(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년04월19일
(11) 등록번호 10-1029969
(24) 등록일자 2011년04월12일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 9/06* (2006.01)
G06F 17/00 (2006.01)
(21) 출원번호 10-2009-0131262
(22) 출원일자 2009년12월24일
심사청구일자 2009년12월24일
(56) 선행기술조사문헌
KR1020110019694 A
정보보호학회논문지, 제20권제3호, pp.113-120, 2010.06.
정보과학회논문지: 컴퓨팅의 실제 및 레터, 제16권제8호, pp.863-867 (2010.08)
KR1020050107535 A
전체 청구항 수 : 총 11 항

(73) 특허권자
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정용화
대전 유성구 지족동 877 열매마을아파트 505동 402호
이성주
서울 마포구 성산동 47-14
(뒷면에 계속)
(74) 대리인
특허법인충현

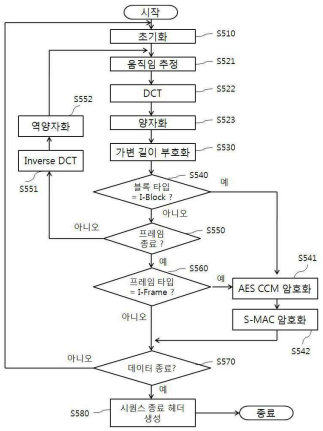
심사관 : 경연정

(54) 멀티미디어 데이터의 선택적 암호화 장치 및 방법, 멀티미디어 데이터 검증 방법, 및 그 기록 매체

(57) 요 약

멀티미디어 데이터의 선택적 암호화 장치 및 방법, 멀티미디어 데이터 검증 방법, 및 그 기록 매체가 개시된다. 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 장치는 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정하여 움직임 벡터를 생성하는 움직임 추정부; 상기 움직임 벡터를 가변 길이 부호화하는 가변 길이 부호화부; 상기 가변 길이 부호화부에서 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하고, 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 선택적 암호화부; 및 상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 시퀀스 종료 헤더 생성부를 포함한다. 본 발명의 실시 예들에 의하면, AES-CCM을 이용하여 대용량 멀티미디어 데이터의 비밀성과 무결성을 동시에 보장할 수 있을 뿐만 아니라, 암호화의 효율을 향상시키고, 데이터의 위변조 여부를 데이터 크기와 상관없이 간단하게 확인할 수 있다.

대 표 도 - 도5



(72) 발명자

홍승우

서울특별시 강남구 삼성동 상아아파트 2차 3동 1012호

최한나

서울특별시 강서구 화곡8동 394-18 해풍맨션 203호

이은지

경상북도 경산시 정평동 130 현대타운 106-602

특허청구의 범위

청구항 1

멀티미디어 데이터의 프레임의 블록마다 움직임을 추정하여 움직임 벡터를 생성하는 움직임 추정부;

상기 움직임 벡터를 가변 길이 부호화하는 가변 길이 부호화부;

상기 가변 길이 부호화부에서 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하고, 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 선택적 암호화부; 및

상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 시퀀스 종료 헤더 생성부를 포함하는, 멀티미디어 데이터의 선택적 암호화 장치.

청구항 2

제 1 항에 있어서,

상기 선택적 암호화부는

상기 AES-CCM 알고리즘에 의한 암호화를 통해 생성되는 S-MAC을 암호화하는 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 장치.

청구항 3

제 2 항에 있어서,

상기 선택적 암호화부는

상기 S-MAC을 암호화하여 V-MAC을 생성하는 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 장치.

청구항 4

제 1 항에 있어서,

상기 움직임 추정부는

블록마다 상기 움직임 벡터를 이산 코사인 변환하고 양자화하는 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 장치.

청구항 5

멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계;

마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계; 및

상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계를 포함하는, 멀티미디어 데이터의 선택적 암호화 방법.

청구항 6

제 5 항에 있어서,

상기 매크로 블록을 암호화하는 단계 및 상기 해당 프레임을 암호화하는 단계는

상기 AES-CCM 알고리즘에 의한 암호화를 통해 생성되는 S-MAC을 암호화하는 단계를 포함하는 단계를 포함하는 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 방법.

청구항 7

제 6 항에 있어서,

상기 S-MAC을 암호화하는 단계는

상기 S-MAC을 암호화하여 V-MAC을 생성하는 단계인 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 방법.

청구항 8

제 5 항에 있어서,

상기 매크로 블록을 암호화하는 단계는

블록마다 움직임을 추정하여 움직임 벡터를 생성하며 상기 움직임 벡터를 이산 코사인 변환하고 양자화하는 단계를 포함하는 것을 특징으로 하는, 멀티미디어 데이터의 선택적 암호화 방법.

청구항 9

멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계;

마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계;

상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계;

검증할 데이터를 디코딩하여 생성된 S-MAC을 암호화하여 검증용 V-MAC을 생성하는 단계; 및

상기 암호화된 데이터의 V-MAC과 상기 검증용 V-MAC을 비교하여 상기 검증할 데이터의 무결성을 판단하는 단계를 포함하는, 멀티미디어 데이터 검증 방법.

