(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0130213
(43) 공개일자 2014년11월07일

(51) 국제특허분류(Int. Cl.)
H04N 21/4623 (2011.01) *H04N 21/6334* (2011.01)
H04N 21/83 (2011.01)
(21) 출원번호 10-2014-7027033
(22) 출원일자(국제) 2013년03월15일
심사청구일자 2014년09월25일
(85) 번역문제출일자 2014년09월25일
(86) 국제출원번호 PCT/US2013/031894
(87) 국제공개번호 WO 2013/148304
국제공개일자 2013년10월03일
(30) 우선권주장
13/434,399 2012년03월29일 미국(US)

(71) 출원인
알까뗄 루슨트
프랑스 92100 불론뉴-비영꾸르 루뜨 들 라 렌느 148/152
(72) 발명자
렌 얀송
미국 텍사스주 75075 플래노 웨스트 플래노 파크웨이 3400
오고만 로렌스
미국 뉴저지주 07974-0636 머레이 힐 마운틴 애비뉴 600-700
(뒷면에 계속)
(74) 대리인
제일특허법인

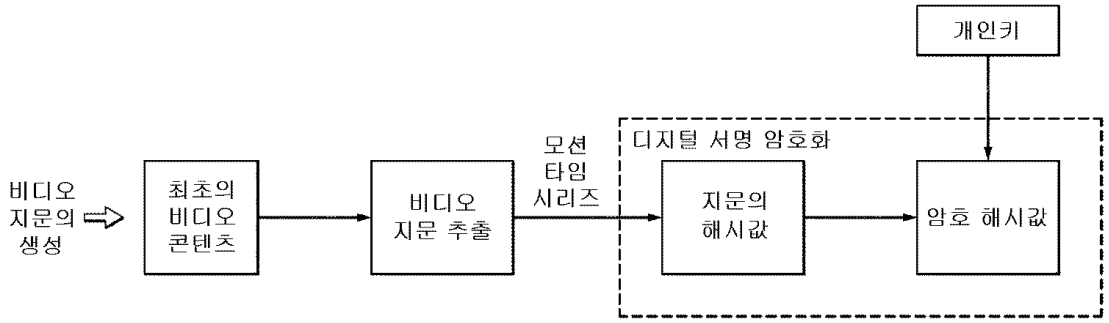
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **비디오 콘텐츠를 인증하는 방법 및 장치**

(57) 요 약

비디오 콘텐츠를 인증하는 방법은 통신 네트워크 내의 수신 노드에서 전송 노드로부터 디지털 서명과, 보호되지 않은 비디오 지문과, 보호되지 않은 비디오 콘텐츠를 수신하는 단계와, 수신 노드에서 상기 디지털 서명이 상기 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여, 보호되지 않은 비디오 지문을 검증하는 단계와, 수신 노드에서 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 상기 보호되지 않은 비디오 지문을 검증하는 단계를 포함한다. 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증된다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서 후속 사용을 위하여 인증된다. 방법과 연관된 수신 노드는 입력 모듈, 지문 검증 모듈, 콘텐츠 검증 모듈 및 컨트롤러 모듈을 포함한다.

대 표 도



(72) 발명자

장 존 알

캐나다 티2엠4지7 앨버타 캘거리 몰리 티알 노스웨스트 2816

우드 토마스 엘

미국 뉴저지주 07733 홈델 홈델-키포트 로드 791

특허청구의 범위

청구항 1

비디오 콘텐츠를 인증하는 방법으로서,

통신 네트워크 내의 수신 노드에서 전송 노드로부터 디지털 서명(a digital signature)과, 보호되지 않은 비디오 지문(an unsecured video fingerprint)과, 보호되지 않은 비디오 콘텐츠를 수신하는 단계와,

상기 수신 노드에서 상기 디지털 서명이 상기 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여, 상기 보호되지 않은 비디오 지문을 검증(verify)하는 단계와,

상기 수신 노드에서 상기 보호되지 않은 비디오 지문이 상기 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 상기 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도(a predetermined measure of loss)를 감내하는(tolerate) 방식으로 상기 보호되지 않은 비디오 콘텐츠를 검증하는 단계를 포함하되,

만일 상기 보호되지 않은 비디오 지문과 상기 보호되지 않은 비디오 콘텐츠가 검증된다면, 상기 보호되지 않은 비디오 콘텐츠는 상기 수신 노드에서 후속 사용을 위하여 인증되는

비디오 콘텐츠 인증 방법.

청구항 2

제 1 항에 있어서,

상기 보호되지 않은 비디오 지문은 최초의 비디오 지문의 수신 버전이고, 상기 최초의 비디오 지문은, 상기 전송 노드에 의한 상기 최초의 비디오 지문의 전송에 앞서서 지문 채취 알고리즘(a fingerprinting algrithm)을 사용하여, 최초의 비디오 콘텐츠로부터 도출되고,

상기 디지털 서명은, 상기 전송 노드에 의한 상기 디지털 서명의 전송에 앞서 암호화(encryption) 알고리즘 및 개인키를 사용하여, 최초의 해시값(hash value)으로부터 생성되고,

상기 최초의 해시값은, 상기 최초의 해시값의 암호화에 앞서 해싱 알고리즘을 사용하여, 상기 최초의 비디오 지문으로부터 도출되는

비디오 콘텐츠 인증 방법.

