



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0053215
(43) 공개일자 2025년04월21일

- | | |
|--|--|
| <p>(51) 국제특허분류(Int. Cl.)
H04N 19/70 (2014.01) H04L 9/06 (2006.01)
H04L 9/40 (2022.01) H04N 19/46 (2014.01)
H04N 21/2347 (2016.01) H04N 21/235 (2011.01)
H04N 21/435 (2011.01) H04N 21/4405 (2016.01)</p> <p>(52) CPC특허분류
H04N 19/70 (2015.01)
H04L 63/0428 (2013.01)</p> <p>(21) 출원번호 10-2025-7011473(분할)</p> <p>(22) 출원일자(국제) 2015년08월07일
심사청구일자 없음</p> <p>(62) 원출원 특허 10-2023-7037532
원출원일자(국제) 2015년08월07일
심사청구일자 2023년11월30일</p> <p>(85) 번역문제출일자 2025년04월08일</p> <p>(86) 국제출원번호 PCT/US2015/044325</p> <p>(87) 국제공개번호 WO 2016/022979
국제공개일자 2016년02월11일</p> <p>(30) 우선권주장
62/034,714 2014년08월07일 미국(US)</p> | <p>(71) 출원인
디빅스, 엘엘씨
미국 캘리포니아 92122 샌디에이고 스위트 950 라
줄라 빌리지 드라이브 4350</p> <p>(72) 발명자
브라네스 제이슨
미국 캘리포니아주 92127 샌 디에고 사우스 세비
체이스 15659
아미데이 윌리엄 데이비드
미국 캘리포니아주 92192 샌 디에고 피오 박스
928365
스리니바산 메이유르
미국 캘리포니아주 92127 샌 디에고 웨인 힐
16064</p> <p>(74) 대리인
특허법인 광장리앤코</p> |
|--|--|

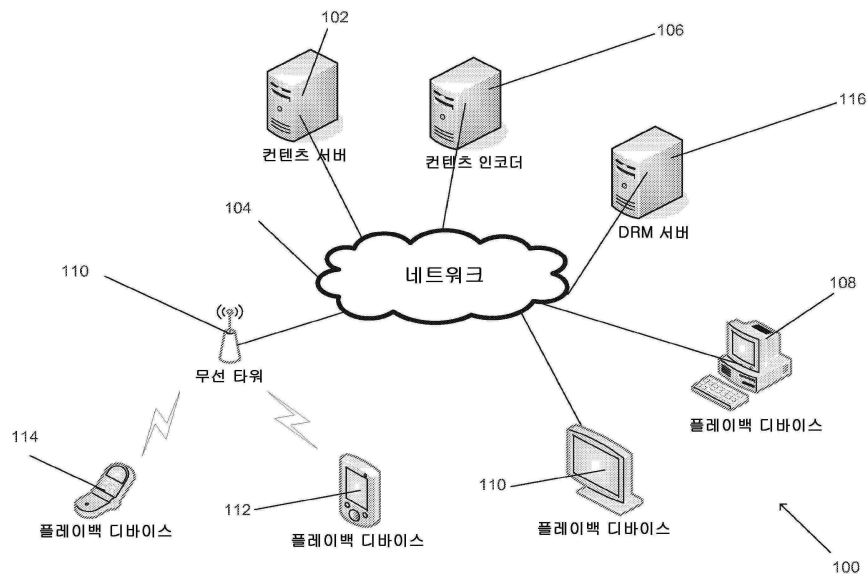
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 독립적으로 인코딩된 타일을 포함한 기본 비트스트림을 보호하는 시스템 및 방법

(57) 요약

본 발명의 실시형태에 따른 부분 프레임 암호화를 위한 시스템 및 방법이 개시된다. 일 실시형태에 있어서, 이 방법은 여러 프레임을 포함하는 비디오 비트스트림을 수신하고, 각 프레임은 그 프레임 내에 여러 개의 독립적으로 인코딩된 압축 단위를 포함하는 것이며, 상기 방법은 여러 프레임 내의 여러 개의 압축 단위의 각각의 압축 단위의 부분을 암호화하고, 압축 단위의 암호화된 부분을 포함한 여러 개의 독립적으로 인코딩된 압축 단위를 포함하는 비트스트림 출력을 생성한다.

대표도



(52) CPC특허분류

H04L 9/065 (2013.01)

H04N 19/46 (2015.01)

H04N 21/23476 (2013.01)

H04N 21/2353 (2013.01)

H04N 21/4353 (2013.01)

H04N 21/44055 (2013.01)

명세서

청구범위

청구항 1

비일시적인 머신 판독 가능 저장 매체.

발명의 설명

기술 분야

[0001] 본 발명은 비디오 정보의 암호화(encryption) 및 복호화(decryption) 분야에 관한 것이다. 보다 구체적으로, 본 발명은 부분 프레임 암호화(partial frame encryption)를 이용하여 압축된 디지털 비디오의 보호 스트림을 생성하는 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 기존의 디지털 비디오 압축 기술은 무압축 비디오 데이터의 단위를 인코딩된 형태로 변환(즉, "인코딩")할 때에 각종 기술에 의존하는 복잡한 프로세스이다. 이러한 인코딩은 원래의 무압축 비디오 데이터의 콘텐츠를 표현하는데 더 적은 비트가 이용되게 한다. 그 결과의 인코딩된 데이터는 원래의 데이터와 시각적으로 유사하거나 동일한 디지털 비디오 단위의 데이터가 되게 하는 가역적 프로세스(즉, "디코딩")를 이용해서 변환될 수 있다. 현대의 디지털 비디오 압축 기술은 초고도의 압축을 달성할 수 있다.

[0003] MPEG(Motion Pictures Experts Group) 및 국제 표준화 기구(ISO)는 비디오 코딩을 위한 비디오 압축 및 압축해제 알고리즘을 명시하는 다양한 국제 표준을 제정하였다. 이들 표준은 MPEG-1, MPEG-2, MPEG-4, H.261, H.264과, 선행 표준들에 비해 실질적으로 향상된 압축 효율을 갖는 새로운 HEVC(High-Efficiency Video Coding) 표준을 포함한다. 특히, HEVC는 이전의 H.264 표준과 비교해서 동일한 주관적 품질에서 2x 압축비를 달성할 수 있다. 이러한 압축 최적화를 달성하기 위해, HEVC 표준은 특히 멀티코더 프로세서 아키텍처 상에서의 비디오 콘텐츠의 병렬 프로세싱에 맞게 설계된 여러 개의 새로운 톨을 도입하고 있다. 특히, 시판되고 있는 다수의 스마트폰과 태블릿 아키텍처는 현재 멀티코어 프로세서를 이용하고 있고, 그래서 이들의 멀티코어 아키텍처를 이용하여 HEVC 콘텐츠를 플레이백할 수 있다. 더욱이, 네트워크를 통한 비디오 트래픽의 증가에 따라, HEVC 표준은 고품질 콘텐츠를 배포하기 위한 대역폭 요건의 일부를 완화시키는 소정의 톨을 제공한다.

[0004] 프라이머시 및 기타 종류의 불법 배포로부터 디지털 콘텐츠의 배포를 보호하는 것은 콘텐츠 제공자의 또 다른 근심거리이다. 디지털 저작권 관리(DRM, Digital Rights Management)라는 용어는 디지털 콘텐츠의 액세스 및/또는 복사를 제어하는데 이용되는 액세스 제어 기술을 기술하는데 이용된다. DRM 시스템은 통상 콘텐츠의 일부에 대한 액세스를 제어하거나 콘텐츠의 일부를 보호하기 위해 암호 정보(cryptographic information)를 사용한다. 콘텐츠 보호는 콘텐츠를 암호화하기 위한 하나 이상의 암호화 키(encryption key)와 같은(그러나 이에 한정되지 않는) 암호 정보를 이용하여 통상 달성된다.

[0005] 데이터를 보호하는데 이용될 수 있는 다양한 유형의 암호화 방식들이 현재 존재한다. 디지털 세계에서는, 일정 단위의 데이터로 예측 가능한 변환을 실행하기 위해 "키"라고 알려진 어떤 길이의 비트의 집합을 이용하여 종종 암호화가 구현된다. 이것은 변환을 실행하는데 이용되는 키의 지식 없이는 "판독"될 수 없는 또 다른 단위의 데이터를 만들어 낸다. 암호화 프로세스는 암호화된 데이터를 다시 원래의 형태로 변환하거나 "복호화"할 때에 암호화 키나 그것의 대응물(예컨대, "공개" 키)을 사용할 수 있는 범위까지만 쉽게 가역적(reversible)일 수 있다. 보통 비디오 데이터는 예컨대 DES(Data Encryption Standard) 또는 AES(Advanced Encryption Standard)에 부합하는 대칭적 블록 암호(symmetrical block cipher)를 이용하여 암호화된다. 디지털 콘텐츠를 암호화하는데 이용되는 특정 기술들은 네트워크를 통한 콘텐츠의 인코딩 및 배포에 대해 고려되어야 하는 추가 프로세싱 리소스도 소비할 수 있다.

