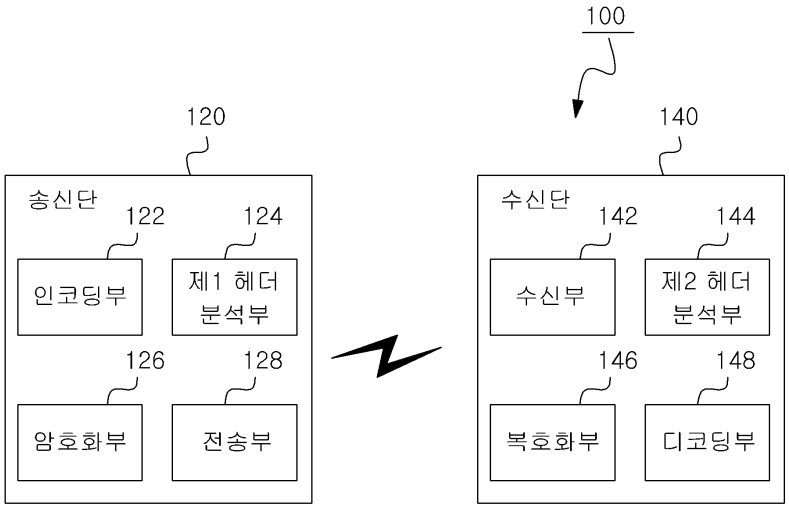
128: 전송부 140: 수신단

142: 수신부 144: 제2헤더분석부

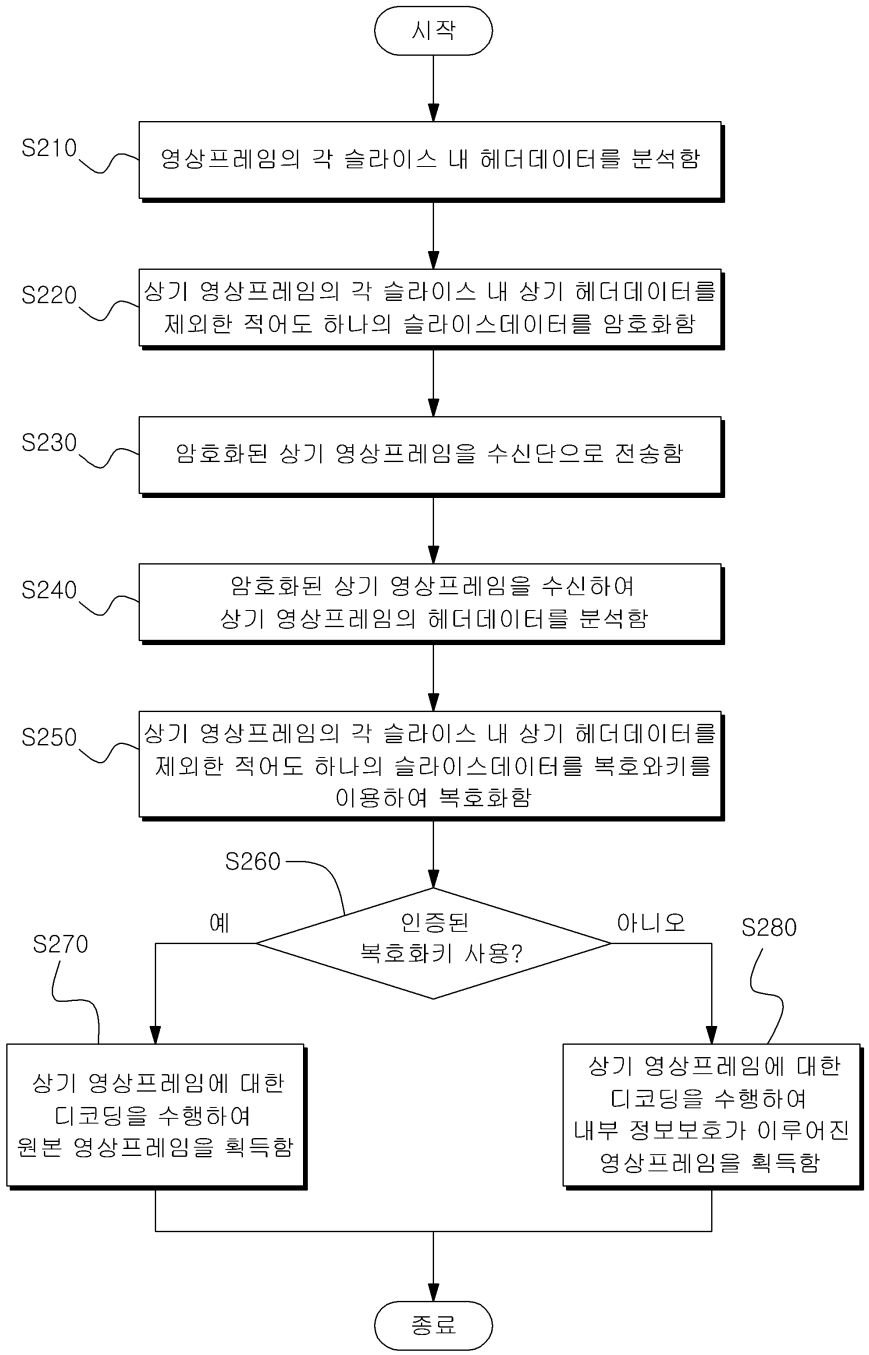
146: 복호화부 148: 디코딩부

도면

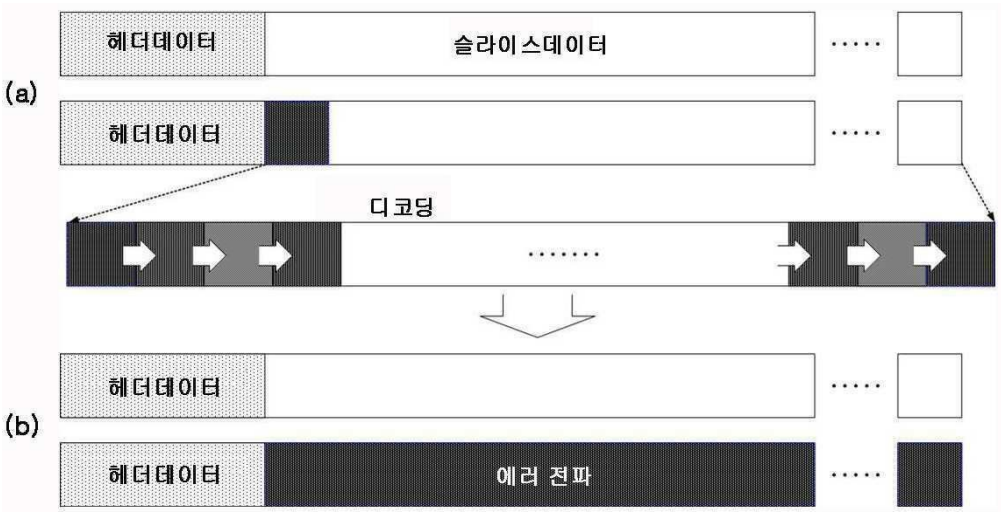
도면1



도면2


시작
S210
영상프레임의 각 슬라이스 내 헤더데이터를 분석함
S220
상기 영상프레임의 각 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 암호화함
S230
암호화된 상기 영상프레임을 수신단으로 전송함
S240
암호화된 상기 영상프레임을 수신하여 상기 영상프레임의 헤더데이터를 분석함
S250
상기 영상프레임의 각 슬라이스 내 상기 헤더데이터를 제외한 적어도 하나의 슬라이스데이터를 복호와키를 이용하여 복호화함
S260
인증된 복호화키 사용?
예
아니오
S270
상기 영상프레임에 대한 디코딩을 수행하여 원본 영상프레임을 획득함
S280
상기 영상프레임에 대한 디코딩을 수행하여 내부 정보보호가 이루어진 영상프레임을 획득함
종료

도면3



도면4