청구항 3

제 1 항에 있어서,

상기 보호되지 않은 비디오 지문의 검증과 관련하여, 상기 방법은,

상기 수신 노드에서 복호 알고리즘과 공개키를 사용하여 상기 디지털 서명을 복호하여, 상기 최초의 해시값과 관련된 복호 해시값을 획득하는 단계와,

상기 수신 노드에서 상기 해싱 알고리즘을 사용하여 상기 보호되지 않은 비디오 지문을 처리하여, 상기 최초의 해시값과 관련된 새로운 해시값을 획득하는 단계와,

상기 수신 노드에서 상기 새로운 해시값을 상기 복호 해시값과 비교하여, 만일 상기 새로운 해시값과 상기 복호 해시값이 매칭한다면, 상기 보호되지 않은 비디오 지문이 검증되도록 하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

청구항 4

제 2 항에 있어서,

상기 보호되지 않은 비디오 콘텐츠의 검증과 관련하여, 상기 방법은,

상기 보호되지 않은 비디오 지문은 최초의 비디오 지문의 수신 버전이고, 상기 최초의 비디오 지문은, 상기 전송 노드에 의한 상기 최초의 비디오 지문의 전송에 앞서서 지문 채취 알고리즘을 사용하여, 최초의 비디오 콘텐츠로부터 도출되고,

상기 지문 채취 알고리즘을 사용하여 상기 수신 노드에서 상기 보호되지 않은 비디오 콘텐츠를 처리함으로써 새로운 비디오 지문을 생성하는 단계와,

복잡도-불변 거리 측정 알고리즘(a complexity-invariant distance measure algorithm)을 사용하여 상기 수신 노드에서 상기 보호되지 않은 비디오 지문과 상기 새로운 비디오 지문 간의 거리 메트릭을 결정하는 단계와,

상기 수신 노드에서 상기 거리 메트릭을 미리 결정된 임계값과 비교하여, 만일 상기 거리 메트릭이 상기 미리 결정된 임계값을 초과하지 않는다면, 상기 보호되지 않은 비디오 콘텐츠가 검증되도록하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

청구항 5

제 4 항에 있어서,

상기 지문 채취 알고리즘의 사용과 관련하여, 상기 방법은

상기 보호되지 않은 비디오 콘텐츠로부터 비디오 프레임의 샘플을 선택하고 상기 샘플 비디오 프레임을 연결된 시간 시퀀스(a concatenated time sequence)로 정렬하는 단계와,

각 샘플 비디오 프레임 내의 돌출 특징점(salient feature points)을 검출하는 단계와,

상기 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의 각 돌출 특징점에 대한 광 흐름의 각도 방향들(angular orientations)을 계산하는 단계와,

각 샘플 비디오 프레임의 상기 돌출 특징점들에 대한 상기 각도 방향들을 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈들(angular range bins)로 분배하는 단계와,

상기 연결된 시간 시퀀스에 걸쳐 상기 샘플 비디오 프레임들에 대한 각각의 각도 레인지 내의 값들을 연결하여 각각의 각도 레인지 빈에 대한 히스토그램을 형성하는 단계와,

상기 각도 레인지 빈들에 대한 일련의 히스토그램을 정규화하여, 상기 새로운 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

청구항 6

제 5 항에 있어서,

상기 지문 채취 알고리즘을 사용하여 상기 새로운 지문을 설정하는 것과 관련하여, 상기 방법은,

선형 세그멘테이션 알고리즘(a linear segmentation algorithm)을 사용해서 각 모션 타임 시리즈 압축하여, 상기 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하는 단계와,

타임 특징과 진폭 특징 중에 적어도 하나의 특징에 대한 미리 결정된 임계값 보다 더 큰 선형 세그먼트 선택에, 적어도 부분적으로 기초하여, 각 압축된 모션 타임 시리즈로부터의 주 경사들(major inclines)을 추출하여, 상기 추출된 주 경사들에 의해 표현되는 상기 새로운 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

청구항 7

비디오 콘텐츠를 인증하는 방법으로,

소스 장치로부터 비디오 콘텐츠를 수신하는 단계와,

지문 채취 알고리즘을 사용하여 상기 비디오 콘텐츠를 처리함으로써, 비디오 지문을 생성하는 단계와,

해싱 알고리즘을 사용하여 상기 비디오 지문을 처리하여, 최초의 해시값을 획득하는 단계와,

암호화 알고리즘과 개인키를 사용하여 상기 최초의 해시값을 암호화하여, 상기 최초의 해시값과 관련된 디지털 서명을 획득하는 단계와,

상기 디지털 서명, 상기 비디오 지문 및 상기 비디오 콘텐츠를 전송 노드에서의 저장 장치 내에 적어도 일시적으로 저장하는 단계와,

상기 디지털 서명, 상기 비디오 지문 및 상기 비디오 콘텐츠를 상기 전송 노드로부터 하나 이상의 통신 세션에서 통신 네트워크 내의 수신 노드로 전송하는 단계를 포함하는

비디오 콘텐츠 인증 방법.