발명의 내용

[0006] 본 발명의 실시형태에 따른 부분 프레임 암호화를 위한 시스템 및 방법이 개시된다. 일 실시형태에 있어서, 이 방법은 여러 프레임을 포함하는 비디오 비트스트림을 수신하고, 각 프레임은 프레임 내에 여러 개의 독립적으로

인코딩된 압축 단위를 포함하는 것이며, 상기 방법은 여러 프레임 내의 여러 개의 압축 단위의 각각의 압축 단위의 부분을 암호화하고, 압축 단위의 암호화된 부분을 포함한 여러 개의 독립적으로 인코딩된 압축 단위를 포함하는 비트스트림 출력을 생성한다.

- [0007] 본 발명의 다른 실시형태에 있어서, 압축 단위는 비디오의 특정 프레임의 독립적으로 디코딩 가능한 부분이어서, 디코딩되기 위해 상기 특정 프레임 내의 다른 압축 단위에 의존하지 않는다.
- [0008] 본 발명의 또 다른 실시형태에 있어서, 상기 방법은 또한 비디오의 프레임 내에서 압축 단위의 위치를 식별하기 위한 메타데이터 헤더를 파싱하고, 그 압축 단위의 위치에 기초하여 비디오 비트스트림의 부분을 암호화한다.
- [0009] 본 발명의 또 다른 실시형태에 있어서, 상기 방법은 비디오 비트스트림과 연관된 헤더 내의 정보에 기초하여 압축 단위가 인에이블(enable)되는 것을 결정함으로써 복수의 압축 단위의 각각의 압축 단위의 부분을 암호화한다.
- [0010] 본 발명의 또 다른 실시형태에 있어서, 상기 방법은 비디오의 프레임에서 각각의 압축 단위의 부분을 암호화하는 단계를 더 포함한다.
- [0011] 본 발명의 또 다른 실시형태에 있어서, 상기 부분은, i) 압축 단위의 선두 N 바이트, ii) 압축 단위의 최종 N 바이트, iii) 압축 단위 내의 중간부의 N 바이트, 및 iv) 압축 단위 내의 패턴의 N 바이트로 이루어진 그룹에서 선택된다.
- [0012] 본 발명의 또 다른 실시형태에 있어서, 압축 단위는 HEVC(High-Efficiency Video Coding) 표준 내의 타일이며, 비디오 비트스트림은 HEVC 표준에 기초하여 인코딩된다.
- [0013] 본 발명의 또 다른 실시형태에 있어서, 상기 방법은 비디오 비트스트림 내에서 타일의 구조를 식별하기 위해 HEVC 비디오 비트스트림의 PPS(Picture Parameter Set)를 파싱하는 단계를 더 포함하고, 그 구조에 기초하여 타일의 부분을 암호화한다.
- [0014] 본 발명의 다른 실시형태에 있어서, 상기 방법은 또한 그 부분을 암호화하기 위해 공통 암호화 포맷(CENC)을 이용하여 여러 개의 압축 단위의 각각의 압축 단위의 부분을 암호화한다.
- [0015] 본 발명의 또 다른 실시형태는 콘텐츠 인코더를 포함하고, 콘텐츠 인코더는 인코더 애플리케이션을 포함하는 메모리와 통신하도록 구성되는 프로세서를 포함하며, 인코더 애플리케이션은 프로세서에, 여러 개의 프레임-각각의 프레임은 그 프레임 내에 여러 개의 독립적으로 인코딩된 압축 단위를 포함함-을 포함하는 비디오 비트스트림을 수신하고, 여러 개의 프레임에서 여러 개의 압축 단위의 각각의 압축 단위의 부분을 암호화하며, 압축 단위의 암호화된 부분을 포함한 여러 개의 독립적으로 인코딩된 압축 단위를 포함하는 비트스트림 출력을 생성하도록 지시한다.
- [0016] 본 발명의 다른 실시형태에 있어서, 압축 단위는 비디오의 특정 프레임의 독립적으로 디코딩 가능한 부분이어서, 디코딩되기 위해 상기 특정 프레임 내의 다른 압축 단위에 의존하지 않는다.
- [0017] 본 발명의 또 다른 실시형태에 있어서, 인코더 애플리케이션 또한 프로세서에, 비디오의 프레임 내에서 압축 단위의 위치를 식별하기 위해 메타데이터 헤더를 파싱하고 그 압축 단위의 위치에 기초하여 비디오 비트스트림의 부분을 암호화하도록 지시한다.
- [0018] 본 발명의 또 다른 실시형태에 있어서, 여러 개의 압축 단위의 각각의 압축 단위의 부분을 암호화하는 것은, 비디오 비트스트림과 연관된 헤더 내의 정보에 기초하여 압축 단위가 인에이블되는 것을 결정하는 것을 포함한다.
- [0019] 본 발명의 또 다른 실시형태에 있어서, 인코더 애플리케이션은 또한 프로세서에, 비디오의 프레임에서 각각의 압축 단위의 부분을 암호화하도록 지시한다.
- [0020] 본 발명의 또 다른 실시형태에 있어서, 상기 부분은, i) 압축 단위의 선두 N 바이트, ii) 압축 단위의 최종 N 바이트, iii) 압축 단위 내의 중간부의 N 바이트, 및 iv) 압축 단위 내의 패턴의 N 바이트로 이루어진 그룹에서 선택된다.
- [0021] 본 발명의 또 다른 실시형태에 있어서, 압축 단위는 HEVC(High-Efficiency Video Coding) 표준 내의 타일이며, 비디오 비트스트림은 HEVC 표준에 기초하여 인코딩된다.
- [0022] 본 발명의 또 다른 실시형태에 있어서, 인코더 애플리케이션은 또한 프로세서에, 비디오 비트스트림 내에서 타일의 구조를 식별하기 위해 HEVC 비디오 비트스트림의 PPS(Picture Parameter Set)를 파싱하고, 구조에 기초하

여 타일의 부분을 암호화하도록 지시한다.

- [0023] 본 발명의 다른 실시형태에 있어서, 복수의 압축 단위의 각각의 압축 단위의 부분을 암호화하는 것은, 그 부분을 암호화하기 위해 공통 암호화 포맷(CENC)을 이용하는 것을 포함한다.
- [0024] 본 발명의 다른 실시형태에 있어서, 콘텐츠 디코더는 디코더 애플리케이션을 포함하는 메모리와 통신하도록 구성되는 프로세서를 포함하며, 디코더 애플리케이션은 프로세서에, 여러 개의 프레임—각각의 프레임은 그 프레임 내에 여러 개의 독립적으로 인코딩된 압축 단위를 포함함—을 포함하는 비디오 비트스트림을 수신하고, 여러 개의 프레임에서 여러 개의 압축 단위의 각각의 압축 단위의 부분을 복호화하며, 플레이백할 디코딩된 비디오 출력을 생성하도록 지시한다.
- [0025] 본 발명의 다른 실시형태에 있어서, 압축 단위는 비디오의 특정 프레임의 독립적으로 디코딩 가능한 부분이어서, 디코딩되기 위해 상기 특정 프레임 내의 다른 압축 단위에 의존하지 않는다.
- [0026] 본 발명의 또 다른 실시형태에 있어서, 디코더 애플리케이션 또한 프로세서에, 비디오의 프레임 내에서 압축 단위의 위치를 식별하기 위한 메타데이터 헤더를 파싱하고, 그 압축 단위의 위치에 기초하여 비디오 비트스트림의 부분을 복호화하도록 지시한다.
- [0027] 본 발명의 또 다른 실시형태에 있어서, 여러 개의 압축 단위의 각각의 압축 단위의 부분을 복호화하는 것은, 비디오 비트스트림과 연관된 헤더 내의 정보에 기초하여 압축 단위가 인에이블되는 것을 결정하는 것을 포함한다.
- [0028] 본 발명의 또 다른 실시형태에 있어서, 디코더 애플리케이션은 또한 프로세서에, 비디오의 프레임에서 각각의 압축 단위의 부분을 복호화하도록 지시한다.
- [0029] 본 발명의 또 다른 실시형태에 있어서, 상기 부분은, i) 압축 단위의 선두 N 바이트, ii) 압축 단위의 최종 N 바이트, iii) 압축 단위 내의 중간부의 N 바이트, 및 iv) 압축 단위 내의 패턴의 N 바이트로 이루어진 그룹에서 선택된다.
- [0030] 본 발명의 또 다른 실시형태에 있어서, 압축 단위는 HEVC(High-Efficiency Video Coding) 표준 내의 타일이며, 비디오 비트스트림은 HEVC 표준에 기초하여 디코딩된다.
- [0031] 본 발명의 또 다른 실시형태에 있어서, 디코더 애플리케이션은 또한 프로세서에, 비디오 비트스트림 내에서 타일의 구조를 식별하기 위하여 HEVC 비디오 비트스트림의 PPS(Picture Parameter Set)를 파싱하고, 그 구조에 기초하여 타일의 부분을 복호화하도록 지시한다.
- [0032] 본 발명의 또 다른 실시형태에 있어서, 복수의 압축 단위의 각각의 압축 단위의 부분을 복호화하는 것은, 그 부분을 복호화하기 위해 공통 암호화 포맷(CENC)을 이용하는 것을 포함한다.

