



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년06월16일
(11) 등록번호 10-2821757
(24) 등록일자 2025년06월12일

(51) 국제특허분류(Int. Cl.)
H04N 21/4405 (2016.01) H04L 9/32 (2006.01)
H04N 21/2343 (2011.01) H04N 21/2347 (2016.01)
H04N 21/266 (2011.01)
(52) CPC특허분류
H04N 21/4405 (2019.01)
H04L 9/3236 (2013.01)
(21) 출원번호 10-2023-0184161
(22) 출원일자 2023년12월18일
심사청구일자 2025년01월31일
(65) 공개번호 10-2024-0119828
(43) 공개일자 2024년08월06일
(30) 우선권주장
23153865.3 2023년01월30일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US07167988 B2
US20110150269 A1
US07120252 B1

(73) 특허권자
엑시스 에이비
스웨덴 룬트 에스이-223 69 그랜덴 1
(72) 발명자
비외른 볼커
스웨덴, 룬드 223 69, 그랜덴 1, 엑시스 커뮤니케이션스 에이비 내
스테판 룬드버그
스웨덴, 룬드 223 69, 그랜덴 1, 엑시스 커뮤니케이션스 에이비 내
(74) 대리인
특허법인(유한) 대아

전체 청구항 수 : 총 15 항

심사관 : 선동국

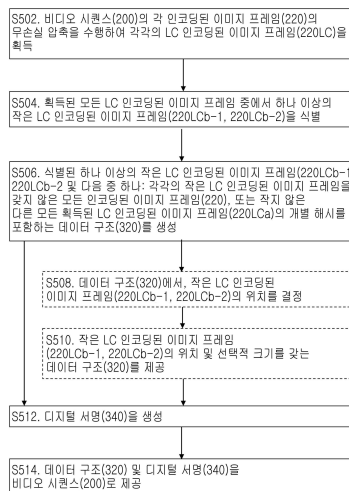
(54) 발명의 명칭 비디오 시퀀스의 검증을 위한 송신기, 수신기 및 그 안의 방법

(57) 요약

본 발명은 데이터 구조 및 디지털 서명을 갖는 시퀀스를 제공하여 인코딩된 이미지 프레임들을 포함하는 비디오 시퀀스의 검증을 가능하게 하는 송신기 및 그 방법에 관한 것이다. 이 방법은:

- 각각의 무손실 압축된, LC, 인코딩된 이미지 프레임들을 획득하기 위해 각각의 인코딩된 이미지 프레임의 무손실 (뒷면에 계속)

대표도 - 도5



압축을 수행하는 단계(S502);

- 상기 획득된 LC 인코딩된 이미지 프레임 중에서, 미리 정의된 바이트 수보다 작은 데이터 크기를 각각 갖는 작은 프레임을 식별하는 단계(S504);
- 상기 식별된 작은 프레임, 및 각각의 작은 프레임이 없는 모든 인코딩된 이미지 프레임 또는 상기 작은 프레임과 다른 모든 획득된 LC 인코딩된 이미지 프레임의 개별 해시를 포함하는 데이터 구조를 생성하는 단계(S506);
- 디지털 서명을 생성하는 단계(S512); 및
- 상기 데이터 구조 및 상기 디지털 서명을 비디오 시퀀스에 제공하는 단계(S514)를 포함한다.

(52) CPC특허분류

H04L 9/3247 (2013.01)

H04N 21/2343 (2013.01)

H04N 21/23473 (2013.01)

H04N 21/26613 (2013.01)

명세서

청구범위

청구항 1

데이터 구조 및 디지털 서명을 갖는 비디오 시퀀스를 제공함으로써 상기 비디오 시퀀스의 검증을 가능하게 하는 송신기에 의해 수행되는 방법 - 상기 비디오 시퀀스는 인코딩된 이미지 프레임들을 포함함 - 에 있어서, 상기 방법은:

- 상기 비디오 시퀀스의 각 인코딩된 이미지 프레임의 무손실 압축을 수행하여 각각 무손실 압축된(losslessly compressed, LC) 인코딩된 이미지 프레임들을 획득하는 단계;
- 상기 획득된 LC 인코딩된 이미지 프레임들 중에서, 각각이 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 하나 이상의 작은 LC 인코딩된 이미지 프레임들을 식별하는 단계;
- 다음을 포함하는 데이터 구조를 생성하는 단계:
 - 상기 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임; 및
 - 다음 중 하나의 개별 해시:

상기 획득된 LC 인코딩된 이미지 프레임의 각각이 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 모든 인코딩된 이미지 프레임; 또는

하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모든 획득된 LC 인코딩된 이미지 프레임의 각각,

상기 개별 해시는 상기 획득된 LC 인코딩된 이미지 프레임의 각각이 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 상기 모든 인코딩된 이미지 프레임들을 개별적으로 해싱하거나, 또는 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 상기 다른 모든 획득된 LC 인코딩된 이미지 프레임의 각각을 개별적으로 해싱함으로써 획득되며;

- 상기 비디오 시퀀스에 대한 디지털 서명을 생성하는 단계; 및
- 상기 데이터 구조 및 상기 디지털 서명을 상기 비디오 시퀀스에 제공함으로써 수신기가 상기 비디오 시퀀스를 검증하도록 하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서,

상기 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임 중 적어도 하나는 제1 유형의 작은 LC 인코딩된 이미지 프레임이고, 각각의 인코딩된 이미지 프레임과 동일하거나 또는 상기 인코딩된 이미지 프레임의 상기 LC 인코딩된 이미지 프레임과 동일한, 방법.

청구항 3

제1항에 있어서,

상기 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임 중 적어도 하나는 제2 유형의 작은 LC 인코딩된 이미지 프레임이고, 저장된 미리 정의된 인코딩된 이미지 프레임의 식별자와 상기 제2 유형의 상기 작은 LC 인코딩된 이미지 프레임과 상기 저장된 미리 정의된 인코딩된 이미지 프레임 간의 가능한 차이를 포함하는, 방법.

청구항 4

제1항에 있어서,

- 각각의 작은 LC 인코딩된 이미지 프레임에 대해, 상기 데이터 구조에서의 위치를 결정하는 단계;
- 상기 데이터 구조에서의 위치를 지정하는 정보와 각각의 작은 LC 인코딩된 이미지 프레임의 선택적인 데이터 크기를 갖는 상기 데이터 구조를 제공하는 단계를 더 포함하는, 방법.

청구항 5

제1항에 있어서,

상기 데이터 구조는 감소된 해시 리스트를 포함하는 문서이고, 상기 감소된 해시 리스트는:

- 상기 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임; 및
- 다음 중 하나의 개별 해시:

상기 획득된 LC 인코딩된 이미지 프레임의 각각이 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 모든 인코딩된 이미지 프레임; 또는

하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모든 획득된 LC 인코딩된 이미지 프레임의 각각으로 구성되는, 방법.

청구항 6

제1항에 있어서,

상기 송신기는 개인-공개 키 쌍에 액세스하고,

상기 디지털 서명을 생성하는 단계는,

상기 개인-공개 키 쌍의 개인 키를 가지고 다음 중 하나:

상기 데이터 구조의 해시; 또는

상기 비디오 시퀀스의 모든 인코딩된 이미지 프레임 또는 모든 상기 획득된 LC 인코딩된 이미지 프레임 중 하나에 대한 개별 해시의 해시를 암호화하여 상기 디지털 서명을 생성하는 단계를 더 포함하는, 방법.

청구항 7

데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스를 검증하기 위해 수신기에 의해 수행되는 방법 - 상기 비디오 시퀀스는 인코딩된 이미지 프레임 포함함 - 에 있어서, 상기 방법은:

- 인코딩된 이미지 프레임을 포함하고 상기 데이터 구조 및 상기 디지털 서명이 제공된 상기 비디오 시퀀스를 송신기로부터 수신하는 단계,

상기 수신된 데이터 구조는:

- 하나 이상의 작은 무손실 압축된(losslessly compressed, LC) 인코딩된 이미지 프레임 - 여기서 각각의 작은 LC 인코딩된 이미지 프레임은 미리 정의된 바이트 수보다 작고, 상기 송신기로부터 전송된 비디오 시퀀스에 포함된 각각 전송된 인코딩된 이미지 프레임의 LC 버전인 데이터 크기를 가짐 - , 및

- 다음 중 하나의 개별 해시:

LC 인코딩된 이미지 프레임의 각각이, 상기 송신기에 의해, 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 모든 전송된 인코딩된 이미지 프레임; 또는

상기 송신기에 의해, 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모

은 LC 인코딩된 이미지 프레임의 각각 - 상기 다른 모든 LC 인코딩된 이미지 프레임의 각각은 상기 전송된 비디오 시퀀스에 포함된 각각 전송된 인코딩된 이미지 프레임의 LC 버전임 - ;

- 상기 수신된 데이터 구조를 이용하여 상기 수신된 디지털 서명을 검증하는 단계; 및
- 상기 수신된 데이터 구조를 이용하여 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지 검증하는 단계를 포함 - 상기 수신된 디지털 서명 및 상기 수신된 인코딩된 이미지 프레임이 검증될 때, 상기 수신된 비디오 시퀀스는 상기 전송된 비디오 시퀀스와 동일한 것으로 검증됨 - 하는, 방법.

청구항 8

제7항에 있어서,

상기 수신된 데이터 구조는, LC 인코딩된 이미지 프레임의 각각이, 상기 송신기에 의해, 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 모든 전송된 인코딩된 이미지 프레임의 개별 해시를 포함하는 경우, 상기 수신된 데이터 구조를 이용하여 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지 확인하는 단계는:

- 상기 수신된 비디오 시퀀스에 포함된 각각 수신된 인코딩된 이미지 프레임의 개별 해시를 생성하는 단계;
- 상기 수신된 데이터 구조에 포함된 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임 각각의 무손실 압축 해제를 수행하여 각각의 인코딩된 이미지 프레임을 획득하는 단계;
- 각 획득된 각각의 인코딩된 이미지 프레임의 개별 해시를 생성하는 단계;
- 상기 수신된 비디오 시퀀스에 포함된 각각 수신된 인코딩된 이미지 프레임의 상기 생성된 개별 해시가 각 획득된 각각의 인코딩된 이미지 프레임의 상기 생성된 개별 해시와 일치할 때, 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한 것으로 검증하는 단계를 포함하는, 방법.

청구항 9

제7항에 있어서,

상기 수신된 데이터 구조는, 상기 송신기에 의해, 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모든 LC 인코딩된 이미지 프레임의 개별 해시를 포함하는 경우, 상기 수신된 데이터 구조를 이용하여 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지를 검증하는 단계는:

- 상기 수신된 비디오 시퀀스에 포함된 각각의 수신된 인코딩된 이미지 프레임의 무손실 압축을 수행하여 각각의 LC 수신된 인코딩된 이미지 프레임을 획득하는 단계;
- 획득된 모든 각각의 LC 수신된 인코딩된 이미지 프레임의 개별 해시를 생성하는 단계;
- 상기 수신된 데이터 구조에 의해 주어진 상기 모든 LC 인코딩된 이미지 프레임에 대한 개별 해시를 생성하는 단계; 및
- 상기 수신된 데이터 구조에 의해 주어진 모든 LC 인코딩된 이미지 프레임에 대한 상기 생성된 개별 해시가 획득된 모든 각각의 LC 수신된 인코딩된 이미지 프레임의 상기 생성된 개별 해시와 일치할 때, 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지 검증하는 단계를 포함하는, 방법.

청구항 10

제9항에 있어서,

상기 작은 LC 인코딩된 이미지 프레임 중 하나 이상은 제1 유형의 작은 LC 인코딩된 이미지 프레임이고, 각각의 전송된 인코딩된 이미지 프레임과 동일하거나 상기 인코딩된 이미지 프레임의 상기 LC 인코딩된 이미지 프레임과 동일하며, 상기 수신된 데이터 구조는 상기 제1 유형의 작은 LC 인코딩된 이미지 프레임의 데이터 구조에서

의 위치 및 선택적인 크기를 지정하는 정보를 더 포함하고, 상기 수신된 데이터 구조에 의해 주어진 모든 LC 인코딩된 이미지에 대한 개별 해시를 생성하는 단계는:

- 상기 수신된 데이터 구조로부터, 상기 제1 유형의 작은 LC 인코딩된 이미지 프레임 및 상기 송신기에 의해, 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 상기 다른 모든 LC 인코딩된 이미지 프레임의 개별 해시를 추출하는 단계;
- 상기 제1 유형의 상기 추출된 작은 LC 인코딩된 이미지 프레임을 개별적으로 해싱함으로써 개별 해시를 생성하는 단계; 및
- 상기 추출된 제1 유형의 작은 LC 인코딩된 이미지 프레임의 상기 생성된 개별 해시와 상기 다른 모든 인코딩된 이미지 프레임의 추출된 개별 해시의 조합으로서 모든 LC 인코딩된 이미지 프레임에 대한 개별 해시를 생성하는 단계를 포함하는, 방법.

청구항 11

제9항에 있어서,

상기 작은 LC 인코딩된 이미지 프레임 중 하나 이상은 제2 유형의 작은 LC 인코딩된 이미지 프레임이고, 저장된 미리 정의된 인코딩된 이미지 프레임의 식별자 및 상기 각각 전송된 인코딩된 이미지 프레임과 상기 저장된 미리 정의된 인코딩된 이미지 프레임간의 가능한 차이를 포함하며, 상기 수신된 데이터 구조는 상기 제2 유형의 작은 LC 인코딩된 이미지 프레임의 데이터 구조에서의 위치 및 선택적인 데이터 크기를 지정하는 정보를 더 포함하고, 상기 수신된 데이터 구조에 의해 주어진 상기 모든 LC 인코딩된 이미지 프레임에 대한 개별 해시를 생성하는 단계는:

상기 수신된 데이터 구조로부터 다음을 추출하는 단계:

상기 제2 유형의 각 작은 LC 인코딩된 이미지 프레임에 대해, 상기 저장된 인코딩된 이미지 프레임의 식별자 및 상기 각각 전송된 인코딩된 이미지 프레임과 상기 저장된 인코딩된 이미지 프레임 간의 가능한 차이; 및

상기 다른 모든 LC 인코딩된 이미지 프레임의 개별 해시;

상기 비디오 시퀀스의 송신기 및 수신기에 액세스 가능한 데이터 저장부로부터, 상기 추출된 식별자를 이용하여 상기 저장된 미리 정의된 인코딩된 이미지 프레임을 검색하는 단계;

상기 검색된 저장된 미리 정의된 인코딩된 이미지 프레임과 상기 가능한 차이를 결합함으로써, 상기 제2 유형의 LC 인코딩된 이미지 프레임의 각각에 대해 각각 전송된 인코딩된 이미지 프레임을 재구성하는 단계;

상기 재구성된 전송된 인코딩된 이미지 프레임의 무손실 압축을 수행하는 단계;

상기 LC 재구성된 전송된 인코딩된 이미지 프레임을 개별적으로 해싱함으로써 개별 해시를 생성하는 단계;

상기 LC 재구성된 전송된 인코딩된 이미지 프레임의 상기 생성된 개별 해시 및 상기 다른 모든 LC 인코딩된 이미지 프레임의 상기 추출된 개별 해시를 포함하도록 추가 데이터 구조를 생성하는 단계를 포함하는, 방법.