청구항 10

멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계;

마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계;

상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계;

검증할 데이터를 디코딩하여 검증용 S-MAC을 생성하는 단계; 및

상기 암호화된 데이터를 디코딩하여 생성된 S-MAC을 상기 검증용 S-MAC을 비교하여 상기 검증할 데이터의 무결성을 판단하는 단계를 포함하는, 멀티미디어 데이터 검증 방법.

청구항 11

제5항 내지 제10항 중 어느 한 항의 방법을 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된, 컴퓨터 시스템이 판독할 수 있는 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 대용량 멀티미디어 데이터의 구조적인 특성에 관한 것으로, 특히, 멀티미디어 데이터의 선택적 암호화 장치 및 방법, 멀티미디어 데이터 검증 방법, 및 그 기록 매체에 관한 것이다.

배 경 기 술

[0002] 최근 MPEG 비디오 스트림 등 대용량 데이터 이용이 증가함에 따라, 이러한 대용량 데이터에 대한 정보 보호 문

제가 이슈화되고 있다. 특히, 데이터의 기밀성을 보장하는 방법 외에 HMAC(Keyed-Hash Message Authentication Code) 등과 같은 메시지 인증 기법을 추가적으로 적용할 필요가 있다. 즉, 메시지 인증을 할 수 있는 암호화 알고리즘을 적용하여 대용량 데이터의 무결성을 동시에 보장해야 한다.

[0003] 대용량 데이터의 무결성 보장을 실시간으로 수행하기 위해 멀티미디어 콘텐츠의 압축과 보호가 밀결합(tightly-coupled)되고, 다양한 장치에서 이용 가능한 SECMPEG(Secure MPEG) 보안레벨 3를 적용할 수 있다. SECMPEG는 여러 분야에서 응용되는 MPEG-2 인코더에 대용량 멀티미디어 콘텐츠의 보호와 성능을 동시에 고려한 선택적 암호화 방식이다. 또한, 위변조를 방지하기 위하여 AES(Advanced Encryption Standard) 기반의 운용모드인 CCM(Counter with CBC-MAC)을 적용하여 메시지 무결성을 보장한다.

[0004] CCM은 주로 대칭키 암호화 기법인 AES와 함께 이용되고 있으며, AES-CCM은 암/복호화 하는데 수행속도가 빠르고, 한번의 수행만으로 기밀성과 메시지의 무결성을 동시에 보장할 수 있는 특성을 갖는다. 따라서, SECMPEG 보안레벨 3에 CCM을 적용한다면, 단 한차례의 수행만으로 대용량 멀티미디어 데이터의 기밀성과 무결성을 동시에 보장할 수 있다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명이 이루고자 하는 첫 번째 기술적 과제는 대용량의 멀티미디어 데이터의 빠른 암호화 및 효율적인 보호를 위해 AES-CCM 알고리즘을 적용하여 비밀성뿐만 아니라 무결성까지 보장할 수 있는 멀티미디어 데이터의 선택적 암호화 장치를 제공하는 데 있다.

[0006] 본 발명이 이루고자 하는 두 번째 기술적 과제는 상기의 멀티미디어 데이터의 선택적 암호화 장치에 적용되는 멀티미디어 데이터의 선택적 암호화 방법을 제공하는 데 있다.

[0007] 본 발명이 이루고자 하는 세 번째 기술적 과제는 상기 멀티미디어 데이터의 선택적 암호화 방법을 적용하여 생성된 데이터를 이용하여 멀티미디어 데이터의 무결성을 검증하는 멀티미디어 데이터 검증 방법을 제공하는 데 있다.

[0008] 본 발명이 이루고자 하는 네 번째 기술적 과제는 상기 멀티미디어 데이터의 선택적 암호화 방법 및 멀티미디어 데이터 검증 방법을 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된 매체로서, 컴퓨터 시스템이 판독할 수 있는 기록매체를 제공하는 데 있다.

과제 해결수단

[0009] 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 장치는 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정하여 움직임 벡터를 생성하는 움직임 추정부; 상기 움직임 벡터를 가변 길이 부호화하는 가변 길이 부호화부; 상기 가변 길이 부호화부에서 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하고, 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 선택적 암호화부; 및 상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 시퀀스 종료 헤더 생성부를 포함한다.

[0010] 한편, 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법은 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계; 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계; 및 상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계를 포함한다.

[0011] 또한, 본 발명의 일 실시 예에 따른 멀티미디어 데이터 검증 방법은 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계; 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계; 상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계; 검증할 데이터를 디코딩하여 생성된 S-MAC을 암호화하여 검증용 V-MAC을 생성하는 단계; 및 상기 암호화된 데이터의 V-

MAC과 상기 검증용 V-MAC을 비교하여 상기 검증할 데이터의 무결성을 판단하는 단계를 한다.