청구항 8

제 7 항에 있어서,

상기 수신 노드는, 상기 디지털 서명, 상기 비디오 지문 및 상기 비디오 콘텐츠를 상기 전송 노드로부터 수신한 후에, 상기 복호 해시값이 상기 수신한 비디오 지문과 일치하는지 여부를 결정하여 상기 수신한 비디오 지문을 검증하고, 또한, 상기 수신한 비디오 지문이 상기 수신한 비디오 콘텐츠와 일치하는지 여부를 결정하여, 상기 수신한 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는(tolerate) 방식으로 상기 수신한 비디오 콘텐츠를 검증하는

비디오 콘텐츠 인증 방법.

청구항 9

제 7 항에 있어서,

상기 지문 채취 알고리즘의 사용과 관련하여, 상기 방법은,

상기 비디오 콘텐츠로부터 비디오 프레임의 샘플을 선택하고 상기 샘플 비디오 프레임을 연결된 시간 시퀀스로 정렬하는 단계와,

각 샘플 비디오 프레임 내의 돌출 특징점을 검출하는 단계와,

상기 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 상기 대응하는 돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의 각 돌출 특징점에 대한 광 흐름의 각도 방향들(angular orientations)을 계산하는 단계와,

각 샘플 비디오 프레임의 상기 돌출 특징점들에 대한 상기 각도 방향들을 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈들(angular range bins)로 분배하는 단계와,

상기 연결된 시간 시퀀스에 걸쳐 상기 샘플 비디오 프레임들에 대한 각 각도 레인지 내의 값들을 연결하여 각 각도 레인지 빈에 대한 히스토그램을 형성하는 단계와,

상기 각도 레인지 빈들에 대한 일련의 히스토그램을 정규화하여, 상기 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

청구항 10

제 9 항에 있어서,

상기 비디오 지문을 설정하는 상기 지문 채취 알고리즘의 사용과 관련하여, 상기 방법은,

선형 세그멘테이션 알고리즘을 사용해서 각 모션 타임 시리즈를 압축하여, 상기 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하는 단계와,

타임 특징과 진폭 특징 중에 적어도 하나의 특징에 대한 미리 결정된 임계값 보다 더 큰 선형 세그먼트 선택에, 적어도 부분적으로 기초하여, 각 압축된 모션 타임 시리즈로부터의 주 경사들(major inclines)을 추출하여, 상기 추출된 주 경사들에 의해 상기 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성하는 단계를 더 포함하는

비디오 콘텐츠 인증 방법.

명 세 서

배 경 기 술

[0001] 본 개시는 다양한 접근 장치, 네트워크 아키텍처 및 통신 프로토콜을 수용하기 위하여 전송 중에 의도적으로 변경될 수 있는 비디오 콘텐츠를 인증하는 방법 및 장치에 관련된다. 다양한 실시예에서, 전송 노드나 수신 노드, 또는 둘 다 이러한 프로세스를 수행한다. 이 프로세스의 다양한 실시예는 비디오 콘텐츠의 비디오 지문(video fingerprint)과 암호화된 디지털 서명을 사용하여 대응하는 비디오 지문과 비디오 콘텐츠를 별도로 검증함으로써 비디오 콘텐츠를 인증한다. 본 출원에 개시되는 비디오 콘텐츠를 인증하는 프로세스의 다양한 실시예는 수신 노드에서 비디오 콘텐츠의 미리 결정된 손실 한도를 감내한다. 예를 들면, 본 출원에 개시되는 방법과 장치는 모바일 및 고정 카메라로부터 정부 안전 기관, 군사 기관, 뉴스 기관 및 일반 대중으로의 광범위한 실시간 비디오 접근을 허용한다.

[0002] 공중 감시 카메라는 길, 도시의 보도, 공항, 지하철, 군사 기지, 학교 및 상점과 같은 다양한 장소에 보안과 안전을 목적으로 설치된다. 10년 전 쯤에, 이러한 비디오 공급은 사적이며, 경찰, 군대 또는 사설 보안 회사 같은 단일 엔티티에 의해서만이 시청 가능하였다. 그러나, 공중 감시 비디오는 복수의 보안 엔티티(예를 들면, 경찰, 소방차, 구급차, 가정 보안, 등)에 의한 사용을 가능하게 하고, 다양한 사용 목적(예를 들면, 보안 태스크의 대중 소싱(crowd-sourcing), 교통 체증에 대한 정보 획득, 등)의 대중 접근을 가능하게 하도록, 온전하게(in-the-clear) 송신되는 것이 점점 더 일상화되고 있다. 온전한(in-the-clear) 비디오 콘텐츠는 암호화되어 있지 않아서, 공개 접근을 가능하게 하거나, 적어도 암호화되어 실행되는 것보다 좀 더 광범위한 접근을 가능하게 한다. 따라서, 소스 데이터 변경과 사람이 개입된 변경을 포함하는 악의적인 공격에 대항하기 위한 콘텐츠 인증에 대한 수요가 있다. 예를 들면, 공격은 비디오 스트림을 가로채고 프레임을 재정렬하거나 사전에 기록된 새로운 비디오를 주입함으로써 범죄 증거를 제거할 수 있다. 인증은 수신기(예를 들면, 수신자) 측(예를 들면, 보안 통제국)에서 수신한 비디오 콘텐츠가 비디오 카메라에서 캡처하거나 송신기 말단에서 다른 소스에 의해 공급된 최초의 비디오 콘텐츠와 동일하다는 것을 보증한다. 예를 들면, 이것은 공중 안전과 최초의 응답자 통신에 사용될 수 있는 LTE 모바일 비디오의 보안에 적절하다.