청구항 12

제7항에 있어서,

상기 수신된 데이터 구조는, 상기 송신기에 의해, 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모든 LC 인코딩된 이미지 프레임의 개별 해시를 포함하는 경우, 상기 수신된 데이터 구조를 이용하여 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지 확인하는 단계는:

- 상기 수신된 비디오 시퀀스에 포함된 각각의 수신된 인코딩된 이미지 프레임의 무손실 압축을 수행하여 각각의 LC 수신된 인코딩된 이미지 프레임을 획득하는 단계;

- 다음을 포함하는 데이터 구조를 생성하는 단계;

각각이 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 것으로 식별된 하나 이상의 작은 LC 수신된 인코딩된 이미지 프레임, 및

상기 송신기에 의해, 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 다른 모든 LC 수신된 인코딩된 이미지 프레임의 개별 해시 - 상기 개별 해시는 상기 송신기에 의해, 상기 하나 이상의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않은 상기 다른 모든 LC 수신된 인코딩된 이미지 프레임 각각을 개별적으로 해싱함으로써 획득됨 - , 및

- 상기 생성된 데이터 구조가 상기 수신된 데이터 구조와 일치할 때 상기 수신된 인코딩된 이미지 프레임이 상기 전송된 인코딩된 이미지 프레임과 동일한지 확인하는 단계를 포함하는, 방법.

청구항 13

제7항에 있어서,

상기 수신기는 상기 송신기의 개인-공개키 쌍 중 공개키에 액세스하고,

상기 수신된 디지털 서명을 검증하는 단계는, 상기 공개키를 이용하여 상기 수신된 디지털 서명을 복호화하고, 상기 수신된 데이터 구조의 해시가 복호화된 것으로서 상기 수신된 디지털 서명과 일치하는 경우 상기 수신된 디지털 서명을 검증하는 단계를 포함하는, 방법.

청구항 14

데이터 구조 및 디지털 서명을 갖는 비디오 시퀀스를 제공함으로써 비디오 시퀀스의 검증을 가능하게 하는 송신기로서, 상기 송신기가 제1항에 따른 단계를 수행하게 하도록 구성된 프로세싱 회로를 포함하는, 송신기.

청구항 15

데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스를 검증하기 위한 수신기로서, 상기 수신기가 제7항에 따른 단계를 수행하게 하도록 구성된 프로세싱 회로를 포함하는, 수신기.

발명의 설명

기술 분야

[0001] 본 발명은 비디오 시퀀스의 검증을 가능하게 하는 송신기 및 그 방법에 관한 것이다. 또한, 본 발명은 비디오 시퀀스를 검증하기 위한 수신기 및 그 방법에 관한 것이다. 특히, 검증은 비디오 시퀀스에 데이터 구조와 디지털 서명을 제공함으로써 가능하다.

배경 기술

[0002] 디지털 서명은 송신기에서 수신기로 비보안 채널을 통해 전송되는 인코딩된 이미지 프레임을 포함하는 비디오 시퀀스와 같은 디지털 메시지에 유효성 검사 및 보안 계층을 제공한다. 송신기는 개인-공개 암호화 키 쌍의 개인 암호화 키를 이용하여 비디오 시퀀스의 하나 이상의 암호화 해시 값을 암호화함으로써 디지털 서명을 생성할 수 있다. 암호화 해시 값은 프레임별 암호화 해시 값일 수 있으며, 각 암호화 해시 값은 각각의 인코딩된 이미지 프레임의 이미지 데이터의 해시 값이거나, 선택적 추가 정보와 결합된 해당 인코딩된 이미지 프레임의 이미지 데이터의 해시 값일 수 있다. 일반적으로 생성된 디지털 서명과 디지털 서명을 생성하는데 사용되는 프레임별 암호화 해시 값은 비디오 시퀀스를 수신기로 전송하기 전에 송신기에 의해 비디오 시퀀스에 제공된다.

[0003] 수신된 비디오 시퀀스가 혐의가 있는(alleged) 송신기의 실제 비디오 시퀀스이고 수신된 비디오 시퀀스가 조작되지 않았는지 확인하려면, 수신기는 디지털 서명과 수신된 인코딩된 이미지 프레임을 모두 확인해야 한다.

[0004] 수신된 디지털 서명을 확인하기 위해, 비디오 시퀀스에 대한 수신기는 송신기의 개인-공개 암호화 키 쌍의 공개

키를 이용하여 수신된 디지털 서명을 복호화하고, 복호화된 수신된 디지털 서명을 수신된 하나 이상의 암호화 해시 값과 비교한다. 복호화된 수신된 디지털 서명이 수신된 암호화 해시 값과 동일(예: 일치)하는 경우, 수신된 디지털 서명은 확인된다. 이로써, 수신기가 수신한 비디오 시퀀스가 혐의가 있는 송신기에 의해 디지털 서명된 것으로 확인한다.

[0005] 디지털 서명의 검증 외에도, 수신기는 수신된 비디오 시퀀스가 송신기에서 전송한 비디오 시퀀스와 동일한지 확인해야 한다. 수신된 인코딩된 이미지 프레임의 시퀀스를 확인하는 한 가지 방법은 송신기가 암호화 해시 값을 생성한 것과 동일한 방식으로 수신기가 수신된 비디오 시퀀스에서 인코딩된 이미지 프레임의 암호화 해시 값을 생성하는 것이다. 따라서, 암호화 해시 값을 생성하는 방법에 대해 송신기와 수신기 간에 합의가 있다. 수신기가 암호화 해시 값을 생성하면, 수신기는 자신이 생성한 암호화 해시 값과 수신된 암호화 해시 값을 비교하고, 이들이 서로 동일(예: 서로 일치)하면, 수신된 비디오 시퀀스는 전송된 비디오 시퀀스와 동일한 것으로 확인된다.

[0006] 그러나, 디지털 서명을 추가하고, 특히 암호화 해시 값을 비디오 시퀀스에 추가하면, 비디오 시퀀스를 전송하는데 필요한 비트율은 증가한다. 사용 가능한 비트율은 통신 채널을 통해 비디오 시퀀스를 전송할 때 제한 요소가 될 수 있으므로, 수신기가 비디오 시퀀스를 검증하는 능력을 희생하거나 저하시키지 않고 디지털 서명 및 암호화 해시 값을 전송하는데 필요한 비트율을 줄일 필요가 있다.

발명의 내용

해결하려는 과제

[0007] 상기 관점에서 볼 때, 본 발명의 목적은 종래 기술의 단점을 완화하고 종래 기술과 비교하여 비디오 시퀀스를 전송하기 위해 필요한 비트율과 검증에 필요한 추가 데이터를 감소시켜 비디오 시퀀스의 검증을 가능하게 하는 것이다. 또 다른 목적은 추가 데이터의 크기를 줄여 전송에 필요한 비트율을 줄이는 것이다. 또 다른 목적은 데이터 구조 및 디지털 서명으로서 비디오 시퀀스에 추가 데이터를 제공하는 것이며, 데이터 구조와 디지털 서명은 비디오 시퀀스를 검증할 수 있도록 하는 동시에 전송을 위해 사용 가능한 비트율 리소스의 양을 줄이는 것이다. 또 다른 목적은 이러한 기능들을 갖춘 송신기와 컴퓨터 프로그램을 제안하는 것이다. 추가 목적은 데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스의 유효성 검사를 수행하는 것이다. 또 다른 목적은 이러한 기능을 갖춘 수신기와 컴퓨터 프로그램을 제안하는 것이다.

[0008] 이들 목적 중 적어도 일부는 독립 청구항들에 의해 정의된 본 발명에 의해 달성된다. 종속 청구항들은 바람직한 실시예에 관한 것이다.

과제의 해결 수단

[0009] 본 개시의 제1 양태에 따르면, 데이터 구조 및 디지털 서명을 갖는 비디오 시퀀스를 제공함으로써 비디오 시퀀스의 검증을 가능하게 하는 송신기에 의해 수행되는 방법이 제공되며, 상기 비디오 시퀀스는 인코딩된 이미지 프레임을 포함한다.

[0010] 상기 방법은 각각의 무손실 압축(losslessly compressed, LC) 인코딩된 이미지 프레임을 획득하기 위해 비디오 시퀀스의 각 인코딩된 이미지 프레임의 무손실 압축을 수행하는 단계를 포함한다.

[0011] 또한, 상기 방법은 획득된 LC 인코딩된 이미지 프레임 중에서, 각각이 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 하나 이상의 작은 LC 인코딩된 이미지 프레임을 식별하는 단계를 포함한다.

[0012] 더욱이, 상기 방법은 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임, 및 다음 중 하나: 각각의 작은 LC 인코딩된 이미지 프레임이 결여된 모든 인코딩된 이미지 프레임; 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임의 개별 해시를 포함하는 데이터 구조를 생성하는 단계를 포함한다. 개별 해시는 각각의 작은 LC 인코딩된 이미지 프레임이 결여된 모든 인코딩된 이미지 프레임을 개별적으로 해싱하거나, 다른 모든 획득된 LC 인코딩된 이미지 프레임 각각을 개별적으로 해싱함으로써 획득된다.

[0013] 또한, 상기 방법은 비디오 시퀀스에 대한 디지털 서명을 생성하는 단계; 및 데이터 구조 및 디지털 서명을 비디오 시퀀스에 제공하는 단계를 포함한다. 이로써 수신기는 비디오 시퀀스를 검증할 수 있게 된다.

[0014] 무손실 압축을 수행하고 식별된 작은 LC 인코딩된 이미지 프레임을 각각의 해시 대신 데이터 구조에 포함함으로

써, 비디오 시퀀스를 검증할 때 데이터 구조의 유용성을 손상시키지 않고 데이터 구조의 크기를 줄일 수 있다.

[0015] 본 개시에서, "데이터 구조"라는 용어는 비디오 시퀀스에 제공되도록 구성되고, 몇 가지 예를 들면, 텍스트의 텍스트 시퀀스로서, 예를 들어 비트스트림인 바이너리 시퀀스로서, 예를 들어 바이트 스트림인 바이트 시퀀스로서, 또는 이들의 조합으로서 임의의 구조, 요소 또는 유닛으로 이해되어야 한다. 때때로 데이터 구조를 문서라고도 한다. 데이터 구조는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 하나 이상의 개별 헤시를 포함하도록 구성된다. 또한, 데이터 구조는 메타데이터, 즉 데이터 구조에 포함된 정보와 관련될 수 있는 데이터를 포함할 수 있다. 따라서, 메타데이터는 하나 이상의 작은 LC 인코딩된 이미지 프레임 및/또는 하나 이상의 개별 헤시와 관련될 수 있다. 아래에 설명되는 것처럼, 때때로 데이터 구조는 하나 이상의 작은 LC 인코딩된 이미지 프레임의 위치에 대한 정보와 또한 선택적인 크기도 포함한다. 따라서, 위치와 크기는 데이터 구조에 포함될 수 있는 메타데이터의 두 가지 예이다. 메타데이터의 또 다른 예는 작은 LC 인코딩된 이미지 프레임 유형이다. 아래에 설명되는 바와 같이, 작은 LC 인코딩된 이미지 프레임은 제1 유형 또는 제2 유형일 수 있으며, 결과적으로 이 정보는 메타데이터로서 데이터 구조에 포함될 수 있다.

[0016] 본 명세서에서 사용되는 "각각의 작은 LC 인코딩된 이미지 프레임이 결합된 모든 인코딩된 이미지 프레임"이라는 표현은 획득된 각각의 LC 인코딩된 이미지 프레임이 각각의 작은 LC 인코딩된 이미지 프레임으로 식별되지 않는 모든 인코딩된 이미지 프레임으로 이해되어야 한다. 다시 말하면, 각각의 작은 LC 인코딩된 이미지 프레임이 결합된 모든 인코딩된 이미지 프레임은 작은 LC 인코딩된 이미지 프레임이 아닌 각각의 LC 인코딩된 이미지 프레임을 갖는다. 따라서, 각각의 작은 LC 인코딩된 이미지 프레임이 결합된 모든 인코딩된 이미지 프레임의 각각의 LC 인코딩된 이미지 프레임의 데이터 크기는 미리 정의된 바이트 수보다 작지 않지만, 대신에 데이터 크기는 미리 정의된 바이트 수와 동일하거나 더 크다.

[0017] 본 명세서에서 사용되는 "작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 LC 인코딩된 이미지 프레임"의 표현은 획득된 LC 인코딩된 이미지 프레임이 작은 LC 인코딩된 이미지 프레임으로 식별되지 않는 것으로 이해되어야 한다. 따라서, 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 LC 인코딩된 이미지 프레임은 각각 미리 결정된 바이트 수보다 작지 않은 데이터 크기를 갖지만, 대신에 미리 결정된 바이트 수보다 크거나 같은 데이터 크기를 갖는다.

[0018] 본 문서에서 사용되는 "디지털 서명"은 송신기의 신원을 확인하기 위해 전송된 비디오 시퀀스에 제공되는 디지털 코드를 의미한다. 디지털 코드는 개인/공개 키 암호화를 통해 생성되고 인증된다. 구체적으로 송신기는 송신기의 암호화 키 쌍 중 개인 키를 이용하여 디지털 코드를 생성하고, 수신기는 송신기의 암호화 키 쌍 중 공개 키를 이용하여 디지털 코드를 인증한다.

[0019] 본 명세서에서 사용되는 "각 인코딩된 이미지 프레임의 무손실 압축을 수행하는"이라는 표현은 이미지 정보의 손실 없이 각 인코딩된 이미지 프레임을 압축된 인코딩된 이미지 프레임으로 압축하는 것을 의미한다. 압축된 인코딩된 이미지 프레임은 인코딩된 이미지 프레임과 동일하거나 더 작은 데이터 크기를 가질 수 있다. 때때로, 압축된 인코딩된 이미지 프레임은 인코딩된 이미지 프레임보다 더 큰 데이터 크기를 가지며, 이러한 경우 인코딩된 이미지 프레임은 압축된 인코딩된 이미지 프레임으로 사용될 수 있다. 다른 경우에, 무손실 압축은 다른 인코딩된 이미지 프레임에 대한 참조를 포함하는 압축된 인코딩된 이미지 프레임을 초래할 수 있다. 다른 인코딩된 이미지 프레임은 비디오 시퀀스의 이전에 인코딩된 이미지 프레임이거나 저장된 인코딩된 이미지 프레임일 수 있다. 중요한 것은, 무손실 압축을 수행할 때 이미지 정보가 손실되지 않는다는 것이다. 무손실 압축에서는 이미지 정보가 손실되지 않으므로, 원래의 인코딩된 이미지 프레임을 이미지 품질의 손실 없이 압축된 인코딩된 이미지에서 완벽하게 재구성할 수 있다. 압축된 인코딩된 이미지 프레임으로부터 원래의 인코딩된 이미지 프레임을 재구성하는 동작은 압축된 인코딩된 이미지 프레임을 원래의 인코딩된 이미지 프레임으로 압축 해제하는 것으로 지칭될 수 있다. 압축된 인코딩된 이미지 프레임은 본 개시에서 무손실 압축(losslessly compressed, LC) 인코딩된 이미지 프레임으로 지칭된다.