도면의 간단한 설명

- [0033] 도 1은 본 발명의 실시형태에 따른 비디오 인코딩 및 전달 시스템의 시스템 도면이다.
- 도 2a는 본 발명의 실시형태에 따라 부분 암호화된 콘텐츠를 생성하도록 구성된 콘텐츠 인코더를 개념적으로 도시하는 도면이다.
- 도 2b는 본 발명의 실시형태에 따라 부분 암호화된 콘텐츠를 관리 및 배포하도록 구성된 콘텐츠 서버를 개념적으로 도시하는 도면이다.
- 도 2c는 본 발명의 실시형태에 따라 부분 암호화된 콘텐츠를 수신 및 플레이백하도록 구성된 플레이백 디바이스를 개념적으로 도시하는 도면이다.
- 도 3은 본 발명의 실시형태에 따라 콘텐츠를 부분 암호화하는 프로세스를 설명하는 도면이다.
- 도 4는 본 발명의 실시형태에 따라 콘텐츠를 부분 암호화하는 프로세스를 설명하는 도면이다.
- 도 5는 본 발명의 실시형태에 따라 부분 암호화된 콘텐츠를 디코딩 및 플레이백하는 프로세스를 설명하는 도면이다.
- 도 6은 본 발명의 실시형태에 따른 비디오의 프레임 내의 타일의 예를 도시하는 도면이다.
- 도 7은 본 발명의 실시형태에 따른 HEVC 비디오 내의 타일에 대한 선택 구조의 예를 도시하는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0034] 전술한 바와 같이, 콘텐츠를 암호화하는 데에 상이한 기술들이 이용될 수 있으며, 각각의 기술은 비디오 콘텐츠를 압축 또는 인코딩하는데 이용되는 압축 기술(예컨대, H.264 또는 HEVC)에 연관된 프로세싱 비용과 함께 상이한 양의 프로세싱 리소스를 소비할 수 있다. 따라서, 본 발명의 다수의 실시형태들은 전체 프레임보다는 프레임의 부분만 암호화함으로써 프레임을 암호화한 보호된 압축 비디오 시퀀스를 생성할 때에 효율을 달성하는 것이 가능하다. 이들 기술은 한 프레임의 일부만 암호화하기 때문에 일반적으로 "부분 프레임 암호화(partial frame encryption)"라고 칭해질 수도 있다. 비디오의 프레임 내에서 암호화되는 하나 이상의 부분은 그 프레임 내에서 시작 위치 및 길이가 지정될 수 있다. 보통, 이 정보는 프레임과 연관된 헤더 내에 제공되며, 복호화를 위해 프레임의 암호화된 부분을 찾기 위해 디코더에 의해 이용될 수 있다.
- [0035] H.264/MPEG-4 AVC(Advanced Video Coding) 등의 다수의 비디오 압축 포맷에는, 프레임 내에 그리고 다수의 프레임에 걸쳐(압축 알고리즘 때문에) 의존성이 있다. 이 의존성 때문에, 암호화되는 일부가 복호화될 수 없고 그래서 적절하게 플레이백될 수 없는 경우에, 암호화된 부분에 의존하는, 프레임 내의 또는 다른 프레임 내의 다른 부분도 플레이백될 수 없다. 이에, AVC 인코딩된 비트스트림에서는, 한 프레임 또는 일련의 단위의 선두 x 개의 바이트를 암호화하는 것만으로, 프레임 또는 다른 단위의 다수의 다른 부분의 디코딩을 피하기에 충분하다.
- [0036] 다수의 실시형태는 암호화를 위해 ISO/IEC 23001 -7:2012 CENC(Common Encryption Scheme) 표준을 이용할 수 있으며, 이 표준은 하나 이상의 디지털 저작권 및 키 관리 시스템(DRM 시스템)에 의해 상이한 DRM 시스템을 이용해 동일한 파일의 복호화를 가능하게 하는데 이용될 수 있는 표준 암호화 및 키 매핑 방법을 명시하는 산업용 암호화 표준이다. 이 방식은 한 프레임의 다수의 비연속 부분을 암호화하는 것이 가능하다.
- [0037] HEVC(High Efficiency Video Coding) 등의 일부 비디오 압축 포맷은, 다른 부분 내의 정보를 참조하거나 의존하는 일 없이, 프레임의 부분들이 독립적으로 인코딩 및 디코딩되게 하고, 프레임 비디오의 상이한 부분들의 동시적인 병렬 프로세싱(parallel processing)을 가능하게 한다. 병렬 프로세싱을 가능하게 하도록 설계된 하나의 이러한 피처(feature)가 HEVC에서의 "타일(tile)"이다. 특히, 픽처(picture)를 직사각형 영역(타일)들로 분할함으로써 상이한 프로세서들에 의해 동시에 프레임의 부분들을 인코딩 및 디코딩하도록 타일이 이용될 수 있으며, 각 타일은 다수의 코딩 트리 단위(coding tree unit, CTU)로 이루어진다.
- [0038] 타일은 단일 NAL(Network Abstraction Layer) 단위 또는 슬라이스 내에 포함될 수 있다. 프레임의 마찬가지로 독립적으로 디코딩 가능한 부분들은 상이한 인코딩 포맷에 걸쳐 압축 단위(compression unit)(즉, HEVC에서의 타일)로서 칭해질 수 있다. 압축 단위는 서로 독립적으로 프로세싱될 수 있기 때문에, 비트스트림 디코딩 시에 병렬화(parallelism)를 가능하게 한다. 인에이블되는 타일을 갖는 HEVC 인코딩된 스트림에서는, 비디오 NAL 단위 또는 프레임의 선두 x 바이트만 암호화되었다면, 다른 부분(타일)은 암호화된 부분(들)과의 독립성 때문에 암호화된 부분(들)을 복호화하지 않고서도 완전히 디코딩 가능할 수 있다.
- [0039] 이에, 다수의 실시형태에 있어서, 타일(또는 다른 압축 단위)을 갖는 인코딩된 비트스트림의 보안성은, 암호화된 부분을 복호화하지 않고서, 프레임의 더 많은 부분들을 복구할 수 없도록 프레임 내의 다수의 타일 중 적어도 일부를 암호화함으로써 향상될 수 있다. 여러 실시형태에 있어서, 타일이 위치하는 곳을 결정하여 타일의 부분을 암호화하기 위해 비트스트림의 적어도 일부를 디코딩하도록 인코더 및/또는 인코딩 프로세스가 설계될 수 있다. 인코더는 다수의 타일 내의 정보를 암호화하고 비트스트림의 더 많은 부분들이 복호화되지 않고서 디코딩되지 않게 보호하기 위해 타일의 구조 및/또는 위치에 관한 정보를 취득할 수 있다. 타일(또는 다른 독립적으로 디코딩 가능한 단위)에 관한 이 정보를 취득하는 방법은 하나 이상의 타일의 시작 위치를 결정하기 위해 NAL 단위 헤더를 파싱하는 단계를 포함할 수 있다. 본 발명의 실시형태에 따른 압축 단위의 부분 프레임 암호화를 위한 시스템 및 방법에 대해서는 이하에서 더 설명한다.
- [0040] 부분 프레임 암호화를 이용한 부분 인코딩 및 플레이백을 위한 시스템 아키텍처
- [0041] 전술한 바와 같이, 다수의 새로운 압축 방법은 멀티코어 아키텍처 상에서의 비디오 콘텐츠의 병렬 프로세싱(즉, 인코딩 및 디코딩)을 가능하게 하는 새로운 틀을 제공한다. 이들 틀은 예컨대 비디오 콘텐츠의 프레임을 별개의 디코딩 가능한 단위로 분할하는데 이용될 수 있는, 유사한 독립적으로 디코딩 가능한 단위의 다른 유형들 중에서, HEVC 표준의 "타일"의 이용을 포함한다. 본원 전체에서 설명하고 있지만, 압축 단위(예컨대, HEVC에서의 타일)은 소정의 인코딩 표준에 적합한 비디오의 단일 프레임의 분할된 그리고/또는 독립적으로 디코딩 가능한 부분들을 일반적으로 지칭할 수 있다. 아울러, "타일"은 HEVC 표준 내에 도입되고 있는 압축 단위의 유형이다. 후술하는 다수의 예에서는 HEVC 표준에 따라 압축된 비디오에 기반한 타일의 부분 프레임 암호화를 기술하고 있지

만, 부분 프레임 암호화는, 본 발명의 실시형태에 따른 특정 애플리케이션의 요건에 적합하다면 비디오 프레임을 분할하는 유사한 유형의 압축 단위를 이용하는 그 외 다른 표준에 따라 압축된 비디오를 암호화하는 데에도 이용될 수 있다.

[0042] 또한, 독립적으로 디코딩 가능한 압축 단위를 이용하여 압축된 디지털 콘텐츠를 보호하기 위해, 비디오의 프레임 내에서 압축 단위(즉, 타일)의 하나 이상의 부분에 부분 프레임 암호화를 적용하는 소정의 암호화 기술이 이용될 수도 있다. 특히, 비디오의 프레임 내에서의 압축 단위의 독립적 디코딩을 가능하도록 설계된 새로운 표준(예컨대, HEVC)에서는, 다른 부분들이, 암호화된 프레임의 적절한 복호화를 필요로 할 프레임간 의존성을 갖게 되는 압축 표준 설계에 기초하여 전체 비디오 프레임(즉, 비디오 픽처)의 일부만을 암호화하는 것이 더 이상 충분하지 않을 수 있다. 전술한 바와 같이, 이들 구 압축 표준에서는, 단일 비디오 프레임의 상이한 부분들 간의 의존성 때문에, 암호화되는 일부가 복호화될 수 없고 그래서 적절하게 플레이백될 수 없는 경우에, 암호화된 부분에 의존하는, 그 프레임 내의 또는 다른 프레임 내의 다른 부분도 플레이백될 수 없다. 이에, 다수의 실시형태에서는, 부분 프레임 암호화가 비디오의 프레임 내에서 하나 이상의 압축 단위의 부분에 적용될 수 있다. 본 발명의 일 실시형태에 따른 부분 프레임 암호화를 이용하는 비디오 콘텐츠 인코딩 시스템이 도 1에 도시된다.