[0012] 또한, 본 발명의 다른 실시 예에 따른 멀티미디어 데이터 검증 방법은 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정한 후 가변 길이 부호화를 수행하면서, 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화하는 단계; 마지막 매크로 블록까지 상기 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우, 상기 해당 프레임을 AES-CCM 알고리즘을 통해 암호화하는 단계; 상기 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를 부가하여 암호화된 데이터를 생성하는 단계; 검증할 데이터를 디코딩하여 검증용 S-MAC을 생성하는 단계; 및 상기 암호화된 데이터를 디코딩하여 생성된 S-MAC을 상기 검증용 S-MAC을 비교하여 상기 검증할 데이터의 무결성을 판단하는 단계를 포함한다.

효 과

[0013] 본 발명의 실시 예들에 의하면, AES-CCM을 이용하여 대용량 멀티미디어 데이터의 비밀성과 무결성을 동시에 보장할 수 있을 뿐만 아니라, 암호화의 효율을 향상시키고, 데이터의 위변조 여부를 데이터 크기와 상관없이 간단하게 확인할 수 있다.

발명의 실시를 위한 구체적인 내용

[0014] 이하에서는 도면을 참조하여 본 발명의 바람직한 실시 예들을 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다.

[0015] 블록 암호화 알고리즘은 데이터를 일정한 크기의 블록단위로 반복적으로 암호화 한다. 따라서 같은 데이터를 같은 키로 암호화하면 계속 같은 패턴의 데이터가 생성되는데 그것을 보안하기 위해 사용하는 것이 운용모드(Modes of Operation)이다. 미국 국가기술표준국(NIST)에서는 5가지 운용모드를 표준으로 제안하고 있다.

[0016] 도 1a는 운용모드 중 CTR(Counter mode)의 과정을 나타낸다.

[0017] 이 과정은 임의의 수(Nonce)와 카운터(Counter)를 일정한 값으로 증가하여 암호화에 사용하기 때문에 블록 암호를 스트림 암호처럼 사용할 수 있게 해준다. 키와 수, 카운터를 암호화하여 평문(Plain Text)과 XOR 연산을 하여 암호화한다.

[0018] 도 1b는 운용모드 중 CBC(Chaining Block Cipher)의 과정을 나타낸다.

[0019] 이 과정은 CBC-MAC으로 무결성을 보장하는 방법으로 사용된다. CBC의 수행으로 생성된 마지막 블록(Result)를 메시지의 무결성을 인증하는 코드인 MAC으로 사용하는 방법이다. CBC는 블록 암호화의 약점인 데이터 사이의 독립성을 제거해 주기 때문에 일부 데이터가 변조되었을 때 나머지 데이터들도 복호화 할 수 없다. 즉, CBC의 마지막 블록을 MAC으로 사용하면 데이터의 무결성을 보장할 수 있다.

[0020] 도 1c는 운용모드인 CCM(Counter with CBC-MAC)의 AES를 이용한 블록 다이어그램이다. 위쪽의 CBC 운용모드(110)는 도 1b의 CBC-MAC과 같고 무결성 보장을 위해 생성하는 MAC을 생성하는데 사용된다. 아래쪽의 CTR 운용모드(120)는 도 1a의 CTR과 같고 평문을 암호화 한다. MAC 생성(130)은 위쪽 CBC-MAC에서 생성된 마지막 블록2의 암호화된 데이터(111)와 아래쪽 CTR의 첫 번째 Ctr0를 암호화한 데이터(121)를 XOR 연산을 통해 만들어 낸다.

[0021] 도 2는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 장치의 블록도이다.

[0022] 움직임 추정부(220)는 멀티미디어 데이터의 프레임의 블록마다 움직임을 추정하여 움직임 벡터를 생성한다. 움직임 추정부(220)는 블록마다 움직임 벡터를 이산 코사인 변환하고 양자화한다.

[0023] 가변 길이 부호화부(230)는 상기 움직임 추정부(220)의 움직임 벡터를 가변 길이 부호화한다.

[0024] 선택적 암호화부(240)는 가변 길이 부호화부(220)에서 매크로 블록이 I-블록인 경우 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화한다. 또한, 선택적 암호화부(240)는 마지막 매크로 블록까지 가변 길이 부호화가 완료되고 해당 프레임이 I-프레임인 경우 해당 프레임을 AES-CCM 알고리즘을 통해 암호화한다. 선택적 암호화부(240)는 AES-CCM 알고리즘에 의한 암호화를 통해 생성되는 S-MAC을 암호화한다. 보다 구체적으로, 선택적 암호화부(240)는 S-MAC을 암호화하여 V-MAC을 생성할 수 있다.

[0025] 시퀀스 종료 헤더 생성부(280)는 멀티미디어 데이터에 대한 가변 길이 부호화가 완료되면, 시퀀스 종료 헤더를

부가하여 암호화된 데이터를 생성한다.

[0026] 도 3은 멀티미디어 데이터용 AES-CCM 알고리즘을 적용하는 방법과 데이터 전체의 위변조를 검증하는 방법을 각각 도시한 것이다.