[0020] 무손실 압축 알고리즘의 예로는 허프만 코딩(Huffman coding), 산술 인코딩(arithmetic encoding), 코드북 기반 인코딩(codebook-based encoding) 및 실행-길이 인코딩(run-length encoding)이 있다. 전술한 바와 같은 무손실 압축을 수행하는 장치를 본 명세서에서는 인코딩된 이미지 프레임의 무손실 압축을 수행하도록 구성된 무손실 압축 모듈이라 지칭한다.

[0021] 본 개시에서 "무손실 압축(LC) 인코딩된 이미지 프레임"은 인코딩된 이미지 프레임의 무손실 압축으로 인한 이미지 프레임을 의미한다.

- [0022] "인코딩된 이미지 프레임에 개별 해싱"의 표현은 개별 해시를 획득하기 위해 각 개별 인코딩된 이미지 프레임에 해시 함수(또는 단방향 함수)를 적용하는 것을 의미한다. 해시 함수는 서명될 비디오 시퀀스의 민감도 및/또는 비디오 시퀀스가 승인되지 않은 당사자에 의해 조작되는 경우 위태로운 가치의 관점에서 적절하다고 간주되는 안전 수준을 제공하는 암호화 해시 함수일 수 있다. 해시 함수의 세 가지 예로는 Secure Hash Algorithm 256비트(SHA-256), Secure Hash Algorithm3 512비트(SHA3-512) 및 Rivest-Shamir-Adleman 1024비트(RSA-1024)가 있다. 해시 함수는 디지털 서명 및/또는 데이터 구조가 수신기에 의해 검증될 때 개별 해시가 재생성될 수 있도록 미리 정의(예: 재현 가능해야 함)되어야 한다.
- [0023] 본 명세서에서 사용되는 "개별 해시"는 개별 인코딩된 이미지 프레임 또는 개별 LC 인코딩된 이미지 프레임에 해시 함수를 적용함으로써 획득된 개별 암호화 해시 값을 의미한다.
- [0024] 본 개시의 제2 양태에 따르면, 데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스를 검증하기 위해 수신기에 의해 수행되는 방법이 제공되며, 여기서 비디오 시퀀스는 인코딩된 이미지 프레임을 포함한다.
- [0025] 상기 방법은, 송신기로부터, 인코딩된 이미지 프레임을 포함하고 데이터 구조와 디지털 서명이 제공되는 비디오 시퀀스를 수신하는 단계를 포함한다.
- [0026] 수신된 데이터 구조는:
- [0027] 하나 이상의 작은 무손실 압축된(LC) 인코딩된 이미지 프레임 - 여기서 각각의 작은 LC 인코딩된 이미지 프레임은 미리 정의된 바이트 수보다 작고, 상기 송신기로부터 전송된 비디오 시퀀스에 포함된 각각 전송된 인코딩된 이미지 프레임의 LC 버전인 데이터 크기를 가짐 - ; 및
- [0028] 각각의 작은 LC 인코딩된 이미지 프레임이 결합된 전송된 모든 인코딩된 이미지 프레임; 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 LC 인코딩된 이미지 프레임 중 하나의 개별 해시를 포함한다. 다른 모든 LC 인코딩된 이미지 프레임 각각은 전송된 비디오 시퀀스에 포함된 각각의 전송된 인코딩된 이미지 프레임의 LC 버전이다.
- [0029] 또한, 상기 방법은 수신된 데이터 구조를 이용하여 수신된 디지털 서명을 검증하는 단계; 및 수신된 데이터 구조를 이용하여 수신된 인코딩된 이미지 프레임이 전송된 인코딩된 이미지 프레임과 동일한지 검증하는 단계를 포함한다. 이로써 수신된 디지털 서명 및 수신된 인코딩된 이미지 프레임이 검증될 때, 수신된 비디오 시퀀스는 전송된 비디오 시퀀스와 동일한지가 검증된다.
- [0030] 본 개시의 제3 양태에 따르면, 비디오 시퀀스에 데이터 구조 및 디지털 서명을 제공함으로써 비디오 시퀀스의 검증을 가능하게 하기 위한 송신기가 제공되며, 여기서 송신기는 송신기로 하여금 제1 양태의 방법의 단계들 중 임의의 것을 수행하게 하도록 구성된 프로세싱 회로를 포함한다.
- [0031] 본 개시의 제4 양태에 따르면, 데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스를 검증하기 위한 수신기가 제공되며, 여기서 수신기는 수신기로 하여금 제2 양태의 방법의 단계들 중 임의의 것을 수행하도록 구성된 프로세싱 회로를 포함한다.
- [0032] 본 개시의 제5 양태에 따르면, 처리 능력을 갖는 장치에 의해 실행될 때, 제1 양태의 방법을 수행하도록 적응된 컴퓨터 코드 명령어들이 저장되어 있는 비일시적 컴퓨터 판독 가능 매체가 제공된다.
- [0033] 본 개시의 제6 양태에 따르면, 처리 능력을 갖는 장치에 의해 실행될 때, 제2 양태의 방법을 수행하도록 적응된 컴퓨터 코드 명령어들이 저장되어 있는 비일시적 컴퓨터 판독 가능 매체가 제공된다.
- [0034] 제2, 제3, 제4, 제5 및 제6 양태는 일반적으로 제1 양태와 동일한 특징 및 장점을 가질 수 있다.
- [0035] 본 개시는 또한 컴퓨터가 위의 방법 중 하나를 수행하도록 하는 명령어들을 포함하는 컴퓨터 프로그램에 관한 것이다. 컴퓨터 프로그램은 데이터 매체에 저장되거나 배포될 수 있다. 본 명세서에 사용된 바와 같이, "데이터 매체(data carrier)"는 변조된 전자기파 또는 광파와 같은 임시 데이터 매체 또는 비일시적 데이터 매체일 수 있다. 비일시적 데이터 매체에는 자기, 광학 또는 솔리드 스테이트 유형의 영구 및 비영구 저장 매체와 같은 휘발성 및 비휘발성 메모리가 포함된다. 여전히 "데이터 매체"의 범위 내에서 이러한 메모리는 고정적으로 장착되거나 휴대 가능하다.
- [0036] 일반적으로, 청구범위에 사용된 모든 용어는 본 명세서에서 명백하게 다르게 정의되지 않는 한, 기술 분야에서의 통상적인 의미에 따라 해석되어야 한다. "a/an/the 요소, 장치, 구성 요소, 수단, 단계 등"에 대한 모든 언급은 명시적으로 언급되지 않는 한, 요소, 장치, 구성요소, 수단, 단계 등의 적어도 하나의 인스턴스를 언급하

는 것으로 공개적으로 해석되어야 한다. 본 명세서에 개시된 임의의 방법의 단계는 명백하게 언급되지 않는 한, 개시된 정확한 순서로 수행될 필요는 없다. 또한, 본 발명은 명백하게 언급되지 않는 한, 본 명세서에 개시된 특징들의 모든 가능한 조합에 관한 것임을 또한 주목해야 한다.

도면의 간단한 설명

[0037] 본 발명의 추가적인 목적, 특징 및 이점은 첨부된 도면을 참조하여 본 발명의 실시예에 대한 다음의 예시적이고 비제한적인 상세한 설명을 통해 더 잘 이해될 것이며, 여기서 유사한 구성요소에 대하여 동일한 참조 번호가 사용될 것이다.

도 1은 비디오 시퀀스의 검증을 가능하게 하고 비디오 시퀀스를 검증하기 위한 시스템의 실시예를 개략적으로 예시한다.

도 2a는 실시예에 따른 비디오 시퀀스를 개략적으로 예시한다.

도 2b는 실시예에 따른 인코딩된 이미지 프레임의 시퀀스, 해당 LC 인코딩된 이미지 프레임의 시퀀스 및 데이터 구조 내용의 두 가지 예를 개략적으로 예시한다.

도 3은 실시예에 따른 송신기를 개략적으로 예시한다.

도 4는 실시예에 따른 수신기를 개략적으로 예시한다.

도 5는 실시예에 따른 비디오 시퀀스의 검증을 가능하게 하기 위해 송신기에 의해 수행되는 방법의 흐름도이다.

도 6은 실시예에 따라 비디오 시퀀스를 검증하기 위해 수신기에 의해 수행되는 방법의 흐름도이다.

도 7a-7c는 실시예에 따라 수신된 인코딩된 이미지 프레임을 검증하기 위해 수신기에 의해 수행되는 하위 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0038] 이제 본 개시의 양태는 본 발명의 특정 실시예가 도시되어 있는 첨부 도면을 참조하여 이하에서 더 완전하게 설명될 것이다. 그러나 이러한 양태는 다양한 형태로 구현될 수 있으며 제한적인 것으로 해석되어서는 안 된다. 오히려, 이들 실시예는 본 개시가 철저하고 완전할 것이며, 본 발명의 모든 양태의 범위가 당업자에게 완전하게 전달되도록 예시로서 제공된다. 유사한 숫자는 설명 전반에 걸쳐 유사한 요소를 나타낸다.

[0039] 통신 네트워크를 통해 비디오 시퀀스를 전송할 때, 특히 비디오 시퀀스의 검증을 가능하게 하는 추가 데이터와 함께 비디오 시퀀스를 전송할 때, 비트율 가용성의 제약을 극복하거나 완화하기 위해, 본 발명은 검증의 신뢰성을 저하시키지 않으면서 추가 데이터의 크기를 줄이는 방법에 관한 것이다. 본 개시에서 추가 데이터는 데이터 구조 및 전자 서명이다. 특히, 본 발명은 검증 신뢰성을 유지하면서 데이터 구조의 콘텐츠의 크기를 줄임으로써 데이터 구조의 크기를 줄이는 것에 관한 것이다.

[0040] 데이터 구조 및 디지털 서명이 제공되는 비디오 시퀀스의 검증을 가능하게 하는 방법과 비디오 시퀀스를 검증하는 방법에 대해 자세히 설명하기 전에, 본 발명이 실현될 수 있는 시스템의 구성 요소에 대해 설명한다.

[0041] 도 1을 참조하여, 비디오 시퀀스의 검증을 가능하게 하고 비디오 시퀀스를 검증하기 위한 시스템(100)의 실시예가 설명될 것이다. 시스템(100)은 비디오 시퀀스의 검증을 가능하게 하도록 구성된 송신기(110)를 포함한다. 송신기(110)는 하나 이상의 카메라(112)를 포함하거나 이에 연결될 수 있다. 또는, 송신기(110)는 카메라(112)에 포함될 수 있다. 송신기(110) 및 하나 이상의 카메라(112)는 카메라 시스템으로 지칭될 수 있다. 카메라 시스템은 하나의 단일 유닛, 즉 송신기(110)와 하나 이상의 카메라(112)를 포함하는 하나의 유닛, 또는 여러 개의 개별 유닛으로 구성될 수 있다. 카메라(112)는 감시 카메라(때때로 감시 카메라라고도 함)일 수 있다. 또한, 카메라(112)는 고정식 카메라와 같은 고정형 카메라일 수도 있고, PTZ(Pan, Tilt and Zoom) 카메라와 같은 이동식 카메라일 수도 있다. 카메라(112)는 가시광선 카메라, 열화상 카메라, 또는 가시광선 카메라와 열화상 카메라를 모두 포함하는 카메라일 수 있다. 카메라(112)는 예를 들어, 캡처 모듈과 같은 이미지 캡처 및 인코딩 모듈과 같은 이미지 프로세싱과 관련된 여러 구성요소를 포함할 수 있으며, 이는 기존 카메라 시스템에서 일반적으로 그 목적과 동작이 해당 분야에 대한 통상의 기술을 가지고 있는 이들에게 잘 알려져 있다는 점에 유의해야 한다. 이러한 구성요소는 명확성을 이유로 도 1의 예시 및 설명에서 생략되었다.

[0042] 도 1에 추가로 도시된 바와 같이, 송신기(110)는 통신 네트워크(120)를 통해 수신기(130)와 통신하도록 구성된

다. 통신 네트워크(120)는 송신기(110)가 비디오 시퀀스를 수신기(130)로 전송하는 유선 또는 무선 통신 네트워크일 수 있다. 수신기(130)는 수신기(130)에 의해 수신된 비디오 시퀀스를 운영자에게 표시하도록 구성된 디스플레이 장치(150)를 포함하거나 이에 연결될 수 있다. 송신기(110) 및 수신기(130)는 데이터 저장부(122)와 직접 또는 통신 네트워크(120)를 통해 통신하도록 구성된다. 데이터 저장부(122)는 인코딩된 이미지 프레임 및/또는 LC 인코딩된 이미지 프레임에 관한 데이터, 예를 들면 비디오 시퀀스에 관한 데이터를 저장하도록 구성될 수 있다. 예를 들어, 데이터 저장부(122)는 미리 정의된 인코딩된 이미지 프레임(220e)을 포함할 수 있다. 미리 정의된 인코딩된 이미지 프레임(220e)은 룩업 테이블로서 데이터 저장부(122)에 저장될 수 있으며, 여기서 각각의 저장된 미리 정의된 인코딩된 이미지 프레임(220e)은 때때로 인덱스 또는 키로 지칭되는 식별자에 의해 식별된다. 일부 실시예에서, 룩업 테이블은 코드북이고, 인덱스/키는 코드워드이다. 데이터 저장부(122)는 비휘발성 메모리일 수 있다. 또한, 데이터 저장부는 공통 라이브러리를 포함할 수 있다.

[0043] 송신기(110)와 통신 네트워크(120) 사이, 통신 네트워크(120)와 수신기(130) 사이, 그리고 데이터 저장부(122), 송신기(120), 통신 네트워크(120) 및 수신기(130) 사이의 전송을 위해 사용될 수 있는 무선 및 유선 전송 모델의 많은 조합이 있다는 것을 이해해야 하고, 도 1은 단지 하나의 예만 보여준다.

[0044] 도 2a는 실시예에 따른 예시적인 비디오 시퀀스(200)를 개략적으로 도시한다. 비디오 시퀀스(200)는 다수의 인코딩된 이미지 프레임(220)을 포함한다. 다른 프레임을 예측-코딩하기 위한 참조로서 사용되는 인코딩된 이미지 프레임을 참조 프레임이라 한다. 다른 프레임의 정보 없이 인코딩된 프레임을 인트라 코딩된 프레임, 인트라 프레임, I-프레임 또는 키 프레임이라고 한다. 하나 이상의 참조 프레임에서 예측을 사용하는 프레임을 인터 코딩된 프레임(inter-coded frame) 또는 인터 프레임(inter-frame)이라고 한다. P-프레임은 하나 이상의 이전 참조 프레임(또는 각 영역의 예측을 위한 하나 이상의 프레임)으로부터 예측을 사용하는 인터 프레임이고, B-프레임은 두 개의 참조 프레임, 하나 이상의 이전 프레임 및/또는 하나 이상의 후속 프레임(가중될 수 있는) 평균으로부터의 예측을 사용하는 인터 프레임이다. 프레임은 픽처라고도 한다.