[0003] 비디오 콘텐츠 인증에 관한 많은 솔루션이 있다. 일반적으로, 이들은 3개의 카테고리, 1) 대칭 암호화, 2) 비대칭 암호화를 사용한 디지털 서명, 3) 워터마킹으로 분류될 수 있다. 그러나 이러한 현존하는 솔루션 중에 어느 것도, 광범위한 장치가 비디오 통신의 소스와 수신자(즉, 수신기) 측 모두에 대해 사용되는 곳에서, 광범위한 수신자 전반에 비디오 콘텐츠를 인증해야 하는 최근의 수요를 충족할 수 없다.

[0004] 대칭 암호화는 많은 상이한 보안 에이전시가 단일의 복호키를 분배하고 공유해야 하기 때문에 충분하지 않다. 보안에서, 이것은 키 관리 문제점으로 알려져 있다. 너무 많은 키를 분배하는 것은 불가피하게 시스템 보안을 감소시킨다. 좀 더 상세하게, 대칭 암호화는 완전히 계층화된 암호화와 선별적이거나 치환-기반(permutation-based)의 암호화를 포함한다. 완전히 계층화된 암호화에서, 비디오 콘텐츠가 압축된 다음에 암호화된다. 이러한 접근 방법은 대개 과중한 계산과 느린 속도를 야기하여, 실시간 비디오 인증에 부적합하게 된다. 선별적인 치환

-기반의 암호화는 선별적으로 바이트를 암호화하거나 또는 치환을 사용하여 비디오 콘텐츠를 스크램블링 한다. 이러한 유형의 접근방법은 전형적으로, H.264나 MPEG 같은, 특정 비디오 포맷을 위해 설계된다. 예를 들면, MPEG에서, 대칭 암호화는 I-프레임, P-프레임 및 B-프레임 간의 관계에 기초하여 바이트를 선택하고 치환하도록 사용된다. 일반적으로, 이러한 접근 방법은 포맷을 준수하지 않는다.

[0005] 비대칭 암호화를 사용하는 디지털 서명은 일반적으로 사용되는 암호화 방법으로서 데이터 인증에 매우 안전하다. 그러나, 암호화 계산의 성격상, 이것은 수신한 데이터가 소스 데이터와 동일할 것을 요구하고, 다르다면 인증하지 않을 것이다. (특히 무선 채널을 통한) 비디오 전송과 관련된 문제점은 최초의 콘텐츠가 채널 내의 노이즈 때문에 변경되거나 또는 장치의 용량 때문에 비디오를 (예를 들면, 모바일 장치의 더 작은 스크린으로) 크기 조절할 수 있다는 것이다. 그러므로, 비록 데이터가 악의적으로 변경되지 않더라도, 수신한 데이터가 최초의 것과 정확하게 동일하지 않을 수 있고, 이 경우에 인증하지 않는 오류(즉, 잘못된 거부)가 발생할 것이다.

[0006] 비대칭 암호화 및 디지털 서명은 하르 웨이블릿(Harr wavelet) 필터, 이산 코사인 변환(DCTs), 또는 웨이블릿 변환을 프레임에 적용하고, 획득한 파라미터에 기초하여 해시값을 생성함으로써 획득될 수 있다. 암호화 보안을 구현하는 규격화된 카메라의 예는 캐나다 산호세의 시스코 시스템즈사의 시스코 비디오 감시 2500 시리즈 IP 카메라이다. 이것은 고급 암호화 표준(advanced encryption standard, AES)을 사용하는 하드웨어 기반의 비대칭 암호화를 포함한다.

[0007] 비대칭 암호화 및 디지털 서명 솔루션의 변종은 암호화 체크섬을 기반으로 하며, 이는 전체 프레임, 주기적 프레임, 패킷 또는 주기적 패킷의 디지털 서명된 체크섬을 제공한다. 암호화 체크섬 솔루션은 변경 검출과 메시지 무결성 검사를 제공한다. 이는 전송 동안 비디오 패킷이 손실되는 케이스를 처리할 수 있다. 그러나, 비디오가 의도적으로 변경되는 경우에, 예를 들면, 4G 모바일에서의 크기-축소나 트랜스코딩(transcoding)의 경우나, 또는 HTTP 적응형 비트율 스트리밍의 경우에, 체크섬이 각각의 변경 노드에서 재적용되지 않는다면, 암호-체크섬은 변경된 비디오에 매칭되지 않을 것이다. 이것은 사유 네트워크(proprietary network)에서 가능하지만, 비-표준이며, 모든 노드에서 암호키(들)를 분배하고 안전하게 유지하기에는, 상당히 복잡한(그리고 잠재적으로 안전하지 않은) 키 관리를 수반할 것이다.

[0008] 워터마킹은 대칭 및 비대칭 암호화와 관련된 문제를 회피할 수 있어서 현 문제점에 대한 유효한 솔루션이다. 그러나, 워터마킹은 고유의 단점을 갖는다. 워터마크는 최초의 비디오에 삽입되기(embedded) 때문에, 비디오를 불가피하게 변경한다. 워터마크의 트레이드오프는 삽입된 워터마크의 비가시성(imperceptibility)과 대비되는, 인증을 수행하기 위한 비디오로부터의 워터마크 추출 능력이다. 현재의 문제에서, 비디오를 변경하는 것은 바람직하지 않고, 인증의 성공을 최대화하는 것이 바람직하다. 이러한 상황에서, 워터마크를 비디오에 삽입하는 것은 바람직하지 않다. 디지털 워터마킹은 정보를 비디오 프레임으로 삽입하여 진본 여부를 검증한다. 워터마킹 기법은 압축되지 않은 비디오와 압축된 비디오(예를 들면, H.264) 모두를 위해 존재한다.