[0027] 도 3의 왼쪽은 멀티미디어 데이터에 AES-CCM 알고리즘을 적용하여 메시지 인증을 위한 V-MAC과 S-MAC을 생성하는 과정이다. V-MAC은 비디오 무결성을 위한 비디오 맥(Video MAC)으로서, 멀티미디어 데이터의 전체적인 무결성을 검증하는데 사용된다. S-MAC은 선택적으로 암호화되는 부분 데이터 각각의 스몰 맥(small MAC)으로서, 전체 동영상 중 변조된 부분을 찾는데 사용된다. 인코딩할 때 생성된 S-MAC의 암호문(S-MAC Cipher)과 V-MAC은 MPEG-2 데이터와 함께 저장된다.

[0028] 도 3의 오른쪽은 검증할 데이터를 이용하여 검증용 V-MAC(도 3의 V-MAC2)을 생성하는 과정을 보여준다.

[0029] 구체적으로, 도 3의 오른쪽은 전체 데이터의 위변조 확인을 위해 멀티미디어 데이터 전체를 복호화하여 생성한 S-MAC을 암호화하여 V-MAC을 생성함으로써 전체 데이터의 무결성을 검증하는 방법이다. 예를 들어, 검증을 필요로 하는 MPEG-2 데이터의 디코딩 결과로 만들어지는 S-MAC을 이용하여 인코딩과 같은 방법으로 V-MAC을 생성한다.

[0030] 본 발명의 일 실시 예에 따른 멀티미디어 데이터 검증 방법에서는 도 2에서 생성된 암호화된 데이터의 V-MAC과 도 3의 검증용 V-MAC을 비교하여 상기 검증할 데이터의 무결성을 판단한다. 데이터 전체의 무결성 검증이 필요로 할 때, V-MAC만 사용함으로써, 각각의 S-MAC을 사용할 때보다 오버헤드를 줄일 수 있다.

[0031] 도 4는 멀티미디어 데이터용 AES-CCM 알고리즘을 적용하는 방법과 데이터 특정 부분의 위변조를 검증하는 방법을 각각 도시한 것이다.

[0032] 부분적인 무결성 검증이 필요한 경우 S-MAC 사이의 무결성을 V-MAC이 보장해 주므로, 선택적으로 암호화해서 만들어진 검증용 S-MAC(도 4의 S-MAC')을 S-MAC 암호문을 복호화한 S-MAC과 비교하여 무결성을 검증할 수도 있다. 즉, 검증용 S-MAC은 부분 데이터의 위변조 확인을 위해 멀티미디어 데이터 전체를 암호화한 암호문을 복호화하여 생성된다.

[0033] 본 발명의 다른 실시 예에 따른 멀티미디어 데이터 검증 방법에서는 검증할 데이터를 디코딩하여 검증용 S-MAC을 생성한 후, 도 2에서 생성된 암호화된 데이터를 디코딩하여 S-MAC을 생성하고, 상기 검증용 S-MAC을 비교하여 검증할 데이터의 무결성을 판단한다.

[0034] 도 5는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법의 흐름도이다.

[0035] 멀티미디어 데이터는 여러 프레임으로 구성되고, 각 프레임은 여러 블록으로 구분될 수 있다. 각 프레임에서 움직임 추정을 하기 위해서는 먼저, 초기화 과정을 수행한다(S510).

[0036] 다음, 하나의 프레임 내에서 각 블록마다 움직임을 추정한다(S521). 움직임 추정의 결과로 움직임 벡터를 생성할 수 있다. 움직임 벡터가 생성되면, 이를 이산 코사인 변환(DCT)하고(S522), 양자화한다(S523).

[0037] 가변 길이 부호화(Variable Length Coding)는 양자화의 결과에 대해 수행되는데(S530), 가변 길이 부호화를 통해 각 매크로(Macro) 블록이 I타입의 블록(I-블록)인지를 확인할 수 있다.

[0038] 매크로 블록이 I-블록인 경우(S540) 상기 매크로 블록을 AES-CCM 알고리즘을 통해 암호화한다(S541). I-블록은 AES-CCM을 통해 선택적으로 암호화되는 것이다. 본 발명의 일 실시 예에서, 이 과정(S541)에 더하여 AES-CCM 알고리즘에 의한 암호화를 통해 생성되는 S-MAC을 암호화하는 과정(S542)을 더 수행할 수도 있다. S-MAC을 암호화하는 과정(S542)에서는 S-MAC을 한번 더 암호화하여 V-MAC을 생성하는 과정이 이루어질 수 있다.

[0039] 하나의 블록에 대해 가변 길이 부호화가 완료될 때마다 역 이산 코사인 변환(S551)과 역양자화 과정(S552)이 이어진다.

[0040] 한 프레임의 마지막 블록까지 인코딩이 끝날 때마다(S550) 그 프레임이 I-프레임인지 확인(S560)하고, I-프레임이라면 AES-CCM 알고리즘을 통해 암호화 한다(S541). 본 발명의 일 실시 예에서, 이 과정(S541)에 더하여 AES-CCM 알고리즘에 의한 암호화를 통해 생성되는 S-MAC을 암호화하는 과정(S542)을 더 수행할 수도 있다. S-MAC을 암호화하는 과정(S542)에서는 S-MAC을 한번 더 암호화하여 V-MAC을 생성하는 과정이 이루어질 수 있다.