[0045] 인코딩된 이미지 프레임(220)은 하나 이상의 GOP(Group of Picture)로 배열될 수 있다. 도 2a에서, 인코딩된 이미지 프레임(220)은 복수의 GOP들로 배열될 수 있으며, 그 중 제1 GOP(210a) 및 제2 GOP(210b)가 도시된다. 예시적인 비디오 시퀀스(200)에 개략적으로 도시된 바와 같이, 제1 GOP(210a)는 제1 I-프레임(I0), 제1 P-프레임(P00), 제2 P-프레임(P01) 및 제3 P-프레임(P02)으로 구성되며; 제2 GOP(210b)는 제1 I-프레임(I1), 제1 P-프레임(P10), 제2 P-프레임(P11) 및 제3 P-프레임(P12)으로 구성된다.

[0046] 기존의 비디오 인코딩 프로토콜에는 여러 가지가 있다. 본 발명의 다양한 실시예와 함께 동작하는 몇 가지 일반적인 비디오 인코딩 프로토콜은 몇 가지 예를 들자면, 다음을 포함한다: H.265 및 MPEG-H Part 2로도 알려진 HEVC(High Efficiency Video Coding); H.264 및 MPEG-4 Part 10이라고도 알려진 AVC(고급 비디오 코딩) H.266, MPEG-I Part 3 및 FVC(Future Video Coding)라고도 알려진 VVC(다용도 비디오 코딩) VP9, VP10 및 AOMedia Video 1(AV1).

[0048] 데이터 구조(320) 및 디지털 서명(340)을 갖는 비디오 시퀀스(200)를 제공함으로써 비디오 시퀀스(200)의 검증을 가능하게 하기 위해 송신기(110)에 의해 수행되는 방법은 이제 도 5의 흐름도를 참조하고, 실시예에 따라 송신기(110)를 개략적으로 예시하는 도 3을 참조하여 설명될 것이다. 실시예에 따른 인코딩된 이미지 프레임의 시퀀스, 대응하는 LC 인코딩된 이미지 프레임의 시퀀스 및 실시 예에 따른 데이터 구조 콘텐츠의 두 가지 예를 개략적으로 예시하는 도 2b도 참조될 것이다.

[0049] 앞서 언급한 바와 같이, 비디오 시퀀스(200)는 인코딩된 이미지 프레임(220)을 포함하고, 비디오 시퀀스(200)는 적어도 하나의 픽처 그룹(GOP)(210a, 210b)으로 구성될 수 있다. 도 2b에 도시된 바와 같이, 인코딩된 이미지 프레임의 시퀀스는 인코딩된 이미지 프레임들(I0, P00, P01, P02, I1, P10, P11, P12, P13 및 I2)을 포함할 수 있으며, 여기서 인코딩된 이미지 프레임들(I0, P00, P01, P02)은 하나의 GOP에 포함될 수 있고, 인코딩된 이미지 프레임들(I1, P10, P11, P12, P13)은 또 다른 GOP에 포함될 수 있고, 인코딩된 이미지 프레임(I2)은 또 다른 GOP에 포함될 수 있다.

[0050] 비디오 시퀀스(200)의 인코딩된 이미지 프레임(220)은 장면을 묘사하는 다수의 이미지 프레임을 캡처하고, 캡처된 이미지 프레임을 인코딩된 이미지 프레임(220)으로 인코딩한 카메라(112)로부터 획득될 수 있다. 카메라(112)는 송신기(110)의 획득 모듈에 인코딩된 이미지 프레임(220)을 제공할 수 있다. 카메라(112)가 송신기(110)(이하 카메라 시스템(110)으로 지칭됨)에 포함되는 경우에, 카메라(112)는 송신기(110)의 획득 모듈을 구현한다. 다른 경우에 여기서, 카메라(112)는 송신기(110)의 외부에 있고 송신기(110)에 연결되어 있으며, 송신기(110)의 획득 모듈(114)은 카메라(112)로부터 인코딩된 이미지 프레임(220)을 수신하고, 수신된 인코딩된 이

미지 프레임(220)을 내부 데이터 저장부에 저장하도록 구성된 내부 데이터 저장부(220)에 의해 실현될 수 있다.

- [0051] 단계 S502에서, 송신기(110)는 비디오 시퀀스(200)의 각 인코딩된 이미지 프레임(220)의 무손실 압축을 수행하여, 각각의 LC 인코딩된 이미지 프레임(220LC)을 획득한다. 이는 무손실 압축이 수행된 인코딩된 이미지 프레임(220)의 크기와 같거나 작은 크기를 갖는 각각의 LC 인코딩된 이미지 프레임을 얻는 동시에 무손실 압축이 수행된 인코딩된 이미지 프레임(220)과 동일한 이미지 품질을 갖는 각각의 LC 인코딩된 이미지 프레임을 획득하기 위해 수행된다. 도 2b에 도시된 바와 같이, LC 인코딩된 이미지 프레임의 시퀀스는 LC 인코딩된 이미지 프레임들(I_{0LC}, P_{00LC}, P_{01LC}, P_{02LC}, I_{1LC}, P_{10LC}, P_{11LC}, P_{12LC}, P_{13LC} 및 I_{2LC})을 포함한다. 또한, 도 2b에서 인코딩된 이미지 프레임들의 시퀀스 중 하나의 인코딩된 이미지 프레임으로부터 LC 인코딩된 이미지 프레임들의 시퀀스 중 하나의 LC 인코딩된 이미지 프레임까지의 화살표에 의해, 인코딩된 이미지 프레임의 무손실 압축은 각각의 LC 인코딩된 이미지 프레임을 초래한다. 예를 들어, 인코딩된 이미지 프레임(I₀)의 무손실 압축은 LC 인코딩된 이미지 프레임(I_{0LC})이 되고, 인코딩된 이미지 프레임(P₀₀)의 무손실 압축은 LC 인코딩된 이미지 프레임(P_{00LC})가 되며, 인코딩된 이미지 프레임(P₀₁)의 무손실 압축은 LC 인코딩된 이미지 프레임이 된다. 따라서, 도 2b에 도시된 바와 같이, 각각의 인코딩된 이미지 프레임은 각각의 무손실 LC 인코딩된 이미지 프레임을 갖는다.
- [0052] 무손실 압축은 단지 몇 가지 예를 들자면, 허프만 코딩(Huffman coding), 산술 인코딩(arithmetic encoding), 코드북-기반 인코딩(codebook-based encoding) 및 실행-길이 인코딩(run-length encoding) 중 하나 이상을 기반으로 수행될 수 있다. 단계 S502는 송신기(110)에 포함되고 인코딩된 이미지 프레임의 무손실 압축을 수행하도록 구성된 무손실 압축 모듈(116)에 의해 수행될 수 있다.
- [0053] 상술한 바와 같이, 무손실 압축의 목적은 각각의 인코딩된 이미지 프레임(220)의 데이터 크기와 같거나 그 보다 작은 데이터 크기를 갖는 각각의 LC 인코딩된 이미지 프레임(220LC)을 획득하는 것이다. 그러나, 무손실 압축은 각각의 LC 인코딩된 이미지 프레임(220LC)이 그 각각의 인코딩된 이미지 프레임(220)의 데이터 크기와 비교하여 동일하거나 감소된 데이터 크기를 갖는 결과를 항상 초래하는 것은 아니다. 따라서, 무손실 압축 모듈(116)은 각각의 LC 인코딩된 이미지 프레임(220LC)의 크기와 각각의 인코딩된 이미지 프레임(220)의 크기를 비교하고, 각각의 LC 인코딩된 이미지 프레임(220LC)의 크기가 더 큰 경우, 무손실 압축 모듈(116)은 각각의 인코딩된 이미지 프레임(220)을 LC 인코딩된 이미지 프레임으로 출력할 것이다. LC 인코딩된 이미지 프레임의 크기를 줄이는 대안적인 방법은 LC 인코딩된 이미지 프레임을 생성하여, 이미지 정보가 부족하지만 저장된 미리 정의된 인코딩된 이미지 프레임(220e)과 같은 다른 인코딩된 이미지 프레임에 대한 참조를 포함하고, 아마도 다른 인코딩된 이미지 프레임에 대한 차이를 포함한다. 이는 송신기(110)가 무손실 압축이 수행된 인코딩된 이미지 프레임을 스킵 프레임으로 판단한 경우일 수 있다.
- [0054] "스킵 프레임(skip frame)"이란 잔여 값 없이 다른 프레임에서 이미지 데이터만을 참조함으로써(예를 들어 참조만 포함시킴으로써) 이미지 데이터를 나타내는 인터 프레임 유형을 의미한다. 스킵 프레임을 디코딩할 때 디코더는 참조된 이미지 데이터를 아무런 조정 없이(잔차 값이 부족하므로) 스킵 프레임으로 표현된 이미지 데이터의 표현으로 사용한다.
- [0055] 단계 S504에서, 송신기(110)는 획득된 LC 인코딩된 이미지 프레임(220LC) 중에서 미리 정의된 바이트 수보다 작은 데이터 크기를 각각 갖는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)을 식별한다. 미리 정의된 바이트 수는 사용된 해시 함수에 따라 설정될 수 있다. 예를 들어 미리 정의된 바이트 수는 SHA-2 해시의 경우 64바이트(512비트), 48바이트(384비트) 또는 32바이트(256비트)일 수 있고, SHA-1 해시의 경우 20바이트(160비트)일 수 있다. 송신기(110)에 포함되고 하나 이상의 작은 LC 인코딩된 이미지 프레임을 식별하도록 구성되는 식별 모듈(117)은 단계 S504를 수행할 수 있다. 식별 모듈(117)은 무손실 압축 모듈(116)에 포함될 수 있다. 대안적으로, 식별 모듈(117)은 송신기(110)의 데이터 구조 생성 모듈(118)에 포함될 수 있다. 데이터 구조 생성 모듈(118)에 대해서는 후술한다.
- [0056] 하나 이상의 식별된 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)은 작은 LC 인코딩된 이미지 프레임(220LCb-1)의 제1 유형일 수 있으며, 여기서 각각은 미리 정의된 바이트 수보다 작은 데이터 크기를 가지며 무손실 압축이 수행된 (원래의) 인코딩된 이미지 프레임(220)과 동일하거나, 또는 LC 인코딩된 이미지 프레임(220LC)이 (원래의) 인코딩된 이미지 프레임(220LC)보다 작고, 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 경우, (원래의) 인코딩된 이미지 프레임(220)의 LC 인코딩된 이미지 프레임(220LC)과 동일하다.
- [0057] 전자는 예를 들어 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 인코딩된 이미지 프레임(220)의 무손실 압축으로 인해 동일한 인코딩된 이미지 프레임(220)이 생성되거나, 인코딩된 이미지의 무손실 압축으로 인해 LC

인코딩된 이미지 프레임(220LC)이 인코딩된 이미지 프레임(220LC)보다 큰 경우일 수 있다. 상술한 바와 같이, 이 경우에, 무손실 압축을 수행하는 무손실 압축 모듈(116)은 원래의 인코딩된 이미지 프레임(220)을 LC 인코딩된 이미지 프레임(220LCb-1)으로서 출력한다.

- [0058] 따라서, 일부 실시예에서, 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 중 적어도 하나는 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1)이고 그 각각의 인코딩된 이미지 프레임(220)과 동일하거나, 인코딩된 이미지 프레임(220)의 LC 인코딩된 이미지 프레임(220LC)과 동일하다.
- [0059] 대안적으로 또는 추가적으로, 하나 이상의 식별된 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)은 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)일 수 있으며, 여기서 각각은 저장된 인코딩된 이미지 프레임(220e)의 일부와 동일하고, 저장된 인코딩된 이미지 프레임(220e)의 식별자 및 가능하게는 차이도 포함한다.
- [0060] 이는 무손실 압축이 수행된 인코딩된 이미지 프레임(220)이 저장된 인코딩된 이미지 프레임(220e)과 동일하거나, 저장된 인코딩된 이미지 프레임(220e)과 부분적으로 동일한 경우일 수 있다. 인코딩된 이미지 프레임이 스킵 프레임인 경우, 저장된 인코딩된 이미지 프레임(220e)과 인코딩된 이미지 프레임(220) 사이에는 차이가 없으며, 결과적으로 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)은 단지 저장된 인코딩된 이미지 프레임(220e)의 식별자만을 포함할 뿐 차이는 없다.
- [0061] 그러나, 인코딩된 이미지(220) 프레임은 저장된 인코딩된 이미지 프레임(220e)과 부분적으로 동일할 수 있으며, 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)은 저장된 인코딩된 이미지 프레임(220e)의 식별자 및 그 차이를 포함할 수 있다. 차이는 특정 시점에서 업데이트되거나 변경되는 일정한 이미지 프레임의 일부와 관련될 수 있다. 예를 들어, 차이는 인코딩된 이미지 프레임(220)에 포함된 카운터 또는 클럭과 관련될 수 있고, 그 차이는 인코딩된 이미지 프레임(220)을 저장된 인코딩된 이미지 프레임(220e)과 다르게 만드는 유일한 것이다. 이러한 경우, 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)에 포함된 차이는 클럭의 카운터 값 또는 시간과 관련된다.
- [0062] 따라서, 일부 실시예에서, 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 중 적어도 하나는 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)이고, 저장된 미리 정의된 인코딩된 이미지의 식별자 및 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)과 저장된 미리 정의된 인코딩된 이미지 프레임(220e) 사이의 가능한 차이를 포함한다.
- [0063] 비디오 시퀀스의 검증을 활성화하려면, 데이터 구조(320)가 필요하다. 따라서, 단계 S506에서, 송신기(110)는 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 및 개별 해시를 포함하는 데이터 구조(320)를 생성한다. 데이터 구조(320)에 포함된 개별 해시는 두 가지 방식으로 생성될 수 있다. 첫째로, 개별 해시는 도 2b의 제1 데이터 구조(320-1)에 도시된 바와 같이, 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결여된 모든 인코딩된 이미지 프레임(220)의 개별 해시일 수 있다. 둘째로, 개별 해시는 도 2b의 대안적인 제2 데이터 구조(320-2)에 도시된 바와 같이, 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시일 수 있다. 따라서, 개별 해시는 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결여된 모든 인코딩된 이미지 프레임(220), 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시이다. 송신기(110)는 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결여된 모든 인코딩된 이미지 프레임(220) 각각을 개별적으로 해싱하거나, 또는 다른 모든 획득된 LC 인코딩된 이미지 프레임(220LCa)의 각각을 개별적으로 해싱함으로써, 각각의 해시를 획득한다. 이하에서 설명되는 바와 같이, 데이터 구조는 비디오 시퀀스를 검증할 때 수신기(130)에 의해 사용된다. 송신기(110)는 데이터 구조를 생성하도록 구성된 데이터 구조 생성 모듈(118)을 포함하고, 데이터 구조 생성 모듈(118)은 단계 S506을 수행할 수 있다.
- [0064] 도 2b에 도시된 예에서, LC 인코딩된 이미지 프레임(P0_{LC}, P0_{LC}, I1_{LC}, P1_{LC} 및 I2_{LC})은 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)인 것으로 식별되며, 따라서 도시된 제1 데이터 구조(320) -1 및 대안적인 제2 데이터 구조(320-2)는 모두 이들 작은 LC 인코딩된 이미지 프레임(P0_{LC}, P0_{LC}, I1_{LC}, P1_{LC} 및 I2_{LC})를 포함한다.
- [0065] 작은 LC 인코딩된 이미지 프레임에 더하여, 제1 데이터 구조(320-1)는 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결여된 모든 인코딩된 이미지 프레임(220)의 개별 해시를 포함한다. 따라서, 도시된 예

에서 (제1) 데이터 구조는 개별 해시(H_{I0} , H_{P00} , H_{P10} 및 H_{P13})도 포함한다.