[0009] 전술한 사항에 기초하여, 비디오 콘텐츠를 인증하는 프로세스는 다양한 네트워크 아키텍처와 통신 프로토콜에 걸쳐서 다양한 사용자 장치를 사용하는 다양한 개인에게 접근을 허용하는 한편, 비디오 콘텐츠가 예상치 못하게 변경되거나, 은밀하게 변경되거나, 또는 사해 의도로 변경되는 경우에 감지할 수 있다. 이러한 폭 넓은 접근을 허용하기 위하여, 프로세스는 전송 동안에 적법하게 예정대로 변경된 비디오 콘텐츠를 감내(tolerate)할 수 있어야 한다.

발명의 내용

과제의 해결 수단

[0010] 일 양태에서, 비디오 콘텐츠를 인증하는 방법이 제공된다. 일 실시예에서, 방법은, 통신 네트워크 내의 수신 노드에서 전송 노드로부터 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠를 수신하는 단계와, 수신 노드에서 디지털 서명이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여, 보호되지 않은 비디오 지문을 검증하는 단계와, 수신노드에서 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도(measure)를 감내하는(tolerate) 방식으로 보호되지 않은 비디오 지문을 검증하는 단계를 포함한다. 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증된다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서 후속 사용을 위

하여 인증된다.

[0011] 다른 양태에서, 비디오 콘텐츠를 인증하는 장치가 제공된다. 일 실시예에서, 장치는 통신 네트워크 내의 수신 노드에서 전송 노드로부터 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠를 수신하도록 구성되는 입력 모듈과, 수신 노드에서 디지털 서명이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여 보호되지 않은 비디오 지문을 검증하도록 구성되는 지문 검증 모듈과, 수신 노드에서 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 보안 되지 않은 비디오 지문을 검증하도록 구성되는 콘텐츠 검증모듈과, 입력 모듈, 지문 검증 모듈 및 콘텐츠 검증 모듈과 동작가능하게 통신하는 컨트롤러 모듈을 포함하고, 컨트롤러 모듈은, 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증된다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서 후속 사용을 위하여 인증되도록 동작을 제어하도록 구성된다. 보호되지 않은 비디오 지문은 최초의 비디오 지문의 수신 버전이다. 최초의 비디오 지문은 전송 노드에 의한 최초의 비디오 지문의 전송 이전에 지문 채취 알고리즘을 사용하여 최초의 비디오 콘텐츠로부터 도출된다.

[0012] 여전히 다른 양태에서, 비디오 콘텐츠를 인증하는 방법이 제공된다. 일 실시예에서, 방법은, 소스 장치로부터 비디오 콘텐츠를 수신하는 단계와, 지문 채취 알고리즘을 사용하여 비디오 콘텐츠를 처리하여 비디오 지문을 생성하는 단계와, 해싱 알고리즘을 사용하여 비디오 지문을 처리하여 최초의 해시값을 획득하는 단계와, 암호화 알고리즘과 개인키를 사용하여 최초의 해시값을 암호화하여 최초의 해시값과 관련된 디지털 서명을 획득하는 단계와, 전송 노드에서 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 저장 장치 내에 적어도 일시적으로 저장하는 단계와, 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 전송 노드로부터 하나 이상의 통신 세션에서 일 통신 네트워크 내의 수신 노드로 전송하는 단계를 포함한다.

[0013] 여전히 다른 양태에서, 비-일시적 컴퓨터-판독가능한 매체가 제공된다. 일 실시예에서, 비-일시적 컴퓨터-판독가능한 매체는, 제1 컴퓨터에 의해 실행될 때, 통신 네트워크와 연관된 컴퓨터-제어되는 수신 노드가 비디오 콘텐츠를 인증하는 방법을 수행하도록 유발하는 제1 프로그램 명령을 저장한다. 일 실시예에서, 방법은, 통신 네트워크 내의 수신 노드에서 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠를 전송 노드로부터 수신한 후에, 수신 노드에서 복호 해시값이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여 보호되지 않은 비디오 지문을 검증하는 단계와, 수신 노드에서 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는(tolerate) 방식으로 보호되지 않은 비디오 콘텐츠를 검증하는 단계를 포함한다. 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증된다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서의 후속 사용을 위하여 인증된다.

[0014] 본 발명이 적용되는 추가적인 영역은 이하 제공되는 상세한 설명으로부터 명백해질 것이다. 그러나, 다양한 변경과 수정은 본 발명이 속하는 기술분야에서 통상의 지식을 갖는 자에게 명백할 것이기 때문에, 발명의 상세한 설명과 특정 예는, 본 발명의 바람직한 실시예로 표현되는 한편, 단지 도해의 목적으로 제공된다는 것이 이해되어야 한다.