[0041] 멀티미디어 데이터에 대한 가변 길이 부호화 등의 인코딩 과정이 완료되면(S570), 시퀀스 종료 헤더를 생성하고

(S580) 시퀀스 종료 헤더를 위에서 생성된 V-MAC 등의 데이터에 부가하여 암호화된 데이터를 생성한다.

[0042] 도 5에 따르면, MPEG-2 인코더의 SECMPEG의 보안레벨 3은 전체 데이터를 모두 암호화하지 않고, I-블록과 I-프레임만을 선택적으로 암호화함으로써 수행속도를 향상시킬 수 있다.

[0043] 도 6a는 멀티미디어 데이터 전체를 암호화 하는 방법에 따라 생성된 데이터의 예를 도시한 것이다.

[0044] 도 6b는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법에 따라 생성된 데이터의 예를 도시한 것이다. 구체적으로, 도 6b는 부분 암호화 SECMPEG에 AES-CCM을 사용하여 추가적인 MAC을 생성한 예를 보여준다.

[0045] 도 7는 멀티미디어 데이터 전체를 암호화 하는 방법과 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법의 수행 시간을 데이터의 량에 따라 비교한 그래프이다.

[0046] 본 발명에서 제안된 방법은 동영상의 전체를 암호화하지 않고 I-블록과 I-프레임만을 암호화 하여 수행 시간을 단축한다. 또한, 메시지 인증을 위해서 CCM 운용모드를 I-블록과 I-프레임에만 적용함으로써 MAC을 생성할 때 필요한 오버헤드를 최소화 시킬 수 있다.

[0047] 본 발명의 실시 예들을 MPEG-2에 적용하는 경우, MPEG-2의 인코딩 특성과 AES-CCM의 암호화 특성을 분석하고 MPEG-2의 중요 프레임을 각각 AES-CCM으로 암호화한 후 무결성을 위한 MAC을 추가적으로 AES-CCM으로 암호화하게 된다.

[0048] 본 발명은 소프트웨어를 통해 실행될 수 있다. 바람직하게는, 본 발명의 실시 예들에 따른 멀티미디어 데이터의 선택적 암호화 방법 및 멀티미디어 데이터 검증 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

[0049] 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0050] 본 발명은 도면에 도시된 일 실시 예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시 예의 변형이 가능하다는 점을 이해할 것이다. 그리고, 이와 같은 변형은 본 발명의 기술적 보호범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

산업이용 가능성

[0051] 본 발명의 실시 예들은 AES-CCM을 이용하여 대용량 멀티미디어 데이터의 비밀성과 무결성을 동시에 보장할 수 있을 뿐만 아니라, 암호화의 효율을 향상시키고, 데이터의 위변조 여부를 데이터 크기와 상관없이 간단하게 확인할 수 있는 것으로, 동영상 인코더, 디코더 등의 멀티미디어 관련 분야에 적용될 수 있다.

도면의 간단한 설명

[0052] 도 1a 및 1b는 AES-CCM을 구성하는 블록 암호 운용모드인 CBC모드와 CTR모드를 도시한 것이다.

[0053] 도 1c는 블록 암호 운용모드인 CBC모드와 CTR모드를 혼용한 AES-CCM를 도시한 것이다.

[0054] 도 2는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 장치의 블록도이다.

[0055] 도 3은 멀티미디어 데이터용 AES-CCM 알고리즘을 적용하는 방법과 데이터 전체의 위변조를 검증하는 방법을 각각 도시한 것이다.

[0056] 도 4는 멀티미디어 데이터용 AES-CCM 알고리즘을 적용하는 방법과 데이터 특정 부분의 위변조를 검증하는 방법을 각각 도시한 것이다.

[0057] 도 5는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법의 흐름도이다.

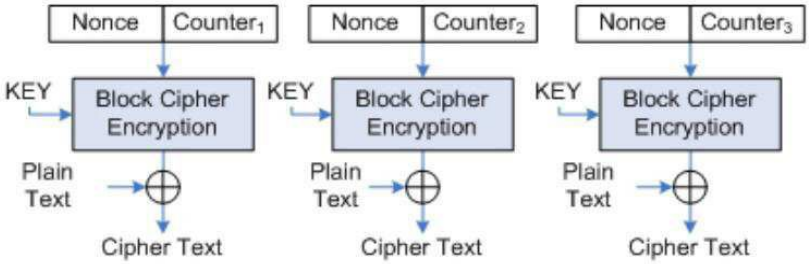
[0058] 도 6a는 멀티미디어 데이터 전체를 암호화 하는 방법에 따라 생성된 데이터의 예를 도시한 것이다.

[0059] 도 6b는 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법에 따라 생성된 데이터의 예를 도시한 것이다.