- [0066] 대안적인 제2 데이터 구조(320-2)는 작은 LC 인코딩된 이미지 프레임에 더하여, 식별된 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시를 포함한다. 따라서, 대안적인 (제2) 데이터 구조는 또한 LC 인코딩된 이미지 프레임(I_{0LC} , P_{00LC} , P_{10LC} 및 P_{13LC})의 개별 해시인 개별 해시(H_{I0LC} , H_{P00LC} , H_{P10LC} 및 H_{P13LC})를 포함한다.
- [0067] 데이터 구조(320)는 감소된 해시 리스트를 포함하는 문서라고 할 수 있다. 해시 리스트는 완전한 해시 리스트처럼 모든 인코딩된 이미지 프레임에 대한 해시를 포함할 뿐만 아니라, 감소된 해시 리스트는 작은 LC 인코딩된 이미지 프레임의 해시 대신, 작은 LC 인코딩된 이미지 프레임을 있는 그대로 즉, 해시되지 않은 상태로 포함하고 있기 때문에 감소된다. 이는 데이터 구조가 비디오 시퀀스의 각 인코딩된 이미지 프레임에 대한 개별 해시로 구성된 완전한 해시 리스트를 포함하는 문서인 경우와 대조된다. 구체적으로, 본 데이터 구조(320)는 작은 것으로 식별되는 각각의 LC 인코딩된 이미지 프레임에 대한 LC 인코딩된 이미지 프레임과, 각각의 작은 LC 인코딩된 이미지 프레임이 결여된 모든 인코딩된 이미지 프레임(220) 또는 미리 정의된 바이트 수보다 크거나 같은 크기를 갖는 모든 LC 인코딩된 이미지 프레임의 개별 해시를 포함한다. 따라서, 감소된 해시 리스트는 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2); 및 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2), 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임(220LCa)이 결여된 모든 인코딩된 이미지 프레임(220)의 개별 해시로만 구성된다.
- [0068] 실시예에서, 비디오 시퀀스가 GOP로 구성되는 경우, 송신기(110)는 하나 이상의 GOP(210a, 210b)마다 하나의 데이터 구조(320) 및 하나의 디지털 서명(340)을 생성한다. 이에 따라, 전송된 비디오 시퀀스는 전체 비디오 시퀀스가 아닌 GOP별로 수신기(130)에 의해 검증될 수 있다. 이는 하나 이상의 인코딩된 이미지 프레임 또는 GOP가 검증될 수 없는 경우, 수신기가 검증된 GOP 및 검증된 GOP의 인코딩된 이미지 프레임의 진위성을 여전히 신뢰할 수 있기 때문에 수신기(130)에 유리하다. 이는 비디오 시퀀스가 전체적으로 검증되어야 하는 경우와 대조되며, 전체 비디오 시퀀스가 검증될 수 없는 경우, 수신기는 비디오 시퀀스의 인코딩된 이미지 프레임 중 임의의 것의 진위를 신뢰할 수 없다.
- [0069] 때로는 작은 LC 인코딩된 이미지 프레임 각각이 데이터 구조의 어디에 위치하는지에 대한 정보를 제공하는 것이 유리할 수 있다. 이는 예를 들어, 수신기(130)가 수신된 데이터 구조로부터 작은 LC 인코딩된 이미지 프레임을 찾아 추출하는 것을 단순화할 수 있다. 수신기(130)에 의해 수행되는 방법을 설명할 때 이하에서 설명되는 바와 같이, 수신기(130)는 수신된 인코딩된 이미지 프레임을 검증할 때, 추출된 작은 LC 인코딩된 이미지 프레임을 이용하여, 대응하는 전송된 인코딩된 이미지 프레임 및 그 해시를 생성, 즉 재구성할 수 있다.
- [0070] 따라서, 일부 실시예는 단계 S508을 포함하며, 여기서 송신기(110)는 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)에 대해, 데이터 구조에서 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)의 위치를 결정한다. 단계 S508에서, 송신기(110)는 또한 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)의 데이터 크기를 결정할 수 있다. 단계 S508은 송신기(110)에 포함되고, 데이터 구조에서 각각의 작은 LC 인코딩된 이미지 프레임의 위치를 결정하도록 구성되는 결정 모듈(119)에 의해 수행될 수 있다. 결정 모듈(119)은 무손실 압축 모듈(116)에 포함될 수 있다. 대안적으로, 결정 모듈(119)은 송신기(110)의 데이터 구조 생성 모듈(118)에 포함될 수 있다. 실시예는 또한 송신기(110)가 데이터 구조를 제공하는 단계 S510을 포함할 수 있는데, 송신기(110)는 데이터 구조(320)에서의 위치 및 각각 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)의 선택적인 데이터 크기를 지정하는 정보를 갖는 데이터 구조(320)를 제공한다. 데이터 구조(320)에 위치 특정 정보를 제공하는 것은 데이터 구조 생성 모듈(118)에 의해 수행될 수 있다.
- [0071] 비디오 시퀀스의 유효성을 검사하려면, 디지털 서명도 필요하다. 따라서, 단계 S512에서, 송신기(110)는 비디오 시퀀스(200)에 대한 디지털 서명(340)을 생성한다. 이 단계는 디지털 서명을 생성하도록 구성되고, 송신기(110)에 포함되는 디지털 서명 생성 모듈(124)에 의해 수행될 수 있다.
- [0072] 송신기(110)는 개인-공개 키 쌍에 액세스할 수 있고, 개인-공개 키 쌍의 개인 키를 이용하여 다음 중 하나를 암호화함으로써 디지털 서명을 생성할 수 있다:
- [0073] 데이터 구조(320)의 해시; 또는
- [0074] 다음 중 하나의 개별 해시의 해시: 비디오 시퀀스(200)의 모든 인코딩된 이미지 프레임(220), 또는 획득된 모든

LC 인코딩된 이미지 프레임(220LC; 220LCa, 220LCb-1, 220LCb-2).

- [0075] 개인-공개 키 쌍 중 개인 키는 송신기(110)에 의해서만 액세스 가능한 보안 저장부에 저장될 수 있다. 보안 저장부는 보안 요소(SE), 예를 들어 변조 방지 프로세서 칩이나 보안 구성 요소의 보안 운영 체제(OS), 또는 신뢰할 수 있는 플랫폼 모듈(TPM), 예를 들어, 보안 암호화 프로세서 또는 보안 칩일 수 있다. 송신기의 개인-공개 키 쌍 중 공개 키는 수신기(130)에 의해 액세스 가능한 데이터 저장부, 예를 들어 데이터 저장부(122)에 저장될 수 있다. 대안적으로, 송신기의 개인-공개 키 쌍의 공개 키는 비디오 시퀀스(200)와 함께 수신기(130)로 전송될 수 있다. 예를 들어, 송신기의 개인-공개 키 쌍의 공개 키는 비디오 시퀀스(200)에 포함되거나 첨부될 수 있다.
- [0076] 단계 S514에서, 송신기(110)는 데이터 구조(320) 및 디지털 서명(340)을 비디오 시퀀스(200)에 제공한다. 이로써 수신기(130)가 비디오 시퀀스(200)를 검증할 수 있게 된다. 송신기(110)에 포함되고 데이터 구조 및 디지털 서명을 비디오 시퀀스에 제공하도록 구성된 제공 모듈(126)은 단계 S514를 수행할 수 있다.
- [0077] 송신기(110)는 예를 들어, 제공 모듈(126)을 통해 비디오 시퀀스(200)의 보충 정보 유닛(SIU)에 데이터 구조(320) 및 디지털 서명(340)을 제공할 수 있다. 보충 정보 유닛은 비디오 시퀀스에 관한 또는 그와 관련된 추가 정보를 포함하도록 구성되는 유닛 또는 메시지이다. 보충 정보 유닛은 예를 들어, H.26x 인코딩 포맷의 SEI(Supplemental Enhancement Information) 메시지가거나 AV1 인코딩 포맷의 OBU(Metadata Open Bitstream Unit)일 수 있다.
- [0078] 수신기(130)는 이하에서 상세히 설명되는 바와 같이, 수신된 디지털 서명 및 수신된 데이터 구조를 이용하여 수신된 비디오 시퀀스를 검증할 수 있다.
- [0080] 데이터 구조(320) 및 디지털 서명(340)이 제공되는 비디오 시퀀스(200')를 검증하기 위해 수신기(130)에 의해 수행되는 방법은 이제 도 6의 흐름도 및 도 4에 개략적으로 도시된 수신기(130)의 실시예를 참조하여 설명될 것이다. 비디오 시퀀스(200')는 인코딩된 이미지 프레임(220')을 포함한다.
- [0081] 단계 S602에서 수신기(130)는 송신기(110)로부터, 인코딩된 이미지 프레임(220')을 포함하고 데이터 구조(320) 및 디지털 서명(340)이 제공되는 비디오 시퀀스(200')를 수신한다. 바람직하게는, 수신기(130)에 의해 수신된 비디오 시퀀스(200')와 송신기(110)에 의해 전송된 비디오 시퀀스(200)는 동일하다. 다만, 전송되는 비디오 시퀀스는 전송 후, 수신되기 전에 조작될 수 있으므로, 전송되는 비디오 시퀀스에는 참조번호 200을, 수신되는 비디오 시퀀스에는 참조번호 200'을 사용한다. 단계 S602는 수신기(130)에 포함되고 비디오 시퀀스를 수신하도록 구성된 수신 모듈(132)에 의해 수행될 수 있다.
- [0082] 수신된 데이터 구조(320)는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)을 포함하며, 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)은 미리 정의된 바이트 수보다 작은 데이터 크기를 가지며, 송신기(110)로부터 전송된 비디오 시퀀스(200)에 포함된 각각의 전송된 인코딩된 이미지 프레임(220)의 LC 버전이다. 수신된 데이터 구조(320)는 또한 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결합된 모든 전송된 인코딩된 이미지 프레임(220), 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시를 포함한다. 다른 모든 LC 인코딩된 이미지 프레임(220LCa) 각각은 전송된 비디오 시퀀스(200)에 포함된 각각의 전송된 인코딩된 이미지 프레임(220)의 LC 버전이다.
- [0083] 앞서 언급한 바와 같이, 송신기(110)에 의해 수행되는 방법을 설명할 때, 미리 정의된 바이트 수는 사용되는 해시 함수에 따라 설정될 수 있다. 송신기(110)와 수신기(130)는 동일한 해시 함수를 사용하므로, 송신기(110)에 설정된 미리 정의된 바이트 수는 수신기(130)에서 사용되는 미리 정의된 바이트 수와 동일한 것으로 이해된다. 미리 정의된 바이트 수는 수신기(130)에 미리 설정될 수 있거나, 송신기(110)에 의해 사용되는 미리 정의된 바이트 수에 대한 정보는, 예를 들어 비디오 시퀀스와 함께, 송신기(110)에서 수신기(130)로 전송될 수 있다.
- [0084] 단계 S604에서 수신기(130)는 수신된 데이터 구조(320)를 이용하여 수신된 디지털 서명(340)을 검증한다. 단계 S604는 수신기(130)에 포함되고 디지털 서명을 검증하도록 구성된 검증 모듈(134)에 의해 수행될 수 있다.
- [0085] 일부 실시예에서 수신기(130)는 송신기(110)의 개인-공개 키 쌍의 공개 키에 액세스할 수 있다. 이러한 실시예에서, 수신기(130)는 공개 키를 이용하여 수신된 디지털 서명(340)을 복호화하고, 수신된 데이터 구조(320)의 해시가 복호화된 수신된 디지털 서명(340)과 일치할 때 수신된 디지털 서명(340)을 검증함으로써, 수신된 디지털 서명(340)을 검증한다. 대안적으로, 수신된 데이터 구조(340)에 의해 주어진 바와 같이, 모든 LC 인코딩된 이미지 프레임에 대한 모든 개별 해시의 해시가 복호화된 수신된 디지털 서명(340)과 일치할 때, 수신된 디지털 서명(340)이 검증된다. 또 다른 대안으로, 수신된 디지털 서명(340)은 수신된 데이터 구조(340)에 의해 주어진

바와 같이 모든 인코딩된 이미지 프레임에 대한 모든 개별 해시의 해시가 복호화된 것으로서 수신된 디지털 서명(340)과 일치할 때 검증된다.