[0043] 시스템(100)은 소스 미디어를 인코딩된 비디오로 인코딩하도록 구성된 콘텐츠 인코더(106)를 포함한다. 여러 실시형태에 있어서, 콘텐츠 인코더는, 비디오의 프레임의 다른 부분을 참조하지 않고서 그 프레임의 부분들의 독립적 인코딩/디코딩을 가능하게 하는, 예컨대 압축 단위(예컨대, 타일)을 비디오의 각 프레임 내에 생성함으로써 콘텐츠의 병렬 프로세싱을 가능하게 하는 압축 표준(예컨대, HEVC 표준)을 이용하여 콘텐츠를 인코딩할 수 있다. 특히, 여러 실시형태에 있어서, 콘텐츠 인코더는 비디오 콘텐츠의 프레임을 인코딩하기 위해 HEVC 표준을 이용하여 콘텐츠를 인코딩할 수 있다. HEVC 표준은 또한 비디오의 각 프레임마다 하나 이상의 독립적으로 디코딩 가능한 타일을 생성할 수 있다.

[0044] 압축 표준(예컨대, HEVC)에 기초하여 비디오의 프레임을 인코딩하는 것과 함께, 다수의 실시형태에 있어서, 콘텐츠 인코더(106)는 또한 비디오 콘텐츠를 불법 배포로부터 보호하기 위해 비디오 콘텐츠의 부분들을 암호화할 수 있다. 비디오 콘텐츠의 암호화와 연관되는 오버헤드 비용을 줄이기 위해, 다수의 실시형태에 있어서, 콘텐츠 인코더(106)는 비디오의 프레임 내에서 하나 이상의 압축 단위(즉, 타일)의 일부만이 암호화되게 하는(비디오 콘텐츠의 전체 프레임을 암호화하는 것이 아니라) 부분 프레임 암호화를 이용하여 비디오 콘텐츠를 인코딩한다. 일부 실시형태에 있어서, 콘텐츠 인코더는 비디오의 프레임 내에서 각 타일의 선두 x개의 바이트를 암호화한다. 다른 실시형태에서는 비트스트림 내의 어딘가에 위치한 x 바이트, 최종 x 바이트, 또는 특정 애플리케이션에 적합하다면 타일 내의 기타 조합의 바이트를 포함한, 타일의 상이한 부분들을 암호화할 수 있다. 소정의 실시형태에 있어서, 콘텐츠 인코더는 프레임 내의 모든 타일의 동일한 부분을 암호화할 수도 있다. 다른 실시형태에 있어서, 콘텐츠 인코더는 상이한 타일들의 상이한 부분들을 암호화할 수도 있다. 여러 실시형태에 있어서, 콘텐츠 인코더는 비디오의 프레임 내에서(예컨대, 전체 타일보다 적은) 소정의 타일만 부분들을 암호화할 수도 있다. 쉽게 이해하는 바와 같이, 암호화된 비디오를 포함하는 컨테이너 파일은 암호화된 부분들의 전체 또는 각각을 암호화하는데 이용되는 암호 정보 및/또는 프레임 내의 타일들의 암호화된 부분의 위치에 관한 정보를 포함하는 별개의 DRM 트랙을 포함할 수 있다.

[0045] 일부 실시형태에 있어서, 콘텐츠 인코더(106)는 마트로스카(Matroska, MKV) 컨테이너 파일에 콘텐츠를 저장한다. 마트로스카 컨테이너는 프랑스 오손에 소재한 비영리기관 마트로스카에 의해 개방형 표준 프로젝트로서 개발된 미디어 컨테이너이다. 마트로스카 컨테이너는 XML(Extensible Markup Language)의 바이너리 파생어인 EBML(Extensible Bindary Meta Language)를 기반으로 한다. 마트로스카 컨테이너의 디코딩은 다수의 가전제품(CE) 디바이스에 의해 지원된다. 다른 실시형태에 있어서, 특정 애플리케이션의 요건에 적합하다면 MPEG-4 파트 14와 같은 MPEG(Motion Picture Experts Group)에 의해 명시되는 MP4 컨테이너 파일 포맷을 포함한(그러나 이것에 한정되지 않음) 각종 컨테이너 파일 포맷의 어떤 것도 이용될 수 있다.

[0046] 일부 실시형태에 있어서, 콘텐츠 인코더(106)가 비디오 시퀀스를 압축 및/또는 암호화한 후에, 콘텐츠 인코더(106)는 인코딩된 비디오를 콘텐츠 서버(102)에 업로드한다.

[0047] 다수의 실시형태에 있어서, 콘텐츠 서버(102)는 소스 미디어를 하나 이상의 플레이백 디바이스(108-114)에 배포하는 것을 돕는다. 본 발명의 여러 실시형태에 따른 콘텐츠 서버(102)는 플레이백 디바이스에의 배포를 위해 보호 콘텐츠를 저장하는 것을 담당할 수 있다. 다수의 실시형태에 있어서, 콘텐츠 서버는 인코딩된 비디오를 다운로드하려고 하는 각종의 플레이백 디바이스(108-114)로부터의 다운로드 요청을 수신하여 프로세싱한다. 일부 실시형태에 있어서, 디바이스는 (i) 전체 파일을 다운로드하는 것, 또는 (ii) 프로그레시브(progressive) 스트리

밍 모드 또는 어댑티브(adaptive) 스트리밍 모드로 플레이백할 스트리밍 비디오를 수신하는 것을 요청할 수 있다. 배포 서버가 플레이백 디바이스로부터 다운로드 요청을 수신할 경우, 이 서버는 플레이백 디바이스에, 저장할 그리고/또는 플레이백할 인코딩된 비디오를 제공할 수 있다.

[0048] 다운로드된 비디오 파일은 비디오의 프레임 내에서의 압축 단위(예컨대, HEVC 인코딩된 비디오의 타일)의 구조를 기술하는 데이터를 포함하는 하나 이상의 헤더를 포함할 수 있다. 헤더는 하나 이상의 타일의 시작 위치에 대한 포인터를 포함할 수 있다. 일부 실시형태에 있어서, 인코딩된 HEVC 비디오 시퀀스 내에서의 타일의 위치는 비디오의 하나 이상의 프레임 내의 타일 구조에 관한 정보를 제공하는 PPS(picture parameter structure)에 명시될 수 있다. 일부 실시형태에서는, 타일이 프레임 내의 소정의 위치에 고정되어 있을 수도 있지만, 다른 실시형태에서는, 타일이 비디오의 상이한 프레임마다 상이한 위치에 있을 수도 있다. 플레이백 디바이스 상의 디코더는 비디오 파일을 플레이백하기 위해 디코딩되어야 하는 프레임의 부분을 결정하기 위해 이 정보를 이용할 수 있다.

[0049] 일부 실시형태에 있어서, 콘텐츠 서버(102)는 각종의 플레이백 디바이스로부터의 스트림 요청을 수신하고 이어서 인코딩된 비디오를 플레이백 디바이스에, 프로그레시브 플레이백을 위해 그리고/또는 어댑티브 비트레이트 스트리밍 시스템의 일부로서 스트리밍한다. 여러 실시형태에 있어서, 각종 플레이백 디바이스는 인터넷 등의 네트워크(104)를 통해 스트림을 요청하기 위해 HTTP 또는 다른 적절한 무상태 프로토콜(stateless protocol)을 이용할 수 있다. 여러 실시형태에 있어서, 각종 플레이백 디바이스는 RTSP를 이용할 수 있는데, 이 RTSP에 의해, 배포 서버는 각각의 플레이백 디바이스의 상태를 기록하고, 플레이백 디바이스로부터 수신된 명령어 및 플레이백 디바이스의 상태를 기술하는 저장된 데이터에 기초하여 스트리밍할 비디오를 결정한다.

[0050] 여러 실시형태에 있어서, DRM(디지털 저작권 관리) 서버(116)는 소스 미디어를 암호화/복호화하는데 필요한 키의 관리를 비롯해, 소스 미디어에 대한 인가(authorization) 및 액세스를 지원한다.

[0051] 본 발명의 소정의 실시형태에 따른 DRM 서버(116)는 플레이백 디바이스에의 배포(예컨대, 스트리밍 및/또는 다운로드)할 보호 콘텐츠 및/또는 콘텐츠의 파일을 저장하는 것을 담당할 수 있다. DRM 서버는 또한 콘텐츠를 보호하는데 이용되는 공통 암호 정보를 저장할 수도 있다. 여러 실시형태에 있어서, 공통 암호 정보는 공통 암호 정보와 연관된 식별자 및 콘텐츠의 일부를 이용하여 식별될 수 있다.