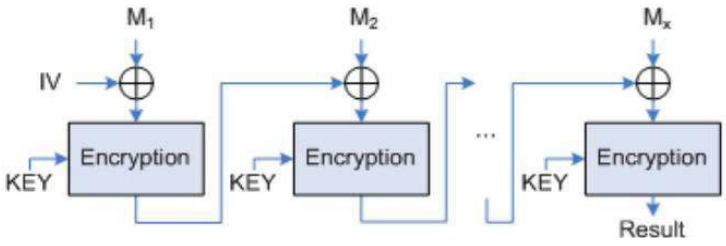
[0060] 도 7는 멀티미디어 데이터 전체를 암호화 하는 방법과 본 발명의 일 실시 예에 따른 멀티미디어 데이터의 선택적 암호화 방법의 수행 시간을 데이터의 량에 따라 비교한 그래프이다.

도면

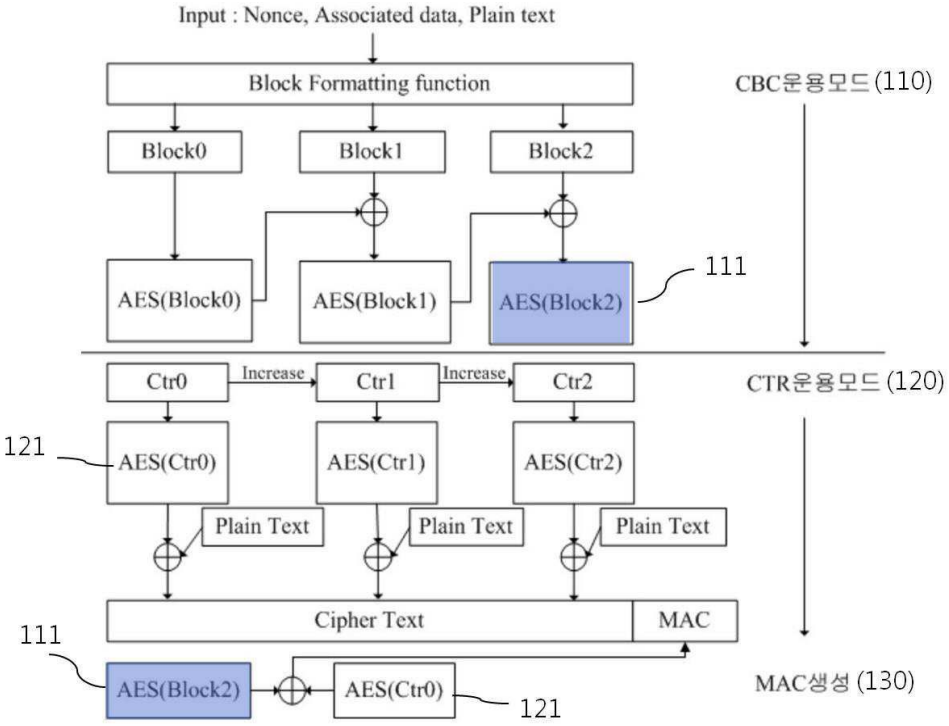
도면1a



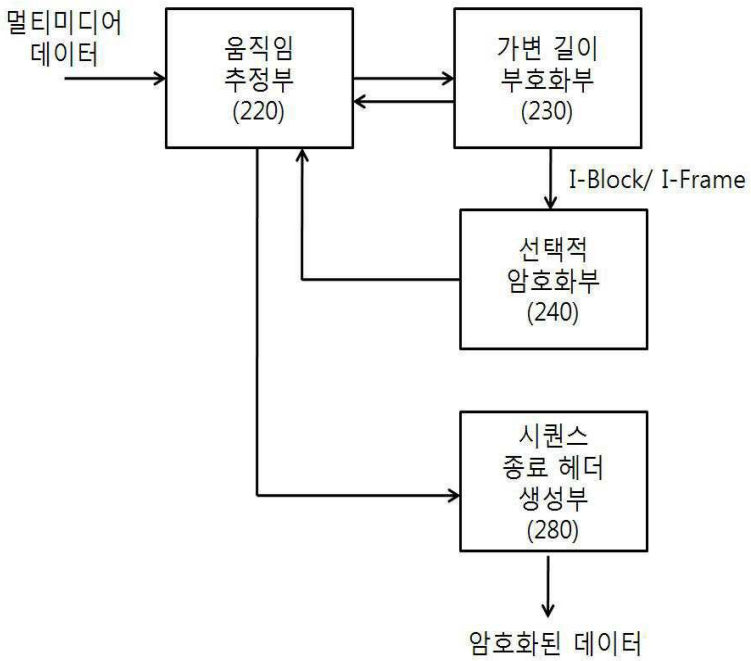
도면1b



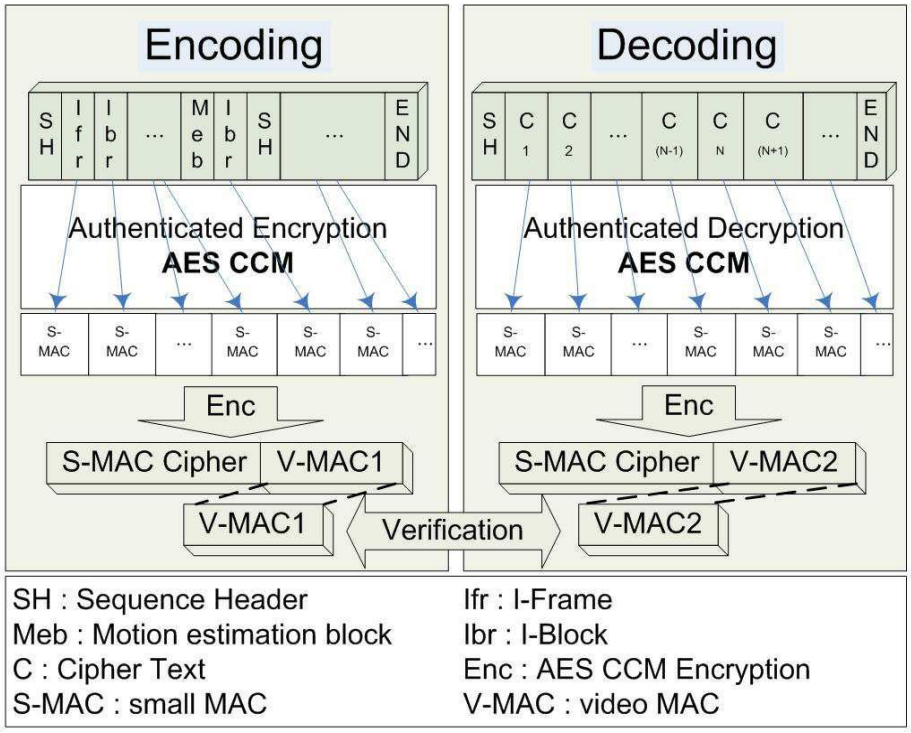
도면1c


Input : Nonce, Associated data, Plain text
Block Formatting function
CBC운용모드(110)