- [0086] 단계 S606에서 수신기(130)는 수신된 데이터 구조(320)를 이용하여, 수신된 인코딩된 이미지 프레임(220')이 전송된 인코딩된 이미지 프레임(220)과 동일한 것으로 을 검증한다. 단계 S606은 수신기(130)에 포함되고 인코딩된 이미지 프레임을 검증하도록 구성되는 검증 모듈(134)에 의해 수행될 수 있다. 수신된 비디오 시퀀스(200')는 수신된 디지털 서명(340) 및 수신된 인코딩된 이미지 프레임(220')이 검증될 때, 전송된 비디오 시퀀스(200)와 동일한 것으로 검증된다.
- [0088] **수신된 인코딩된 이미지 프레임(220')의 검증(단계 S606)**
- [0089] 수신된 인코딩된 이미지 프레임(220')의 검증(단계 S606)은 이제 몇 가지 다른 실시예를 참조하여 더 자세히 설명될 것이다. 세부적으로 들어가기 전에, 일반적으로 검증은 수신된 데이터 구조에 의해 주어질 바와 같이(아래의 일부 제1 실시예에서와 같이), 수신된 인코딩된 이미지 프레임의 해시를 인코딩된 이미지 프레임의 해시와 비교함으로써, 수신된 데이터 구조에 의해 주어질 바와 같이(아래의 일부 제2 실시예에서와 같이), LC 수신된 인코딩된 이미지 프레임을 LC 인코딩된 이미지 프레임과 비교함으로써 또는 수신된 데이터 구조를 생성된 데이터 구조(아래의 일부 제3 실시예에서와 같이)와 비교함으로써 이루어진다고 말할 수 있다.
- [0090] 또한, 송신기(110)에 의해 전송되고 수신기(130)에 의해 수신되는 데이터 구조(320)는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)에 추가하여, 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)(아래의 일부 제1 실시예에서와 같이)이 결합된 모든 전송된 인코딩된 이미지 프레임(220), 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 LC 인코딩된 이미지 프레임(220LCa) 220LCb-1, 220LCb-2(아래의 일부 제2 및 제3 실시예에서와 같음) 중 하나의 개별 해시를 포함한다는 것을 기억해야 한다.
- [0092] 일부 제1 실시예
- [0093] 일부 제1 실시예에서, 수신된 데이터 구조(320)는 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)에 추가하여, 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 결합된 모든 전송된 인코딩된 이미지 프레임(220)의 개별 해시를 포함한다. 이러한 제1 실시예에서, 수신기(130)는 수신된 인코딩된 이미지 프레임의 해시를 생성해야 하고, 수신된 데이터 구조(320)에 포함된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)의 각각의 인코딩된 이미지 프레임의 개별 해시(들)를 결정해야 한다. 따라서, 수신된 데이터 구조(320)를 이용하여 수신된 인코딩된 이미지 프레임(220')이 전송된 인코딩된 이미지 프레임(220)과 동일한지 확인하는 단계(단계 S606)는 도 7a에 도시된 4개의 하위 단계(S606.1.1-S606.1.4)를 포함한다.
- [0094] 하위 단계 S606.1.1에서, 수신기(130)는 수신된 비디오 시퀀스(200')에 포함된 각각의 수신된 인코딩된 이미지 프레임(220')의 개별 해시를 생성한다. 수신기(130)에 포함된 해시 생성 모듈(136)은 개별 해시의 생성을 수행할 수 있다.
- [0095] 하위 단계 S606.1.2에서, 수신기(130)는 수신된 데이터 구조(320)에 포함된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 각각의 무손실 압축 해제를 수행하여, 각각의 인코딩된 이미지 프레임을 획득한다. LC 인코딩된 이미지 프레임(220LC)에 대해 무손실 압축 해제를 수행함으로써, 송신기(110)가 LC 인코딩된 이미지 프레임을 획득하기 위해 무손실 압축을 수행한 (원래의) 인코딩된 이미지 프레임(220)이 획득될 것이다. 무손실 압축 해제 알고리즘의 몇 가지 예로는 허프만 디코딩(Huffman decoding), 산술 디코딩(arithmetic decoding), 코드북-기반 디코딩(codebook-based decoding) 및 실행 길이 디코딩(run-length decoding)이 있다. 수신기(130)에 포함된 무손실 압축 해제 모듈(138)은 무손실 압축 해제를 수행할 수 있다.
- [0096] 하위 단계 S606.1.3에서, 수신기(130)는 획득된 각각의 인코딩된 이미지 프레임(220) 각각의 개별 해시를 생성한다. 이는 해시 생성 모듈(136)에 의해 수행될 수 있다.
- [0097] 하위 단계 S606.1.4에서, 수신기(130)는 수신된 비디오 시퀀스(200')에 포함된 각 수신된 인코딩된 이미지 프레임(220')의 생성된 개별 해시가 획득된 각각의 인코딩된 이미지 프레임(220)의 각각의 생성된 개별 해시와 일치할 때, 수신된 인코딩된 이미지 프레임(220')은 전송된 인코딩된 이미지 프레임(220)과 동일한 것으로 검증된다. 이는 검증 모듈(134)에 의해 수행될 수 있다.
- [0099] 일부 제2 실시예
- [0100] 일부 제2 실시예에서, 수신된 데이터 구조(320)는 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)에 추가하여, 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 LC 인코딩된 이미지

프레임(220LCa)의 개별 해시를 포함한다. 이러한 제2 실시예에서, 수신된 데이터 구조(320)를 이용하여 수신된 인코딩된 이미지 프레임(220')이 전송된 인코딩된 이미지 프레임(220)과 동일한지를 검증하는 것(단계 S606)은 도 7b에 도시된 4개의 하위 단계(S606.2.1 - S606.2.4)를 포함한다.

- [0101] 하위 단계 S606.2.1에서, 수신기(130)는 수신된 비디오 시퀀스(200')에 포함된 각각의 수신된 인코딩된 이미지 프레임(220')의 무손실 압축을 수행하여, 각각의 LC 수신된 인코딩된 이미지 프레임(220LC'; 220LCa', 220LCb-1', 220LCb-2')을 획득한다. 무손실 압축 알고리즘의 예로는 허프만 코딩, 산술 인코딩, 코드북 기반 인코딩 및 실행 길이 인코딩이 있다. 수신기(130)에 포함된 무손실 압축 모듈(140)은 무손실 압축을 수행할 수 있다.
- [0102] 하위 단계 S606.2.2에서, 수신기(130)는 획득된 모든 각각의 LC 수신된 인코딩된 이미지 프레임(220LC'; 220LCa', 220LCb-1', 220LCb-2')의 개별 해시를 생성한다. 이는 해시 생성 모듈(136)에 의해 수행될 수 있다.
- [0103] 하위 단계 S606.2.3에서, 수신기(130)는 수신된 데이터 구조(320)에 의해 주어진 바와 같이, 모든 LC 인코딩된 이미지 프레임(220LC; 220LCa, 220LCb-1, 220LCb-2)에 대한 개별 해시를 생성한다. 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시가 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 다르기 때문에, 수신된 데이터 구조(320)에 포함되어 있는 경우, 수신기(130)는 데이터 구조(320)로부터 이를 직접 검색할 수 있다. 또한, 수신기(130)는 수신된 데이터 구조(320)에 포함된 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)을 검색한 후 개별적으로 해시한다. 수신기(130)는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)이 제1 유형인지, 제2 유형인지 여부에 따라 개별 해시를 다르게 생성할 것이다. 하위 단계 S606.2.3은 해시 생성 모듈에 의해 수행될 수 있다. 개별 해시 생성에 대한 상세한 설명은 하위 단계 S606.2.4의 설명 이후에 제공된다.
- [0104] 하위 단계 S606.2.4에서, 수신기(130)는 수신된 데이터 구조(320)로서 주어진 모든 LC 인코딩된 이미지 프레임(220LC; 220LCa, 220LCb-1, 220LCb-2)이 획득된 모든 각각의 LC 수신된 인코딩된 이미지 프레임(220LC'; 220LCa', 220LCb-1', 220LCb-2')의 생성된 개별 해시와 일치할 때, 수신된 인코딩된 이미지 프레임(220')은 전송된 인코딩된 이미지 프레임(220)과 동일한 것으로 검증한다. 이는 검증 모듈(134)에 의해 수행될 수 있다.
- [0106] 모든 LC 인코딩된 이미지 프레임에 대한 개별 해시 생성(하위 단계 S606.2.3)
- [0107] 수신기(130)가 수신된 데이터 구조(320)에 의해 주어진 모든 LC 인코딩된 이미지 프레임(220LC; 220LCa, 220LCb-1, 220LCb-2)에 대한 개별 해시를 생성하는 방법(위의 하위 단계 S606.2.3)은 이제 두 가지 시나리오를 참조하여 더 자세히 설명될 것이다.
- [0108] 제1 시나리오에서, LC 인코딩된 이미지 프레임(220LC)이 인코딩된 이미지 프레임(220)보다 작고, 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 경우, 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1)은 제1 유형이고, 미리 정의된 바이트 수보다 작거나 인코딩된 이미지 프레임(220)의 LC 인코딩된 이미지 프레임(220LC)과 같은 데이터 크기를 갖는 인코딩된 이미지 프레임(220)과 동일하다. 인코딩된 이미지 프레임(220)은 송신기(110)에 의해 전송된 원래의 인코딩된 이미지 프레임이다. 작은 LC 인코딩된 이미지 프레임(220LCb-1)은 원래의 인코딩된 이미지 프레임에 대해 무손실 압축을 수행할 때 송신기의 무손실 압축 모듈(116)에 의해 획득된 LC 인코딩된 이미지 프레임이 원래의 인코딩된 이미지 프레임보다 큰 크기를 갖고, 무손실 압축 모듈(116)이 획득된 LC 인코딩된 이미지 프레임으로서 원래의 인코딩된 이미지 프레임을 출력할 때, 인코딩된 이미지 프레임(220)과 동일하다. 따라서, 제1 시나리오에서, 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 중 하나 이상은 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1)이고, 각각의 전송된 인코딩된 이미지 프레임(220)과 동일하거나, 또는 인코딩된 이미지 프레임(220)의 LC 인코딩된 이미지 프레임(220LC)과 동일하다. 수신된 데이터 구조(320)는 데이터 구조(320)에서, 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1) 위치 및 선택적 크기를 지정하는 정보를 더 포함한다. 이 제1 시나리오에서, 수신된 데이터 구조(320)에 의해 주어진 모든 LC 인코딩된 이미지 프레임(220LCa, 220LCb-1, 220LCb-2)에 대한 개별 해시를 생성하는 단계는:
 - [0109] - 수신된 데이터 구조(320)로부터, 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1) 및 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시를 추출하는 단계;
 - [0110] - 추출된 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1)을 개별적으로 해싱하여 개별 해시를 생성하는 단계; 및
 - [0111] - 추출된 제1 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-1)의 생성된 개별 해시와 추출된 다른 모든 인코딩된 이미지 프레임(220LCa)의 개별 해시를 결합하여 모든 LC 인코딩된 이미지 프레임(220LCa, 220LCb-1,

220LCb-2)에 대한 개별 해시를 생성하는 단계를 포함한다.

- [0112] 제2 시나리오에서, 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-2)은 제2 유형이다. 이는 송신기(110)가 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)의 각각의 (원래의) 인코딩된 이미지 프레임(220)이 저장된 인코딩된 이미지 프레임(220e)의 일부와 동일하다고 판단한 경우일 수 있다. 예를 들어, 송신기(110)가 예를 들어 무손실 압축 모듈(116)을 통해 각각의 인코딩된 이미지 프레임(220)이 저장된 인코딩된 이미지 프레임(220e)과 동일한 스킵 프레임이라고 결정하는 경우, 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)은 다른 이미지 데이터 없이 저장된 인코딩된 이미지 프레임(220e)의 식별자만을 포함하도록 생성될 수 있다. 다른 예로서, 송신기(110)는 예를 들어 무손실 압축 모듈(116)에 의해, 각각의 인코딩된 이미지 프레임(220)이 저장된 인코딩된 이미지 프레임(220e)과 부분적으로 동일하다고 결정할 수 있다. 그러면, 저장된 인코딩된 이미지 프레임(220e)의 식별자와 저장된 인코딩된 이미지 프레임(220e)에 대한 차이를 포함하는 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)이 생성될 수 있다. 따라서, 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2) 중 하나 이상은 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)이고, 저장된 미리 정의된 인코딩된 이미지 프레임(220e)의 식별자 및 각각의 전송된 인코딩된 이미지 프레임(220)과 저장된 미리 정의된 인코딩된 이미지 프레임(220e) 간의 가능한 차이를 포함한다. 수신된 데이터 구조(320)는 데이터 구조(320)에서, 제2 유형의 작은 LC 인코딩된 이미지 프레임(220LCb-2)의 위치 및 선택적인 데이터 크기를 지정하는 정보를 더 포함한다. 이 제2 시나리오에서, 수신된 데이터 구조(320)에 의해 주어진 모든 LC 인코딩된 이미지 프레임(220LCa, 220LCb-1, 220LCb-2)에 대한 개별 해시를 생성하는 단계는 다음을 포함한다:
- [0113] 수신된 데이터 구조(320)로부터 다음을 추출하는 단계:
- [0114] 제2 유형의 각각의 작은 LC 인코딩된 이미지 프레임(220LCb-2)에 대해, 저장된 미리 정의된 인코딩된 이미지 프레임(220e)의 식별자 및 각각의 전송된 인코딩된 이미지 프레임(220)과 저장된 인코딩된 이미지 프레임(220e) 간의 가능한 차이; 및
- [0115] 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시;
- [0116] 비디오 시퀀스(200)의 송신기(110) 및 수신기(130)에 액세스 가능한 데이터 저장부(122)로부터, 추출된 식별자를 이용하여 저장된 인코딩된 이미지 프레임(220e)을 검색하는 단계;
- [0117] 검색된 저장된 미리 정의된 인코딩된 이미지 프레임(220e)과 가능한 차이를 결합함으로써, 제2 유형의 각각의 LC 인코딩된 이미지 프레임(220LCb-2)에 대한 각각의 전송된 인코딩된 이미지 프레임(220)을 재구성하는 단계;
- [0118] 재구성된 전송된 인코딩된 이미지 프레임의 무손실 압축을 수행하는 단계;
- [0119] LC 재구성된 전송된 인코딩된 이미지 프레임을 개별적으로 해싱함으로써 개별 해시를 생성하는 단계; 및
- [0120] LC 재구성된 전송된 인코딩된 이미지 프레임(220)의 생성된 개별 해시 및 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 추출된 개별 해시를 포함하도록 추가 데이터 구조(330)를 생성하는 단계.
- [0122] 일부 제3 실시예
- [0123] 일부 제3 실시예에서, 수신된 데이터 구조(320)는 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1, 220LCb-2)과 상이한 다른 모든 LC 인코딩된 이미지 프레임(220LCa)의 개별 해시를 포함한다. 수신된 인코딩된 이미지 프레임(220')을 검증하기 위해, 수신기(130)는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 하나 이상의 작은 인코딩된 이미지 프레임과 상이한 모든 LC 인코딩된 이미지 프레임의 개별 해시를 포함하는 데이터 구조를 생성하고, 이를 수신된 데이터 구조와 비교한다. 따라서, 이러한 제3 실시예에서, 수신된 데이터 구조(320)를 이용하여 수신된 인코딩된 이미지 프레임(220')이 전송된 인코딩된 이미지 프레임(220)과 동일한지 확인하는 단계(단계 S606)는 도 7c에 도시된 3개의 하위 단계(S606.3.1 - S606.3.3)를 포함한다.
- [0124] 하위 단계 S606.3.1에서, 수신기(130)는 수신된 비디오 시퀀스(200')에 포함된 각각의 수신된 인코딩된 이미지 프레임(220')의 무손실 압축을 수행하여 각각의 LC 수신된 인코딩된 이미지 프레임(220LCa', 220LCb-1', 220LCb-2')을 획득한다. 무손실 압축 알고리즘의 예로는 허프만 코딩, 산술 인코딩, 코드북 기반 인코딩 및 실행 길이 인코딩이 있다. 수신기(130)에 포함된 무손실 압축 모듈(미도시)은 무손실 압축을 수행할 수 있다.
- [0125] 하위 단계 S606.3.2에서, 수신기(130)는 다음을 포함하는 데이터 구조(320')를 생성한다:
- [0126] 각각이 미리 정의된 바이트 수보다 작은 데이터 크기를 갖도록 식별된 하나 이상의 작은 LC 수신된 인코딩된 이미지 프레임(220bLC-1', 220LCb-2'), 및