[0052] 도시하는 실시형태에서는, 플레이백 디바이스가 개인용 컴퓨터(108-110)와 모바일 폰(112-114)을 포함한다. 다른 실시형태에 있어서, 플레이백 디바이스는 DVD 플레이어, 블루레이 플레이어, 텔레비전, 셋톱 박스, 비디오 게임 콘솔, 태블릿, 및 HTTP를 통해 서버에 접속 가능하고 인코딩된 비디오를 플레이백할 수 있는 기타 디바이스 등의 가전 디바이스를 포함할 수도 있다.

[0053] 도시하는 실시형태에서는, 콘텐츠 인코더, 콘텐츠 서버, 및 DRM 서버는 서버 컴퓨터 하드웨어 상에서 실행하도록 구성된 서버 애플리케이션이다. 다른 실시형태에 있어서, 콘텐츠 인코더, 콘텐츠 서버, 및 DRM 서버는, 프로세서를 포함하고 비디오, 오디오, 및/또는 자막을 포함한(그러나 이들에 한정되지 않는) 소스 미디어의 암호화, 배포, 및 디지털 저작권 관리를 수행하기에 충분한 리소스를 구비한 임의의 프로세싱 디바이스일 수 있다. 특정 아키텍처를 도 1에 도시하고 있지만, 본 발명의 실시형태에 따른 특정 애플리케이션의 요건에 적합하다면 부분 프레임 암호화되어 있는 인코딩된 비디오를 플레이백 디바이스가 요청하게 할 수 있는 다양한 아키텍처의 어떤 것도 이용될 수 있다.

[0054] 본 발명의 일 실시형태에 따른 콘텐츠 인코더(202)의 기본 아키텍처가 도 2a에 도시된다. 콘텐츠 인코더(210)는 비휘발성 메모리(208), 휘발성 메모리(206), 및 네트워크 인터페이스(214)와 통신하는 프로세서(204)를 포함한다. 도시하는 실시형태에서는 비휘발성 메모리가 콘텐츠(212)를 인코딩하도록 프로세서를 구성하는 콘텐츠 인코더 애플리케이션(210)을 포함한다. 여러 실시형태에 있어서, 콘텐츠 인코더 애플리케이션(210)은 압축된 비디오의 암호화와 연관된 오버헤드를 줄이기 위해, 전체 프레임보다는, 비디오의 프레임 내의 하나 이상의 압축 단위(예컨대, 타일)의 부분만이 암호화되게 하는 부분 프레임 암호화를 이용하여 콘텐츠를 암호화한다.

[0055] 여러 실시형태에 있어서, 네트워크 인터페이스(214)는 프로세서(204), 휘발성 메모리(206) 및/또는 비휘발성 메모리(208)와 통신할 수 있다. 특정 콘텐츠 인코더 아키텍처가 도 2a에 도시되어 있지만, 본 발명의 실시형태에 따른 콘텐츠 인코더를 구현하기 위해, 콘텐츠 인코더 애플리케이션이 디스크 상에 또는 어떤 다른 저장 형태로 위치해 있고 실행시에 휘발성 메모리에 로드되는 아키텍처를 비롯한 다양한 아키텍처의 어떤 것도 이용될 수 있다.

[0056] 본 발명의 일 실시형태에 따른 콘텐츠 서버(222)의 기본 아키텍처가 도 2b에 도시된다. 콘텐츠 서버(222)는 비

휘발성 메모리(228), 휘발성 메모리(226), 및 네트워크 인터페이스(234)와 통신하는 프로세서(224)를 포함한다. 도시하는 실시형태에서는 비휘발성 메모리가 콘텐츠(232)를 배포하도록 프로세서를 구성하는 콘텐츠 배포 애플리케이션(230)을 포함한다. 여러 실시형태에 있어서, 네트워크 인터페이스(234)는 프로세서(224), 휘발성 메모리(226) 및/또는 비휘발성 메모리(228)와 통신할 수 있다. 특정 콘텐츠 서버 아키텍처가 도 2b에 도시되어 있지만, 본 발명의 실시형태에 따른 콘텐츠 서버를 구현하기 위해, 콘텐츠 배포 애플리케이션이 디스크 상에 또는 어떤 다른 저장 형태로 위치해 있고 실행시에 휘발성 메모리에 로딩되는 아키텍처를 비롯한 다양한 아키텍처의 어떤 것도 이용될 수 있다.

[0057] 본 발명의 일 실시형태에 따른 플레이백 디바이스의 기본 아키텍처가 도 2c에 도시된다. 플레이백 디바이스(252)는 비휘발성 메모리(258), 휘발성 메모리(256), 및 네트워크 인터페이스(240)와 통신하는 프로세서(254)를 포함한다. 도시하는 실시형태에서는 비휘발성 메모리가 콘텐츠(262)를 디코딩하도록 프로세서를 구성하는 디코더 애플리케이션(260)을 포함한다. 일부 실시형태에 있어서, 디코더 애플리케이션(260)은 비디오의 프레임 내에서 압축 단위의 위치를 식별하기 위해 비디오 컨테이너 파일 및/또는 비디오 스트림 내에 제공되는 정보를 이용하며, 비디오를 디코딩하기 위해 압축 단위의 소정 부분만을 복호화한다.

[0058] 여러 실시형태에 있어서, 네트워크 인터페이스(264)는 프로세서(254), 휘발성 메모리(256) 및/또는 비휘발성 메모리(258)와 통신할 수 있다. 특정 플레이백 디바이스 아키텍처가 도 2c에 도시되어 있지만, 본 발명의 실시형태에 따른 플레이백 디바이스를 구현하기 위해, 디코더 애플리케이션이 디스크 상에 또는 어떤 다른 저장 형태로 위치해 있고 실행시에 휘발성 메모리에 로딩되는 아키텍처를 비롯한 다양한 아키텍처의 어떤 것도 이용될 수 있다.

[0059] 부분 프레임 암호화를 위한 시스템 및 방법

[0060] 전술한 바와 같이, 일부 비디오 압축 포맷(예컨대, HEVC)은 프레임의 부분들이, 그 프레임(또는 다른 프레임)의 다른 부분 내의 정보를 참조하거나 의존하는 일 없이, 독립적으로 인코딩 및 디코딩되게 한다. 프레임의 이 독립적으로 디코딩 가능한 부분들은 상이한 인코딩 포맷에 걸쳐 압축 단위로서 칭해질 수 있다. 그렇기 때문에 독립적 압축 단위를 갖는 스트림의 암호화 중에, 프레임의 선두 x 바이트만이 암호화되었다면, 다른 부분(압축 단위 또는 타일)은 암호화된 압축 단위와의 독립성 때문에, 압축 단위의 암호화된 부분을 복호화는 일 없이 완전히 디코딩될 수 있다. 이에, 타일(또는 다른 압축 단위)을 갖는 인코딩된 비트스트림의 보안성은, 암호화된 부분을 복호화하지 않고서, 프레임의 더 많은 부분들을 복구할 수 없도록 프레임 내의 다수의 타일 중 적어도 일부를 암호화함으로써 향상될 수 있다. 본 발명의 일 실시형태에 따른 비디오 비트스트림의 압축 단위의 부분 프레임 암호화 프로세스가 도 3에 도시된다.

[0061] 이 프로세스는 비디오 데이터를 수신한다(302). 일부 실시형태에 있어서, 프로세스는 하나 이상의 콘텐츠 배포자로부터 비디오 데이터를 다운로드할 수도 있다. 다른 실시형태에 있어서, 프로세스는 비디오 플레이백 중에 비디오 데이터를 스트리밍할 수도 있다.

[0062] 프로세스는 비디오 데이터 내에서 복수의 압축 단위의 위치를 결정한다(304). 그 위치는 비디오의 프레임과 연관된 하나 이상의 헤더(들)에 의해 제공되는 정보에 기초하여 결정될 수 있다. 일부 실시형태에 있어서, 헤더는 프레임 내의 각각의 압축 단위의 시작 위치에 관한 정보를 제공할 수 있다. 일부 실시형태에 있어서, 각각의 압축 단위의 위치는 비디오의 각각의 프레임 내에 고정될 수도 있기 때문에, 헤더에 의해 식별될 필요가 없을 수도 있다. 예컨대, 인코더는 비디오 시퀀스의 구조에 관한 정보가 미리 프로그래밍되어 있을 수도 있다.

[0063] 프로세스는 암호화할 비디오의 프레임 내의 각각의 압축 단위의 부분을 결정한다(306). 일부 실시형태에 있어서, 프로세스는 각각의 압축 단위의 고정된 x 바이트가 암호화되어야 할 것을 결정한다. 여러 실시형태에 있어서, 프로세스는 압축 단위의 특성에 기초하여 상이한 압축 단위의 상이한 부분을 결정한다. 다른 실시형태에 있어서, 프로세스는 비디오의 프레임마다 하나 이상의 압축 단위에서 중간 또는 최종 x개의 바이트를 인코딩할 수도 있다. 소정의 실시형태에 있어서, 프로세스는 비디오의 소정 프레임의 부분만 암호화하면서 비디오의 다른 프레임은 암호화하지 않을 수도 있다. 쉽게 이해되겠지만, 암호화되는 특정 프레임의 특정 부분과 암호화 방식은 통상 애플리케이션의 요건에 종속된다.

[0064] 프로세스는 압축 단위의 부분을 암호화한다(308). 일부 실시형태에 있어서, 프로세스는 표준 DES 및/또는 AES 암호를 이용하여 부분을 암호화한다. 다른 실시형태는 특정 애플리케이션의 요건에 적합하다면 다른 암호화 메커니즘을 이용할 수도 있다.