Block0
Block1
Block2
AES(Block0)
AES(Block1)
AES(Block2)
111
Ctr0
Increase
Ctr1
Increase
Ctr2
CTR운용모드(120)
121
AES(Ctr0)
AES(Ctr1)
AES(Ctr2)
Plain Text
Plain Text
Plain Text
Cipher Text
MAC
111
AES(Block2)
AES(Ctr0)
121
MAC생성(130)

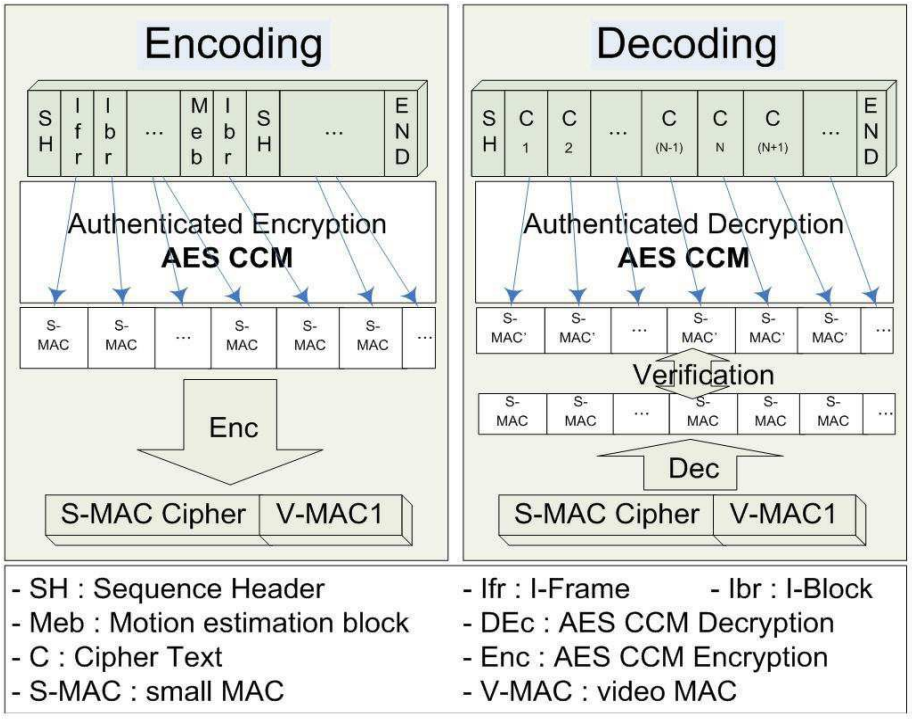
도면2


멀티미디어 데이터
움직임 추정부 (220)
가변 길이 부호화부 (230)
I-Block/ I-Frame
선택적 암호화부 (240)
시퀀스 종료 헤더 생성부 (280)
암호화된 데이터