도면의 간단한 설명

[0015] 본 발명은 장치의 구조, 배열 및 여러 부품의 조합과, 방법의 단계에 존재하며, 고려되는 목적은 아래에서 좀더 충분하게 설명되고, 청구범위에 명시적으로 기술되며, 또한 첨부되는 도면에 도시된다.

도 1은 비디오 콘텐츠를 인증하는 프로세스의 표본 실시예를 보여주는 기능적 다이어그램이다.

도 2는 특징점을 검출하고, 특징점에 대한 광 흐름의 각도 방향을 다음 샘플 프레임과 관련하여 시간에 걸쳐서 계산하고, 각도 방향을 각도 레인지 빈(angular range bins)으로 분배하는 지문 채취(fingerprinting) 알고리즘의 표본 실시예를 사용하여 분석된 비디오 콘텐츠의 샘플 프레임의 표본 예를 보여준다.

도 3은 도 2와 연관된 지문 채취 알고리즘의 표본 실시예를 사용하는 비디오 콘텐츠에 대한 비디오 지문의 생성과 관련하여 시간 경과에 따른 표본 각도 레인지 빈에 대한 모션 타임 시리즈를 보여주는 그래프이다.

도 4는 선형 세그멘테이션 처리 이후의 도 3의 표본 모션 시리즈를 보여주는 그래프이다.

도 5는 주 경사(major inclines) 추출 이후의 도 4의 표본 모션 시리즈를 보여주는 그래프이다.

도 6은 비디오 콘텐츠를 인증하는 프로세스의 다른 표본 실시예를 보여주는 기능적 다이어그램이다.

도 7은 비디오 콘텐츠의 비디오 지문을 생성하는 프로세스의 일 실시예를 보여주는 기능적 다이어그램이다.

도 8은 다양한 지문 채취 알고리즘의 성능의 계량적인 비교 결과를 보여주는 테이블이다.

도 9는 비디오 콘텐츠를 인증하는 프로세스의 표본 실시예의 흐름도이다.

도 10은 도 9와 조합하여, 비디오 콘텐츠를 인증하는 프로세스의 다른 표본 실시예의 흐름도이다.

도 11은, 도 9 및 도 10과 조합하여, 비디오 콘텐츠를 인증하는 프로세스의 또 다른 표본 실시예의 흐름도이다.

도 12는, 도 9와 조합하여, 비디오 콘텐츠를 인증하는 프로세스의 또 다른 표본 실시예의 흐름도이다.

도 13은, 도 9 및 도 12와 조합하여, 비디오 콘텐츠를 인증하는 프로세스의 또 다른 표본 실시예의 흐름도이다.

도 14는 비디오 콘텐츠를 인증하는 수신 노드의 표본 실시예의 블록도이다.

도 15는, 도 14의 수신 노드와 연관되는, 지문 검증 모듈의 표본 실시예의 블록도이다.

도 16은, 도 14의 수신 노드와 연관되는, 지문 검증 모듈의 표본 실시예의 블록도이다.

도 17은 비디오 콘텐츠를 인증하는 프로세스의 다른 표본 실시예의 흐름도이다.

도 18은, 도 17과 조합하여, 비디오 콘텐츠를 인증하는 프로세스의 또 다른 표본 실시예의 흐름도이다.

도 19는 비디오 콘텐츠를 인증하는 전송 노드의 표본 실시예의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 비디오 콘텐츠를 인증하는 방법과 장치의 다양한 실시예가 본 출원에서 개시된다. 실시예는 비디오 지문(video fingerprint)과 디지털 서명을 결합하는 비디오 인증 솔루션을 기술한다. 특정 실시예에서, 비디오 지문과 디지털 서명은 (삽입 되지 않고) 비디오 콘텐츠와는 별도로 송신된다. 다른 실시예에서, 비디오 지문과 디지털 서명은 비디오 콘텐츠에, 예를 들면, 워터마크로서 또는 적합한 삽입 기법으로, 삽입될 수 있다. 본 출원에서 설명되는 인증 프로세스는 비디오 콘텐츠가 예고 없이 변경되거나, 억지로 변경되거나, 또는 사해 의도로 변경되는 경우에 이를 검출하는 한편, 전송 동안 적법하게 예정대로 변경된 비디오 콘텐츠를 인증할 수 있도록 구성된다. 본 출원에서 기술되는 다양한 실시예는, 1995년 2월 25일에 출원되어, Lucent Technologies사에 양도된, 미국 특허 제5,799,092호에 개시된, 자가-검증 식별 카드와 관련된 몇몇 인증 개념을 기반으로 하며, 그 내용은 본 출원에서 전체적으로 참고문헌으로 인용된다.

[0017] 도 1을 참조하면, 비디오 콘텐츠를 인증하는 프로세스의 표본 실시예는 최초의 비디오 콘텐츠로부터 비디오 지문을 추출하면서 시작된다. 비디오 지문은 비디오 콘텐츠에 대한 명확하고 정확한 서술(description)을 제공한다. 비디오 지문은 디지털 서명을 획득하기 위하여 암호화되어 서명된다. 예를 들면 비디오 지문은 해시값을 획득하기 위해서 해시 함수(a hash function)를 사용하여 처리될 수 있다. 최초의 해시값은 최초의 비디오 콘텐츠의 소스와 연관된 개인키를 사용하여 암호화되어 디지털 서명을 생성할 수 있다. 디지털 서명은 두 개의 속성을 갖는데, 1) 최초의 비디오에 대해 유일하고, 2) 비디오 콘텐츠의 진본 소스를 캡처하는, 개인키의 소유자를 제외한 어느 누구에 의해서도 생성될 수 없다. 따라서, 디지털 서명은 비디오 콘텐츠의 진정성을 인증하는 상당히 안전한 수단이다.