[0065] 프로세스는 부분이 암호화되어 있는 압축 단위를 포함하는 비트스트림 출력을 생성한다(310). 그런 다음 프로세

스가 끝난다.

- [0066] 압축 단위의 부분을 암호화하는 특정 프로세스가 도 3에서 설명되지만, 본 발명의 실시형태에 따른 특정 애플리케이션의 요건에 적합하다면 압축 단위의 부분을 암호화하기 위해 다양한 프로세스의 어떤 것도 이용될 수 있다.
- [0067] HEVC 표준의 개관
- [0068] 전술한 바와 같이, HEVC 비디오 압축 표준은 병렬 프로세싱을 지원하는 멀티코어 아키텍처를 이용한 비디오 콘텐츠의 플레이백에 맞게 설계된 여러 새로운 툴을 포함한다. 이 툴은 슬라이스 구조와 함께 WPP(Wavefront Parallel Processing) 및 타일을 포함한다. WPP 및/또는 타일이 이용될 경우, 1 픽처에 대응하는 비디오 스트림은 독립적으로 디코딩 가능한 비트 스트림의 서브세트로 패키징될 수 있다. 특히, HEVC는 비디오의 프레임을 소정 사이즈의 직사각형 영역으로 분할하는 독립적으로 디코딩 가능한 타일을 포함한다. 본 발명의 실시형태에 따른 비디오의 프레임 내의 타일의 예를 도 6에 도시한다. 특히, 도 6은 수평 및 수직 차원의 프레임을 9개의 타일, 즉 좌측 상단 모서리의 타일 1부터 우측 하단 모서리의 타일 9까지 균등하게 분할하는 예를 도시하는 도면이다. 각각의 타일은 코딩 트리 단위를 포함한다.
- [0069] 타일 관련 파라미터는 HEVC에서는 PPS(Picture Parameter Set) 내에 시그널링될 수 있다. 비디오 시퀀스 내에서, 상이한 픽처들은 상이한 PPS를 이용하는 것이 가능하다. 타일 파라미터는 동일한 비디오 시퀀스에서 픽처마다 변할 수 있다. 대부분의 비디오 애플리케이션에서는, 타일 수와 타일 위치가 비디오 시퀀스(예컨대, 일련의 픽처) 내에서 동일할 수도 있지만, 타일의 구성이 동일한 비디오 시퀀스에서 픽처마다 변하게 될 뿐만 아니라 타일의 그룹핑이 픽처마다 변하게 되는 상황들이 발생할 수 있다.
- [0070] 도 7은 HEVC 비디오에 있어서 PPS(Picture Parameter Set)에서의 타일에 대한 선택 구조의 일례를 도시하고 있다. `tiles_enabled_flag`가 턴온되면, 각 차원에서의 타일의 수가 시그널링될 수 있다. 타일들이 균일한 사이즈를 갖는다면(예컨대, `uniform_spacing_flag`가 1이면), 시그널링되는 추가 정보는 없다. 타일의 폭과 높이가 시그널링될 수 있다. 예를 들어, 도 7에 나타내는 바와 같이, `num_tile_columns_minus1`과 `num_tile_rows_minus1`이 2로 설정될 수 있고, `uniform_spacing_flag`가 1로 설정될 수 있다.
- [0071] 인코더는 새로운 타일 파티션 파라미터를 갖는 새로운 PPS를 시그널링함으로써 프레임마다 타일을 분할하는 방식을 변경할 수도 있다. 다수의 실시형태에 있어서, 타일들은 서로 비교하여 동일한 사이즈로 유지될 필요가 없고, 혹은 이전의 인스턴스에서의 동일한 타일과 비교하여 동일한 사이즈를 유지할 필요가 없다. 특히, 인코더는 하나 이상의 프레임의 새로운 세트에 적용될 새로운 타일 파티션 파라미터를 갖는 새로운 PPS를 시그널링할 수 있다.
- [0072] HEVC에서의 부분 프레임 암호화
- [0073] 전술한 바와 같이, HEVC 표준은 고도의 병렬 프로세싱을 지원하는 소정의 툴을 도입한다. 특히, HEVC는 프레임을 직사각형 영역들로 분할한 다음에 독립적으로 인코딩 및 디코딩될 수 있게 하는 타일을 포함한다. 프레임은 타일로 균일하게 또는 불균일하게 분할될 수 있다. 각 타일에 대한 진입점(entry point)은 슬라이스 헤더에 명시될 수 있다. HEVC 표준을 이용하여 비디오 파일의 부분 암호화를 가능하게 하기 위해서, 본 발명의 다수의 실시형태에서는 비디오 콘텐츠를 암호화하기 위해 다수의 타일을 부분적으로 암호화할 수 있다. 본 발명의 일 실시형태에 따른 HEVC 타일의 부분 암호화를 위한 프로세스가 도 4에 도시된다.
- [0074] 이 프로세스는 타일의 인에이블 여부를 결정한다(402). 다수의 실시형태에 있어서, 타일이 인에이블될 경우, 비트스트림은 각 코어가 파티션에 즉시 액세스하기에 필요한 각 픽처 파티션의 시작 위치를 나타내는 진입점 오프셋을 포함할 수 있다.
- [0075] 프로세스는 프레임 및/또는 비트스트림 내에서의 NAL 단위의 구조를 결정한다(404).
- [0076] 프로세스는 NAL 단위 내의 타일의 구조를 결정한다(406). 일부 실시형태에 있어서, 프로세스는 비디오의 프레임 내에서 각각의 타일의 시작 위치를 결정하기 위해 NAL 헤더를 파싱한다. 일부 실시형태에 있어서, HEVC 타일은 픽처를 소정 사이즈의 직사각형 영역으로 분할할 수 있다. 타일에 대한 파라미터 구조는 HEVC의 경우에는, PPS(Picture Parameter Set), VUI(video usability information), 및/또는 SEI(supplemental enhancement information)에 명시될 수 있다. HEVC에서의 PPS의 일례가 도 7에 도시된다. `tiles_enabled_flag`가 턴온되면, 각 차원에서의 타일의 수가 시그널링될 수 있다. 일부 실시형태에 있어서, 타일들이 균일한 사이즈를 갖는다면(예컨대, `uniform_spacing_flag`가 1이면), 시그널링되는 추가 정보는 없다. 또한 PPS는 타일의 폭 및 높이를 시

그넨링할 수도 있다.