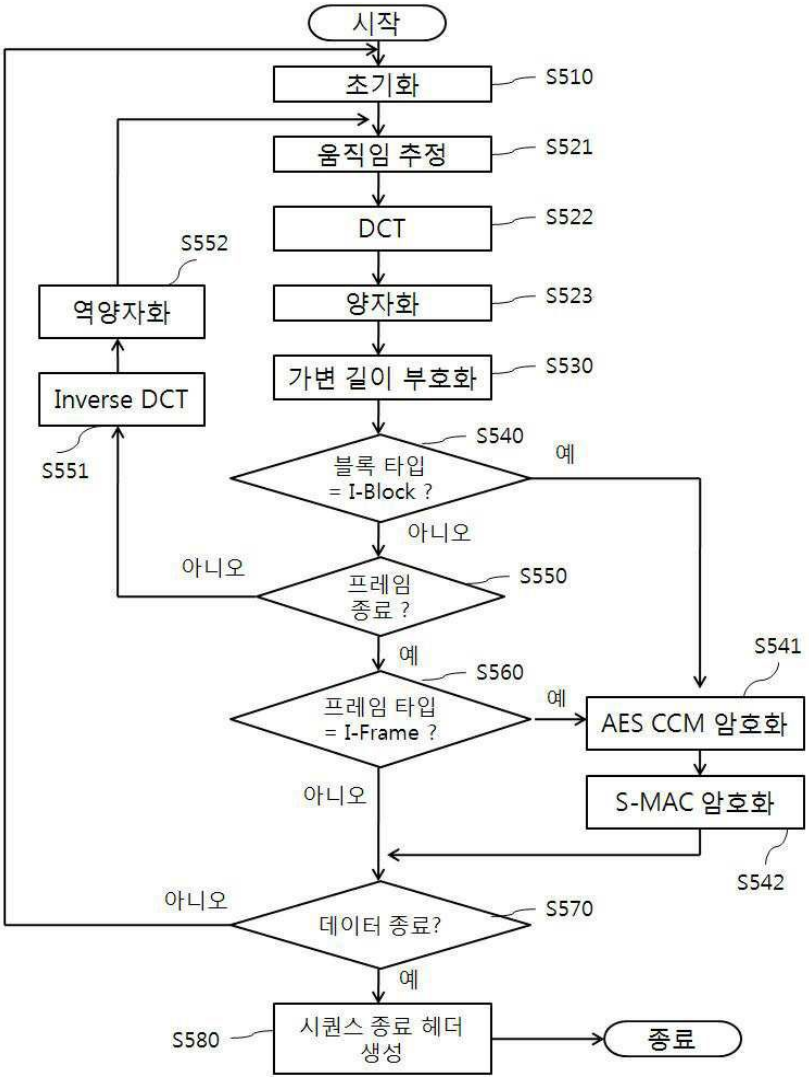
도면3


Encoding
Decoding
SH
Ifr
Ibr
...
Meb
Ibr
SH
...
END
SH
C 1
C 2
...
C (N-1)
C N
C (N+1)
...
END
Authenticated Encryption
AES CCM
Authenticated Decryption
AES CCM
S-MAC
Enc
S-MAC Cipher
V-MAC1
V-MAC2
Verification
SH : Sequence Header
Meb : Motion estimation block
C : Cipher Text
S-MAC : small MAC
Ifr : I-Frame
Ibr : I-Block
Enc : AES CCM Encryption
V-MAC : video MAC

도면4


Encoding
Decoding
SH
Ifr
Ibr
...
Meb
Ibr
SH
...
END
SH
C 1
C 2
...
C (N-1)
C N
C (N+1)
...
END
Authenticated Encryption
AES CCM
Authenticated Decryption
AES CCM
S-MAC
S-MAC'
Enc
Verification
Dec
S-MAC Cipher
V-MAC1
- SH : Sequence Header
- Meb : Motion estimation block
- C : Cipher Text
- S-MAC : small MAC
- Ifr : I-Frame
- Ibr : I-Block
- DEc : AES CCM Decryption
- Enc : AES CCM Encryption
- V-MAC : video MAC

도면5



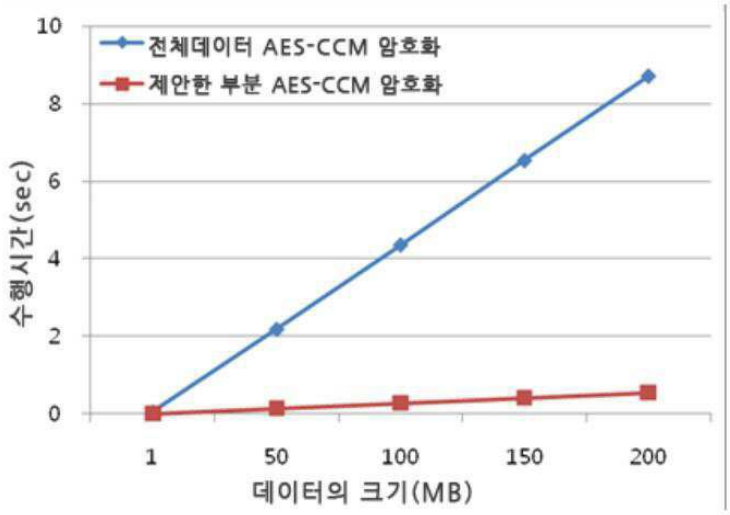
도면6a



도면6b



도면7


10
8
6
4
2
0
수행시간(sec)
전체데이터 AES-CCM 암호화
제안한 부분 AES-CCM 암호화
1
50
100
150
200
데이터의 크기(MB)