[0018] 만일 비디오 스트림이, 전송 이전이나, 전송 동안이나, 또는 전송 이후에, 의도적으로 변경된다면, 아마도 4G 무선 전송(그리고 다른 어플리케이션)에 대하여, 표준 디지털 서명은 단독으로 비디오 콘텐츠를 인증하도록 사용될 수 없는데, 이는 수신한 비디오 콘텐츠가 특정 적법한 상황에서의 인증에 대하여 최초의 비디오 콘텐츠와 반드시 정확하게 일치하지 않을 수 있기 때문이다. 따라서, 온전한(in-the-clear)(즉, 암호화되지 않은(unencrypted)) 비디오 지문이 디지털 서명 및 온전한(즉, 암호화되지 않은) 비디오 콘텐츠와 함께 비디오 수신자에게 송신된다.

[0019] 좀 더 상세하게, 비디오 송신자(예를 들면, 비디오 캡처, 비디오 소스, 등) 측에서, 비디오 콘텐츠를 인증하는 프로세스의 표본 실시예는 최초의 비디오 콘텐츠에 대한 비디오 지문을 생성하는 단계를 포함한다. 비디오 지문은 모션 타임 시리즈를 생성하도록 비디오 콘텐츠의 돌출 특징(salient features)의 궤적을 추적함으로써 획득될 수 있다. 최초의 비디오 콘텐츠는 주기적으로 또는 랜덤하게 샘플링된 프레임 시퀀스로 표현될 수 있다. 각 샘플링된 프레임에 대해서, 가속된 세그먼트 테스트로부터의 특징(FAST) 알고리즘 같은, 국소(local) 특징 검출

기가 돌출 특징점을 검출하도록 사용될 수 있다. FAST 알고리즘에 대한 추가적인 정보는, 그 내용이 본 출원에서 전체적으로 참조문헌으로 인용되는, Rosten et al., Machine Learning for High-Speed Corner Detection, Proceedings of European Conference on Computer Vision, 2006, pp. 430-443을 참조하라.

[0020] 검출된 특징점들의 궤적은, 루카스-카나데(Lucas-Kanade) 알고리즘과 같은, 광 흐름 기술을 사용하여 추적될 수 있다. 루카스-카나데 알고리즘의 추가적인 정보는, 그 내용이 본 출원에서 전체적으로 참조문헌으로 인용되는, Lucas et al. An Iterative Image Registration Technique with an Application to Stereo Vision, Procedings of DARPA Imaging Understanding Workshop, April, 1981, pp. 121-130을 참조하라.

[0021] 특징점의 이동 방향은 특정 수의 빈(bin)으로 나뉠 수 있다. 예를 들면, 8 개의 빈의 경우에, 각각의 빈이 45도 방향 범위를 표현하면서, 360도의 방향 레인지를 커버한다(예를 들면, 빈 1 - 0-45도, 빈 2 - 45-90도, 등). 특징점은 방향의 각도에 기초하여 각 빈으로 집합된다. 각 빈에 대하여, 빈의 값을 시간에 걸쳐 연결함으로써 히스토그램이 생성된다.

[0022] 도 2를 참조하면, 검출된 특징점과 이들의 계산된 광 흐름을 갖는 비디오 프레임의 예가 도시된다. 프레임의 오른편 윗쪽에 도시된 히스토그램은 광 흐름의 방향에 대한 빈의 값을 보여준다. 가장 윗 쪽 빈은 0도에서 45도 사이의 방향을 갖는 점의 개수이다. 각 빈은 히스토그램의 위에서 아래로 내려가면서 45도씩 증가하면서 45-도 레인지에 대한 점의 개수를 반영한다. 이미지 내에, 돌출점이 여러 방향으로 움직이는 것을 볼 수 있다.

[0023] (시간에 걸쳐 정규화된) 히스토그램은, 비디오 지문이 각 빈에 대한 모션 타임 시리즈를 포함하는, 모션 타임 시리즈를 형성한다. 예를 들면, 8 개의 빈에 의해, 8 개의 모션 타임 시리즈가 비디오 지문을 형성한다. 도 3은 타임 시리즈의 예를 보여준다. 도 4는 타임 시리즈에 선형 세그멘테이션을 수행한 후의 표본적인 결과를 보여준다. 도 5는 선형 세그멘테이션으로부터 주 경사(major inclines)를 추출한 이후의 표본적인 결과를 보여준다.

[0024] 다시 도 1을 참조하면, 추출된 비디오 지문은 해싱 함수를 통과하여 큰 체크섬 값을 생성한다. 예를 들면, 해싱 함수는 SHA-1로 알려진 암호화 해싱 함수를 사용하거나, SHA-256으로 알려진 다른 암호화 해싱 함수를 사용하여 구현될 수 있다. SHA-1은 160 비트를 사용하고 2^{160}의 보안 강도를 제공한다. SHA-256은 256 비트를 사용하고 2^{256}의 보안 강도를 사용한다. 안전한 해싱 알고리즘(SHAs)(예를 들면, SHA-1, SHA-256 등)에 대한 추가적인 정보는, 그 내용이 전체적으로 본 출원에서 참조 문헌으로 인용되는, Federal Information Processing Standards Publication(FIPS PUB) 180-3, Secure Hash Standard(SHS), Information Technology Laboratory, National Institute of Standards and Technology, October, 2008, 32 pages를 참조하라.