- [0077] 프로세스는 NAL 단위의 수를 선택한다(408). 일부 실시형태에 있어서, 프로세스는 NAL 단위의 전부를 선택할 수도 있다. 소정의 실시형태에 있어서, 프로세스는 하나 이상의 NAL 단위를 선택할 수도 있다.
- [0078] 프로세스는 선택된 NAL 단위의 각각에서의 타일의 수를 선택한다(410). 일부 실시형태에 있어서, 인코더는 새로운 타일 파티션 파라미터를 갖는 새로운 PPS를 시그널링함으로써 픽처마다 타일을 분할하는 방식을 변경할 수도 있다. 도 7은 PPS에 의한 타일 시그널링의 일례를 도시하고 있다. 일부 실시형태에 있어서, 타일들은 서로 비교하여 상이한 사이즈일 수도 있고, 혹은 이전의 인스턴스에서의 동일한 타일과 비교하여 상이한 사이즈일 수도 있다. 일부 실시형태에 있어서, 인코더는 새로운 픽처마다 또는 타일 파티션이 이전 픽처와 바뀔 경우에 새로운 타일 파티션 파라미터를 가진 PPS를 시그널링할 수 있다.
- [0079] 프로세스는 선택된 타일의 적어도 일부를 암호화한다(308). 일부 실시형태에 있어서, 프로세스는 타일의 비트스트림의 소정의 부분 내에 있는, 선두 x개의 바이트, 최종 x 바이트, 또는 어떤 x개의 바이트를 암호화할 수 있다. 여러 실시형태에 있어서, 프로세스는 타일 내의 다수의 블록을 암호화할 수도 있다. 다른 실시형태에서는 특정 애플리케이션의 요건에 적합하다면 타일의 다른 부분을 암호화할 수도 있다. 다수의 실시형태에 있어서, 프로세스는 비트스트림을 암호화하는 방법에 관한 공통 사양(specification)을 이용하는 공통 암호화 포맷(CENC, common encryption format)을 사용해 타일의 부분을 암호화한다. CENC는 타일의 복호화를 가능하게 하기 위하여 DRM 시스템에 의해 이용될 수 있는 키 매핑 방법 및 산업용 표준 암호화를 지정한다. 이 방식은 보호 스트림을 복호화하는데 필요한 암호화 관련 메타데이터에 대한 공통 포맷을 정의함으로써 운용된다. 이 방식은 다양한 다른 고려사항 중에서 저작권 매핑(rights mapping)의 상세, 키 취득 및 저장, DRM 준수 규칙을, CENC 방식을 지원하는 DRM 시스템에 위임한다. 더욱이, 다수의 실시형태에 있어서, 암호화 정보는 MKV 컨테이너 내에 저장될 수도 있다.
- [0080] 그런 다음 프로세스가 끝난다. HEVC 비디오 콘텐츠에서 타일의 부분을 암호화하는 특정 프로세스가 도 4에서 설명되지만, 본 발명의 실시형태에 따른 특정 애플리케이션의 요건에 적합하다면 타일의 부분을 암호화하기 위해 다양한 프로세스의 어떤 것도 이용될 수 있다.
- [0081] 부분 암호화된 비디오의 디코딩
- [0082] 본 발명의 일 실시형태에 따른 부분 암호화된 비디오를 디코딩하는 프로세스가 도 5에 도시된다.
- [0083] 이 프로세스는 암호화된 비디오 데이터를 수신한다(502). 일부 실시형태에 있어서, 프로세스는 콘텐츠 제공자로부터 비디오 콘텐츠를 다운로드, 스트리밍, 및/또는 비디오 콘텐츠를 다운로드하기 위해 스트리밍할 수 있다. 다른 실시형태에 있어서, 비디오 데이터는 디스크 상에 저장될 수도 있고, 혹은 특정 애플리케이션의 요건에 적합하다면 기타 메커니즘에 의해 취득될 수도 있다.
- [0084] 프로세스는 비디오 데이터 내에서 복수의 압축 단위(예컨대, HEVC에서의 타일)의 위치를 결정한다(504). 일부 실시형태에 있어서, 타일의 위치는 비디오의 하나 이상의 프레임 내에 고정될 수도 있다. 다른 실시형태에 있어서, 타일의 위치는 프레임들 사이에서 또는 프레임의 세트들 사이에서 변할 수 있다. 타일의 위치는 프레임에 대응하는 PPS 내에 포함된 정보에 기초하여 결정될 수 있다. 구체적으로, 프로세서는 암호화된 타일 내에서 특정 바이트를 식별하기 위해 PPS를 파싱할 수 있다.
- [0085] 프로세스는 압축 단위의 암호화 여부를 결정하고, 암호화된 압축 단위를 복호화한다(506). 일부 실시형태에 있어서, 프로세스는 암호화된 콘텐츠를 복호화하기 위한 복호화 키를 취득할 수 있다. 복호화 키는 콘텐츠와 연관된 DRM 서버로부터 수신되는 인가(authorization)에 기초하여 취득될 수 있다.
- [0086] 프로세스는 압축 단위를 디코딩한다(508). 다수의 실시형태에 있어서, 프로세서는 비디오(예컨대, HEVC 비디오)를 인코딩하는데 이용된 특정 압축 표준에 기초하여 콘텐츠를 디코딩한다.
- [0087] 프로세스는 플레이백할 디코딩된 비디오 출력을 생성한다(510), 그런 다음 프로세스가 끝난다.
- [0088] 압축 단위의 부분을 복호화하는 특정 프로세스가 도 5에서 설명되지만, 본 발명의 실시형태에 따른 특정 애플리케이션의 요건에 적합하다면 압축 단위의 부분을 복호화하기 위해 다양한 프로세스의 어떤 것도 이용될 수 있다.
- [0089] 소정의 특정 양태에 대해 본 발명을 설명하였지만, 다수의 추가 수정 및 변형이 당업자에게 분명할 것이다. 그러므로, 본 발명은 구체적으로 기술한 것 이외의 방식으로 실시될 수 있음을 이해해야 한다. 따라서, 본 발명

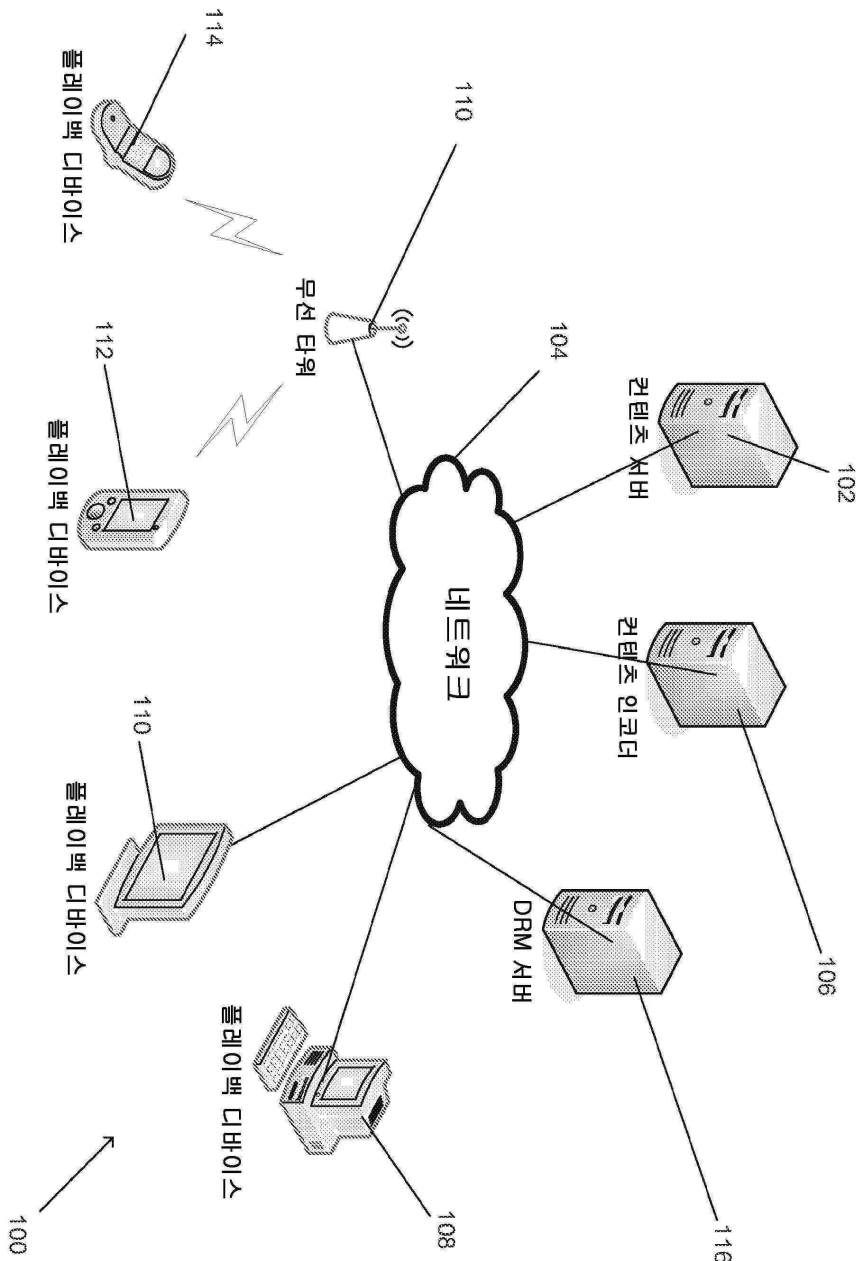
의 실시형태들은 모든 면에서 예시적인 것으로서 그리고 제한적이지 않은 것으로서 고려되어야 한다.

[0090]

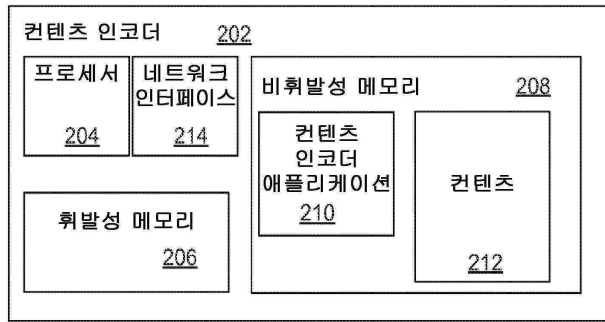
또, 기술한 설명은 본 발명의 단지 예시적인 실시형태를 개시하고 설명한 것이다. 당업자라면 본 발명의 사상 및 범위를 벗어나지 않고 다양한 변경, 수정 및 변형이 이루어질 수 있음을 이러한 논의 및 첨부된 도면으로부터 용이하게 인식할 것이다. 그러므로, 본 발명은 개시하는 특정 실시형태에 한정되지 않으며, 본 발명은 첨부한 청구범위의 범주 내에 있는 모든 실시형태를 포함할 것이다.