- [0127] 하나 이상의 작은 LC 인코딩된 이미지 프레임(220LCb-1', 220LCb-2')과 상이한 다른 모든 LC 수신된 인코딩된 이미지 프레임(220LCa')의 개별 해시. 상기 개별 해시는 다른 모든 LC 수신된 인코딩된 이미지 프레임(220LCa')의 각각을 개별적으로 해싱함으로써 획득된다.
- [0128] 이는 수신기(130)에 포함된 데이터 구조 생성 모듈(142)에 의해 수행될 수 있다.
- [0129] 하위 단계 S606.3.3에서, 수신기(130)는 생성된 데이터 구조(320')가 수신된 데이터 구조(320)와 일치할 때, 수신된 인코딩된 이미지 프레임(220')이 전송된 인코딩된 이미지 프레임(220)과 동일한 것으로 검증한다. 이는 검증 모듈(134)에 의해 수행될 수 있다.
- [0131] 실시예는 또한 프로세싱 능력을 갖는 장치에 의해 실행될 때, 본 명세서에 설명된 방법의 실시예를 수행하도록 적용된 컴퓨터 코드 명령이 저장되어 있는 비일시적 컴퓨터 판독 가능 매체에 관한 것이다.
- [0133] 전술한 바와 같이, 송신기(110)는 비디오 시퀀스에 데이터 구조와 전자 서명을 제공함으로써, 비디오 시퀀스의 검증이 가능하도록 하는 방법을 구현하도록 구성될 수 있고, 수신기(130)는 비디오 시퀀스에 데이터 구조와 디지털 서명을 제공하여 비디오 시퀀스의 검증을 위한 방법을 구현하도록 구성될 수 있다. 이를 위해, 송신기(110) 및 수신기(130)는 각각 본 명세서에 설명된 다양한 방법 단계를 구현하도록 구성되는 프로세싱 회로(111, 131)를 각각 포함할 수 있다.
- [0134] 하드웨어 구현에서, 프로세싱 회로(111, 131)는 하나 이상의 방법 단계를 구현하도록 전용으로 특별히 설계될 수 있다. 회로는 하나 이상의 주문형 집적 회로 또는 하나 이상의 현장 프로그래밍 가능 게이트 어레이와 같은 하나 이상의 집적 회로 형태일 수 있다.
- [0135] 예를 들어, 송신기(110)는 다음과 같은 사용시에, 프로세싱 회로(111)를 포함할 수 있다:
- [0136] 비디오 시퀀스의 각각의 인코딩된 이미지 프레임의 무손실 압축을 수행하여 각각의 LC 인코딩된 이미지를 획득;
- [0137] 획득된 LC 인코딩된 이미지 프레임 중에서, 각각이 미리 정의된 바이트 수보다 작은 데이터 크기를 갖는 하나 이상의 작은 LC 인코딩된 이미지 프레임을 식별;
- [0138] 식별된 하나 이상의 작은 LC 인코딩된 이미지 프레임, 및 다음 중 하나의 개별 해시를 포함하는 데이터 구조를 생성: 각각의 작은 LC 인코딩된 이미지 프레임이 결합된 모든 인코딩된 이미지 프레임; 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 획득된 LC 인코딩된 이미지 프레임 - 상기 개별 해시는 각각의 작은 LC 인코딩된 이미지 프레임이 결합된 모든 인코딩된 이미지 프레임 각각을 개별적 해싱, 또는 다른 모든 획득된 LC 인코딩된 이미지 프레임 각각을 각각 해싱하여 획득됨 - ;
- [0139] 비디오 시퀀스에 대한 디지털 서명을 생성; 및
- [0140] 비디오 시퀀스에 데이터 구조와 디지털 서명을 제공. 이로써 수신기가 비디오 시퀀스를 검증할 수 있게 된다.
- [0141] 예를 들어, 수신기(130)는 다음과 같은 사용 시에, 프로세싱 회로(131)를 포함할 수 있다:
- [0142] 인코딩된 이미지를 포함하고 데이터 구조와 디지털 서명이 제공되는 비디오 시퀀스를 수신. 수신된 데이터 구조는 하나 이상의 작은 LC 인코딩된 이미지를 포함하며, 각각의 작은 LC 인코딩된 이미지는 미리 정의된 바이트 수보다 작은 데이터 크기를 가지며, 송신기로부터 전송된 비디오 시퀀스에 포함된 각각의 전송된 인코딩된 이미지 프레임의 LC 버전; 및 다음 중 하나의 개별 해시: 각각의 작은 LC 인코딩된 이미지가 결합된 전송된 모든 인코딩된 이미지 프레임; 또는 하나 이상의 작은 LC 인코딩된 이미지 프레임과 상이한 다른 모든 LC 인코딩된 이미지 프레임. 다른 모든 LC 인코딩된 이미지 프레임 각각은 전송된 비디오 시퀀스에 포함된 각각의 전송된 인코딩된 이미지 프레임의 LC 버전이다.
- [0143] 수신된 데이터 구조를 이용하여 수신된 디지털 서명을 검증; 및 수신된 데이터 구조를 이용하여 수신된 인코딩된 이미지 프레임이 전송된 인코딩된 이미지 프레임과 동일한지 검증. 이로써 수신된 비디오 시퀀스는 수신된 디지털 서명 및 수신된 인코딩된 이미지 프레임이 검증될 때 전송된 비디오 시퀀스와 동일한 것으로 검증된다.
- [0144] 소프트웨어 구현에서, 회로는 대신 마이크로프로세서와 같은 프로세서의 형태일 수 있으며, 마이크로 프로세서는 비휘발성 메모리와 같은 (비일시적) 컴퓨터 판독 가능 매체에 저장된 컴퓨터 코드 명령어들과 관련하여, 송신기(110) 및 수신기(130)가 각각 본 명세서에 개시된 각각의 방법을 수행하게 한다. 비휘발성 메모리의 예로는 읽기 전용 메모리, 플래시 메모리, 강유전성 RAM, 자기 컴퓨터 저장 장치, 광 디스크 등이 있다. 소프트웨어의

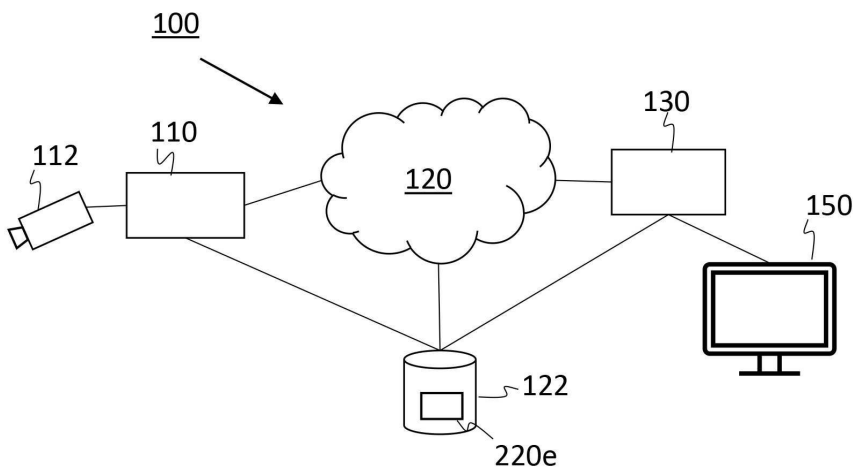
경우, 위에 설명된 방법 단계들 각각은 프로세서에 의해 실행될 때, 송신기(110)와 수신기(130)가 각각 본 명세서에서 개시된 각각의 방법을 수행하게 하는 컴퓨터 판독 가능 매체에 저장된 컴퓨터 코드 명령어의 일부에 대응할 수 있다.

[0145] 하드웨어와 소프트웨어 구현을 결합하는 것도 가능하다는 점을 이해해야 하며, 이는 일부 방법 단계가 하드웨어에서 구현되고 다른 단계가 소프트웨어에서 구현된다는 의미이다.

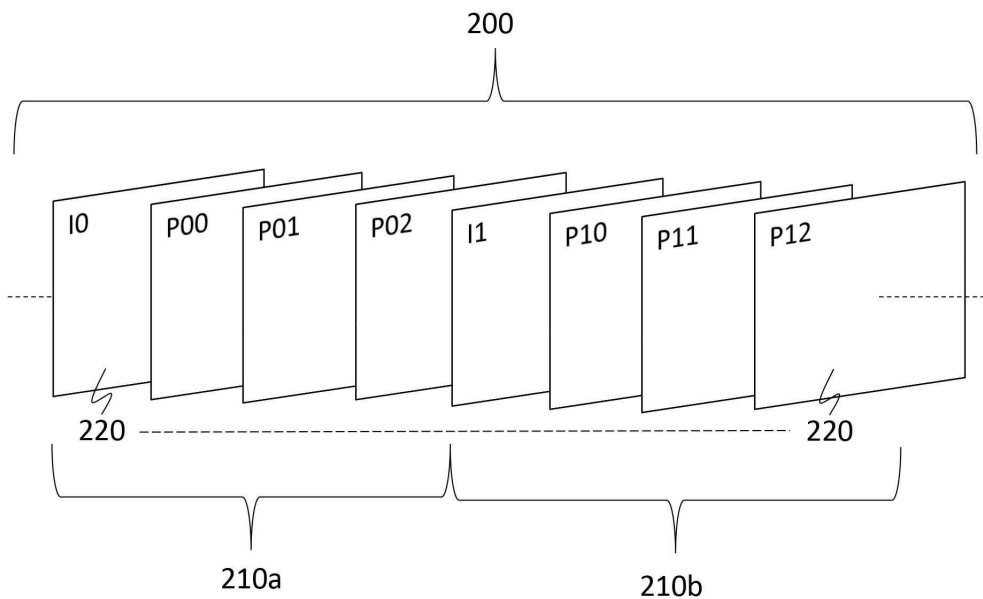
[0146] 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예들을 다양한 방식으로 수정할 수 있고, 상술한 실시예에 도시된 바와 같은 본 발명의 장점을 계속 사용할 수 있다는 것을 이해할 수 있을 것이다. 따라서, 본 발명은 도시된 실시예에 제한되어서는 안되며 첨부된 청구범위에 의해서만 정의되어야 한다. 또한, 통상의 지식을 가진 자가 이해하는 바와 같이, 도시된 실시예는 결합될 수 있다.