도면

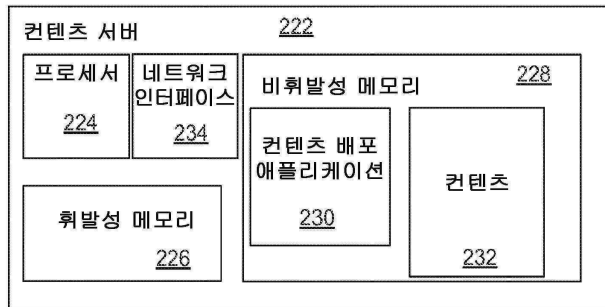
도면1



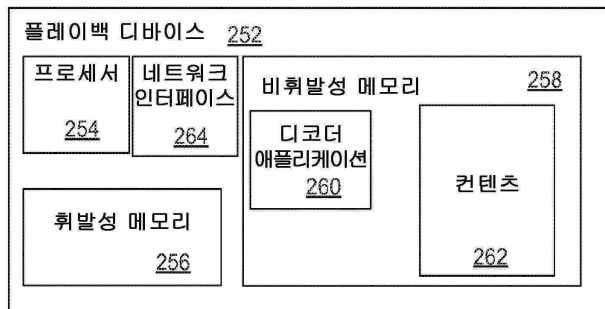
도면2a



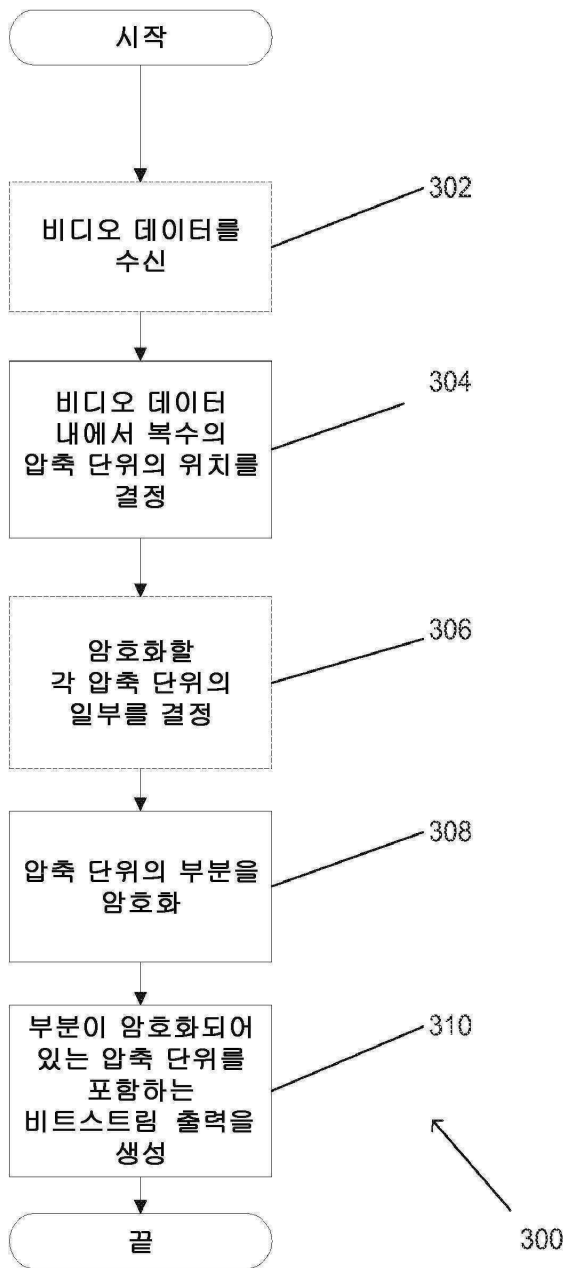
도면2b



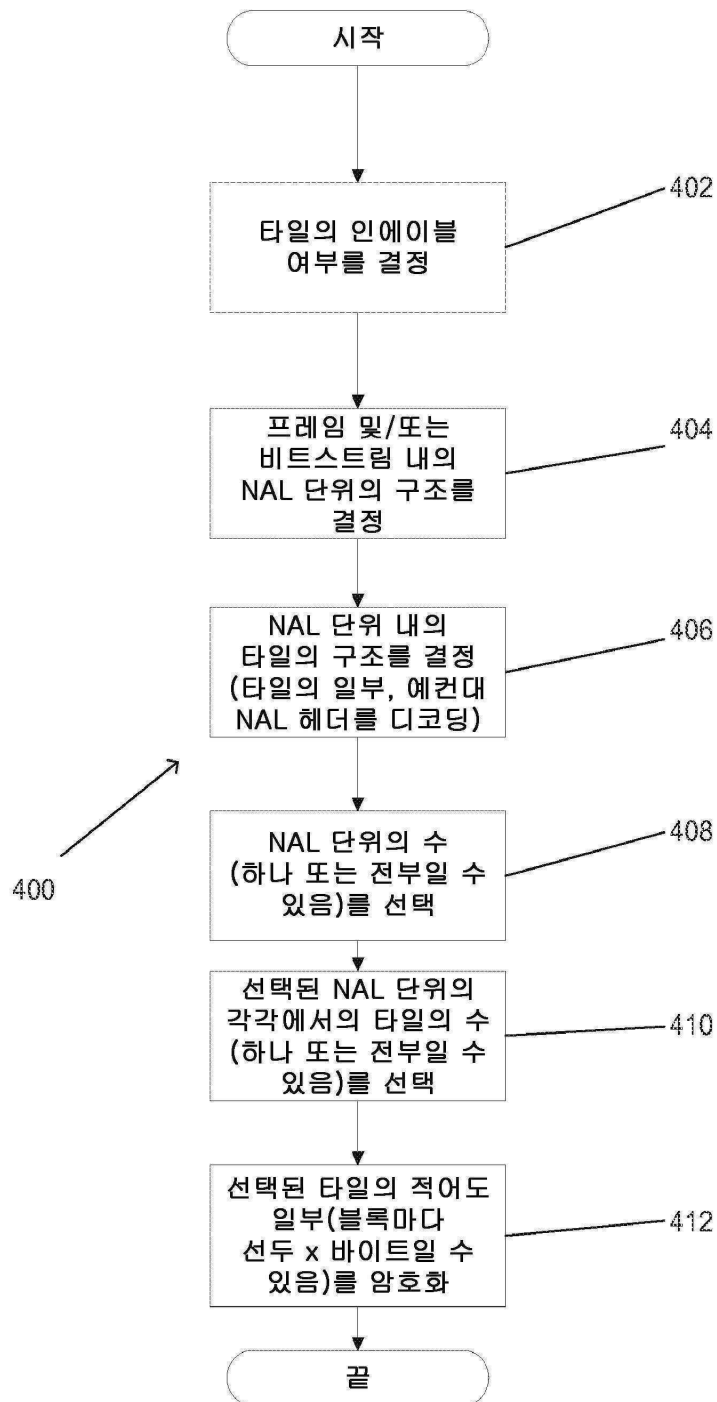
도면2c



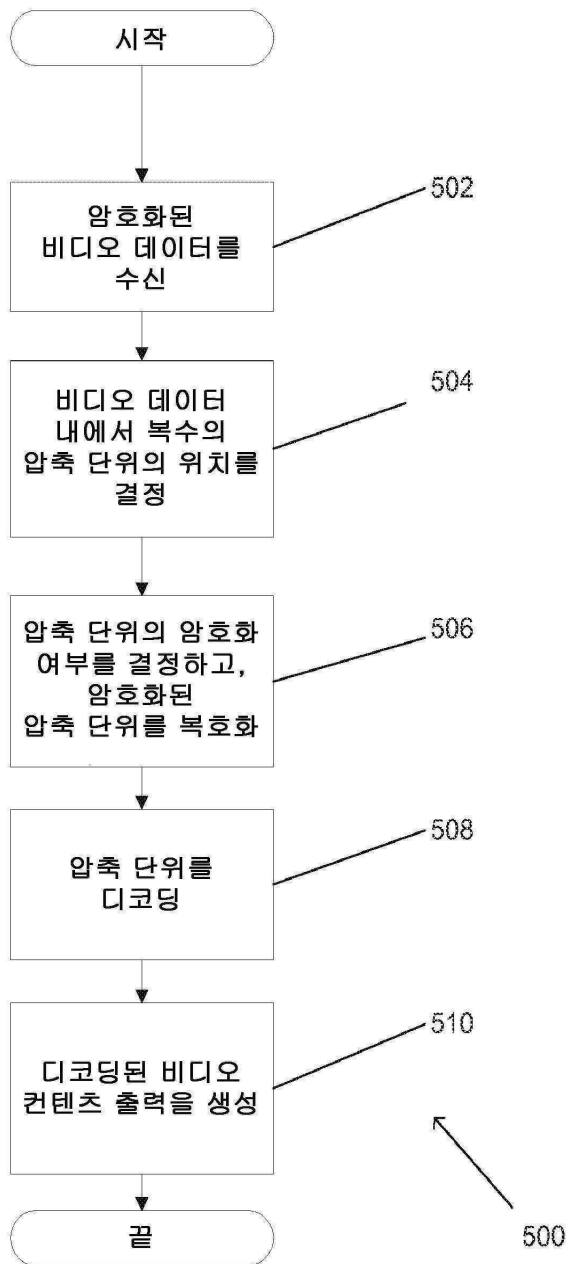
도면3



도면4



도면5



도면6

0	1	2	3	12	13	14	21	22	23	24
4	타원 1 5	6	7	15	타원 2 16	17	25	타원 3 26	27	28
8	9	10	11	18	19	20	29	30	31	32
33	34	35	36	41	42	43	47	48	49	50
37	38	39	40	44	타원 5 45	46	51	52	53	54
55	56	57	58	63	64	65	69	70	71	72
59	60	타원 7 61	62	66	타원 8 67	68	73	타원 9 74	75	76

CTU

타원들

도면7

PPS에서의 타일의 시그널링 예

pic_parameter_set_rbsp{ }	Descriptor
...	
tiles_enabled_flag	u(1)
entropy_coding_sync_enabled_flag	u(1)
entropy_slice_enabled_flag	u(1)
if(tiles_enabled_flag){	
num_tile_columns_minus1	ue(v)
num_tile_rows_minus1	ue(v)
uniform_spacing_flag	u(1)
if(!uniform_spacing_flag) {	
for(i = 0; i < num_tile_columns_minus1;	
i++)	
column_width_minus1[i]	ue(v)
for(i = 0; i < num_tile_columns_minus1; i++)	
row_height_minus1[i]	ue(v)
}	
loop_filter_across_tiles_enabled_flag	u(1)
}	
...	
}	