도면

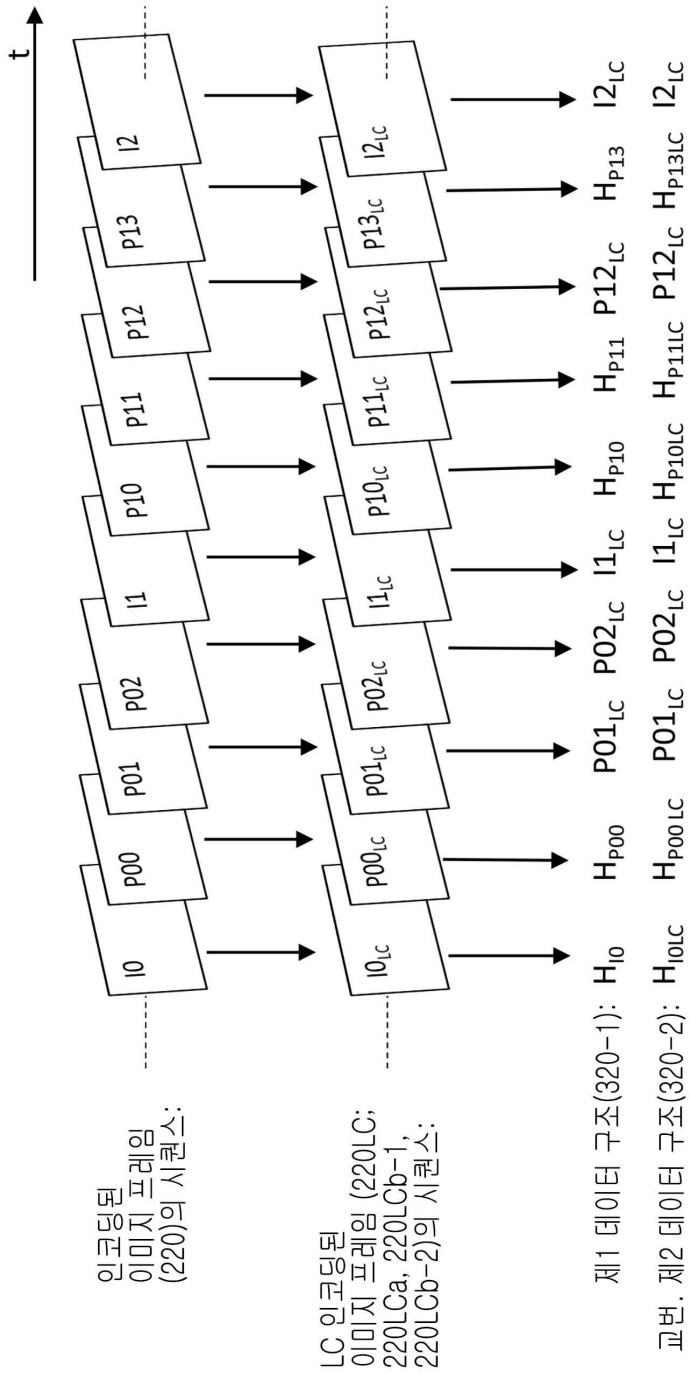
도면1



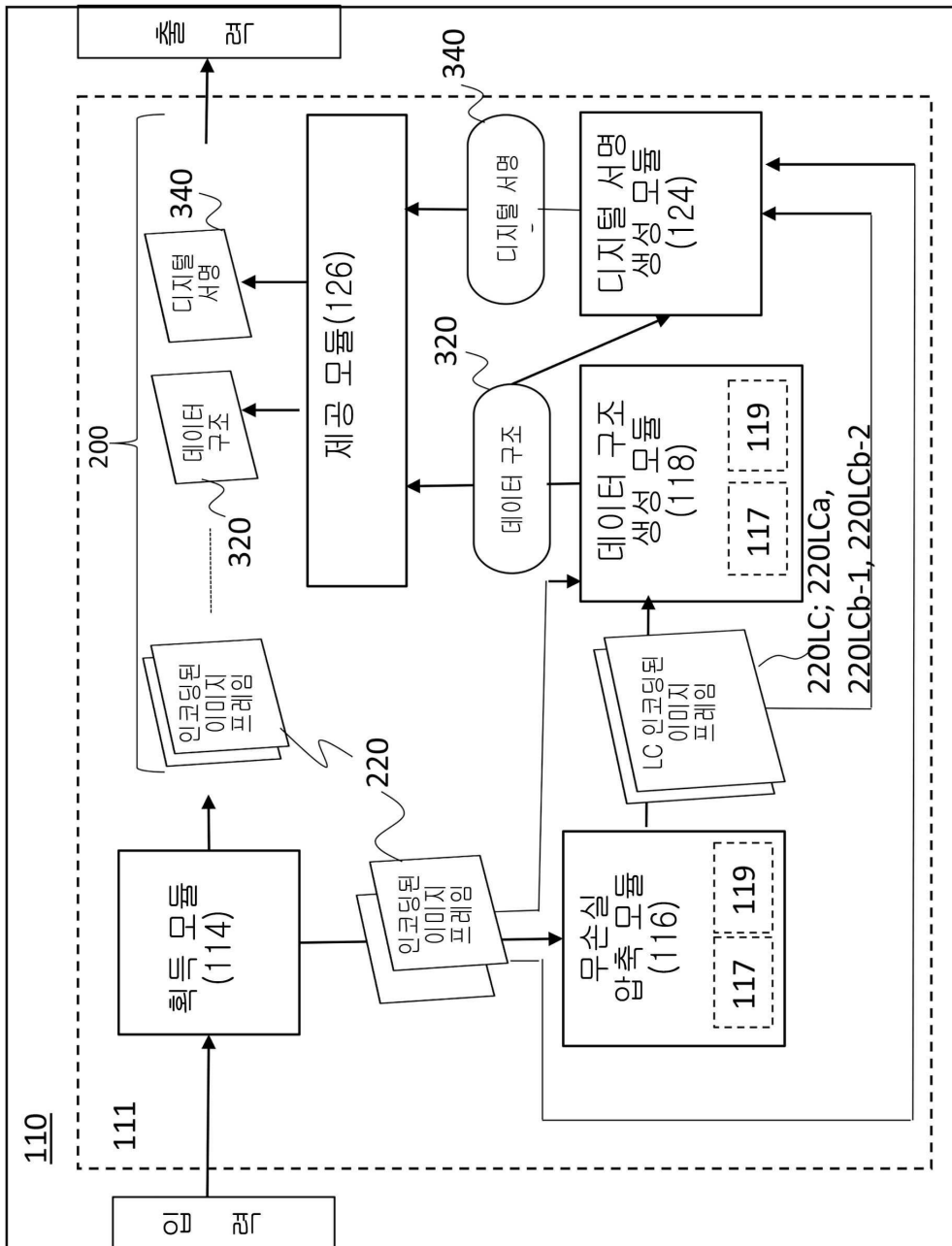
도면2a



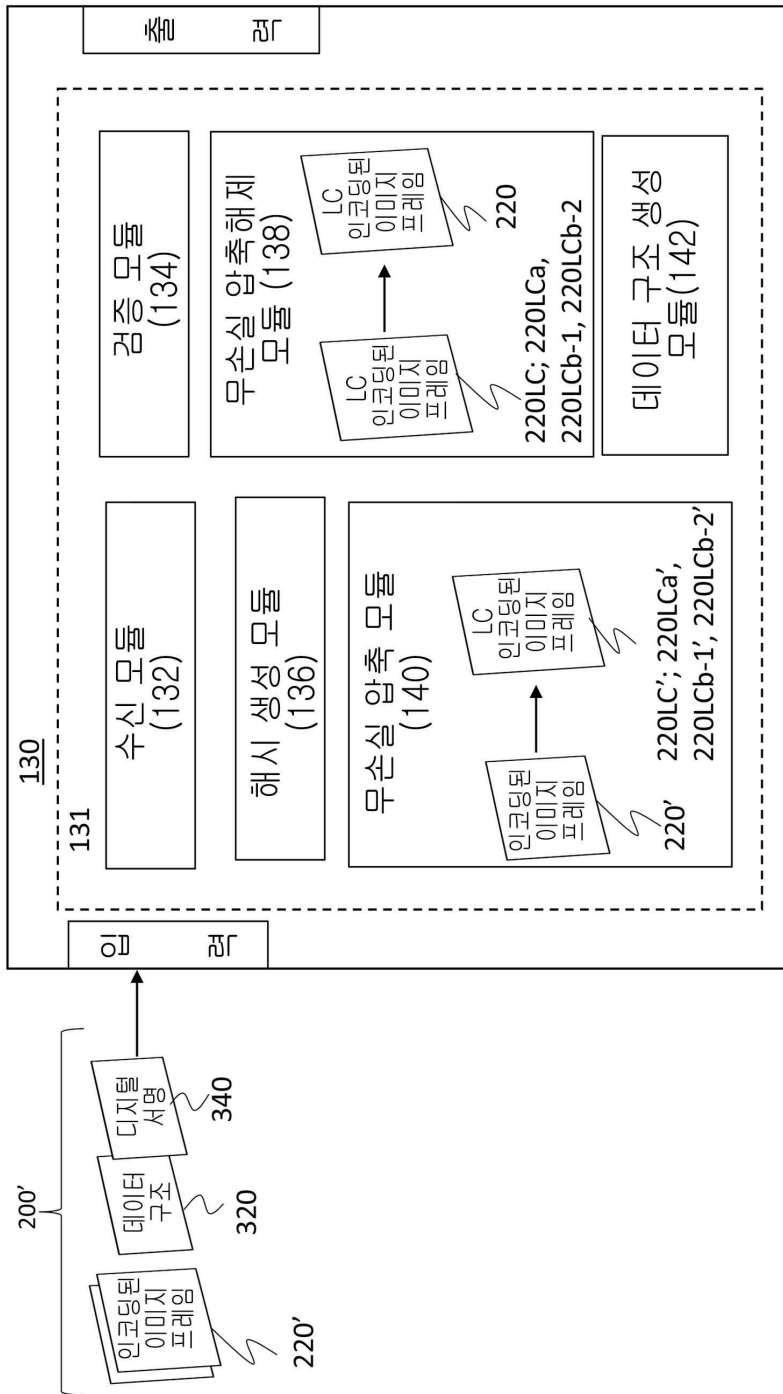
도면2b



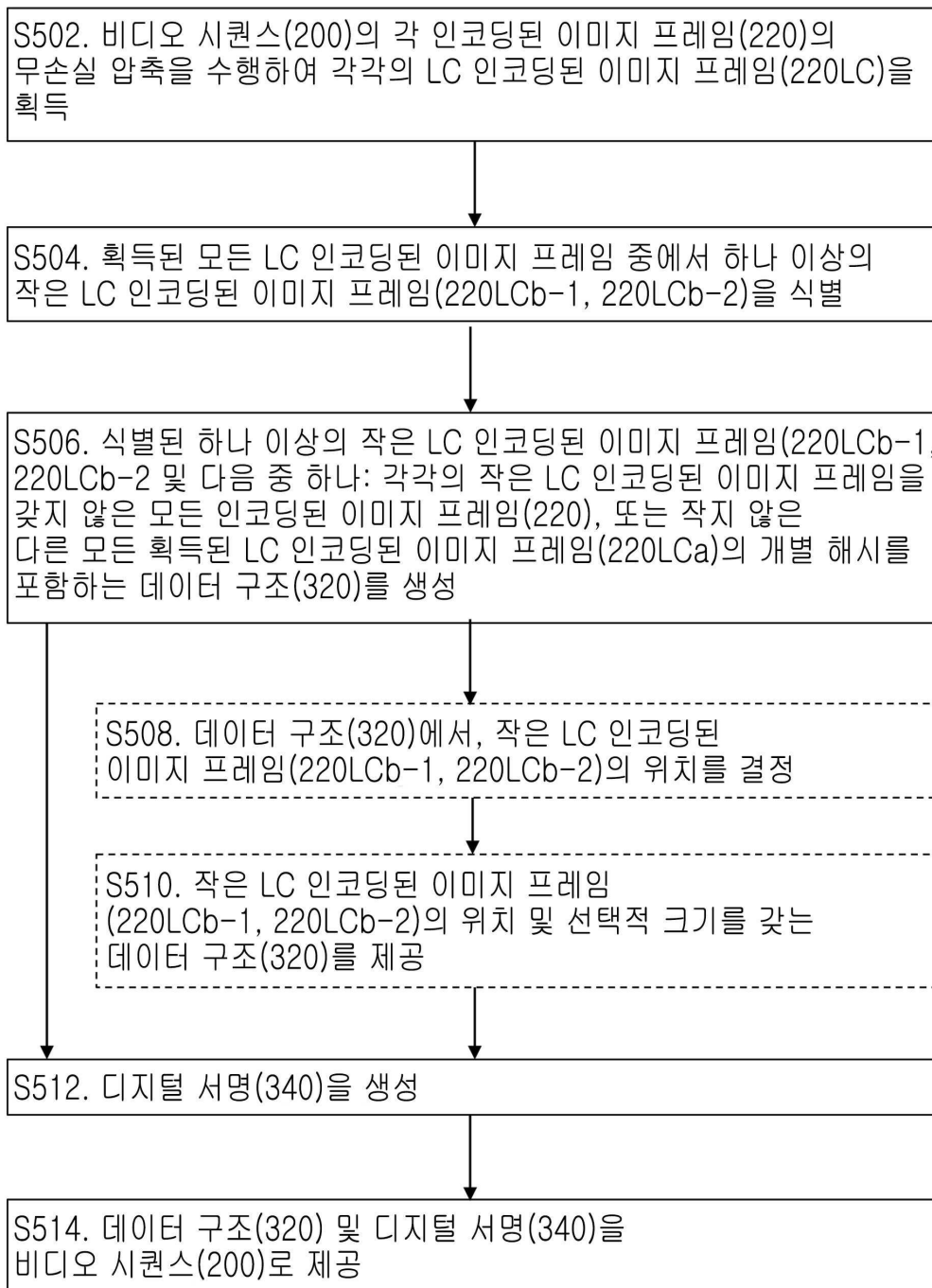
도면3



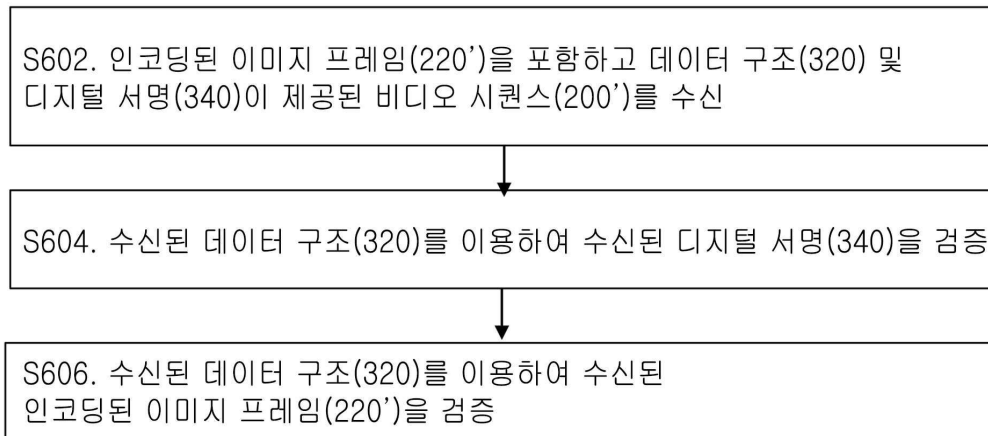
도면4



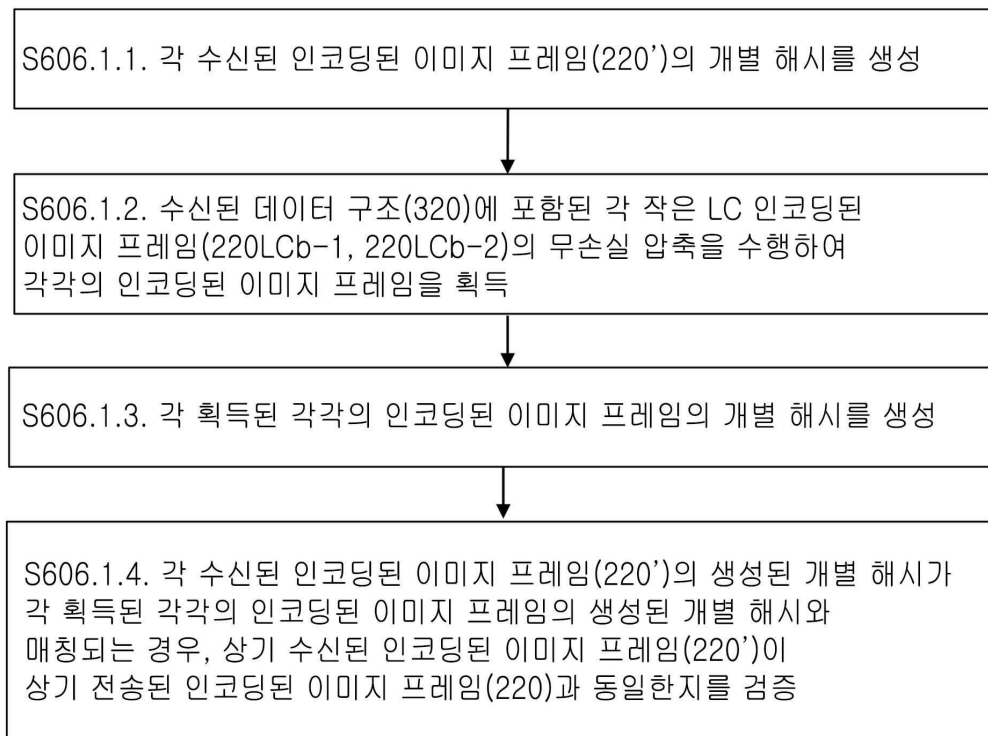
도면5



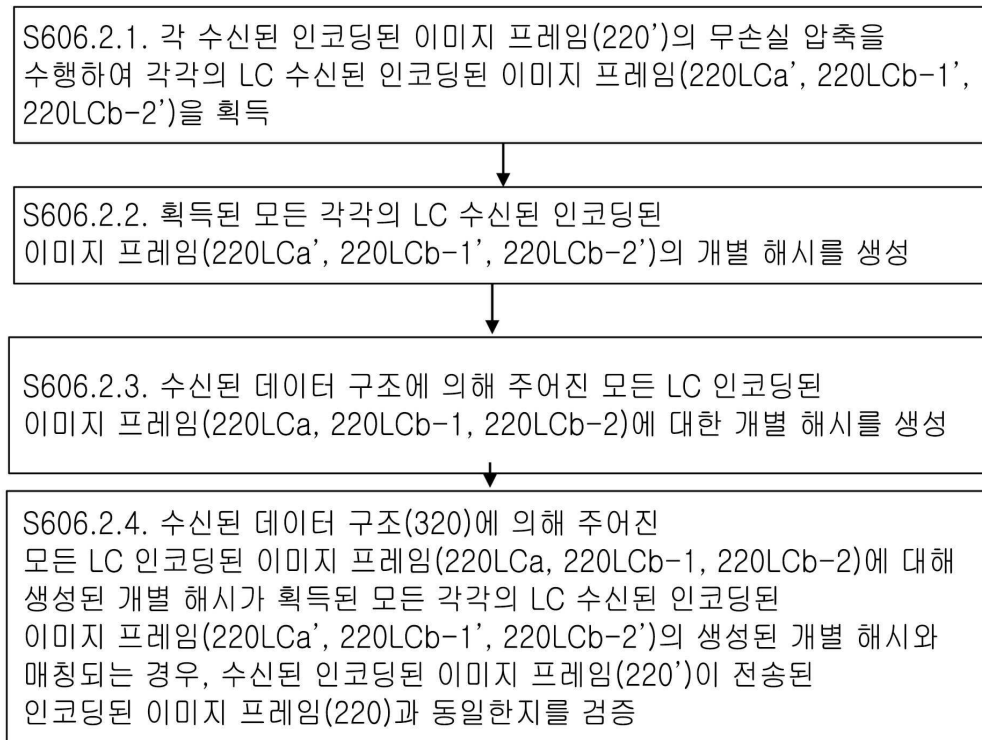
도면6



도면7a



도면7b



도면7c