[0025] 비디오 지문은 개인키로 암호화되고 공개키로 복호될 수 있다. 다시 말해서, 공개키를 사용하여, 수신자는 암호화된 비디오 지문을 복호하여 최초의 비디오 지문을 획득할 수 있다. 비록 제 3자가 공개키에 접근할 수 있다고 하더라도, 제 3자가 암호화된 비디오 지문이나 암호화되지 않은 비디오 지문을 갱신하여, 인증 수신자에 의해 제작된 복호화된 비디오 지문이, 센서 측에서 생성된 비디오 지문에 매칭하도록 하는 것은, 계산적으로 가능하지 않다. 예를 들면, 공개키 암호화는 리베스트-셰미르-아델만(Rivest-Shamir-Adelman, RSA) 알고리즘이나 타원 곡선 암호(elliptic curve cryptography, ECC) 알고리즘을 사용하여 구현될 수 있다. RSA 알고리즘에 대한 추가적인 정보는, 그 내용이 전체적으로 본 출원에서 참조 문헌으로 인용되는, Rivest et al., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21, No. 2, February, 1978, pp. 120-126을 참조하라. ECC 알고리즘에 대한 추가적인 정보는, 1) Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol. 48, No. 177, January, 1987, pp. 203-209, 또는 2) Miller, Use of Elliptic curves in Cryptography, Advances in Cryptology - Crypto Proceedings: Lecture Notes in Computer Science, 1986, pp. 417-426을 참조하라. Koblitz와 Miller 문서의 내용은 전체적으로 본 출원에서 참조 문헌으로 인용된다.

[0026] 비디오 송신기 측으로부터의 출력은 온전한 비디오 콘텐츠, 온전한 비디오 지문 및 디지털 서명을 포함한다. 비디오 지문과 디지털 서명을 수신기(즉, 수신자) 측으로 송신하는 몇 가지 방법이 있는데, 1) 최초의 비디오 콘텐츠의 앞이나 뒤에 첨부하여, 2) 별도의 통신 경로(예를 들면, 보안 터널)를 통해, 또는 3)최초의 비디오 콘텐츠 내에 삽입(예를 들면, 워터마크로서)될 수 있다.

[0027] 도 6을 참조하면, 비디오 콘텐츠 전송의 수신기(즉, 수신자) 측에서 비디오 콘텐츠를 인증하는 프로세스의 일 실시예는 두-단계의 프로세스를 포함한다. 즉, 1) 수신한 디지털 서명이 복호화되고 그 결과인 복호 해시값은 수신한 비디오 지문의 새로운(즉, 새롭게 계산된) 해시값과 비교되며, 또한 2) 새로운(즉, 새롭게 계산된) 비디오 지문은 수신한 비디오 콘텐츠로부터 생성되고 수신한 비디오 지문과 비교된다. 만일 새로운 해시값이 수신한

디지털 서명에 정확하게 매칭되고, 또한 새로운 비디오 지문이 수신한 비디오 지문에 거의 매칭된다면, 수신한 비디오 콘텐츠는 최초의 비디오 콘텐츠의 진본으로 간주된다.

[0028] 좀 더 상세하게, 수신기 측에서, 비디오 콘텐츠를 인증하는 프로세스는 비디오 지문의 디지털 서명에 기초한 검증 체크와 비디오 지문에 기초한 다른 검증 체크를 포함한다. 수신한 디지털 서명은 공개키를 사용하여 복호화된다. 수신한 비디오 지문은 송신기 측에 사용된 것과 동일한 해싱 함수를 사용하여 새로운 해시값을 획득하도록 처리된다. 복호된 해시값은 수신한 비디오 지문과 수신한 디지털 서명의 무결성을 체크하기 위하여 새로운 해시값과 비교된다. 만일 복호된 해시값과 새로운 해시값이 매칭된다면, 프로세스는 비디오 지문에 기초하여 2차 검증 체크를 계속한다. 만일 디지털 서명이 매칭되지 않는다면, 프로세스는 종료하고 수신한 비디오 콘텐츠는 진본이 아닌 것으로 간주 된다.

[0029] 2차 검증 체크는 송신자 측에서 사용되는 동일한 지문 채취 알고리즘을 사용하여 새로운 비디오 지문을 획득하도록 수신한 비디오 콘텐츠를 처리하는 단계를 포함한다. 수신한 비디오 지문은 타임 시리즈 매칭을 위한 거리 메트릭을 적용함으로써 새로운 비디오 지문과 비교된다. 거리 메트릭을 측정하는 알고리즘의 다양한 실시예가 이러한 비교의 속도나 정확성을 증가시키기 위해 사용될 수 있다.

[0030] 일반적으로, 수신한 비디오 콘텐츠(예를 들면, Q)와 최초의 비디오 콘텐츠(예를 들면, C)가 주어지면, 거리 메트릭이 두 개의 비디오 지문 내의 대응하는 타임 시리즈 간의 최소 유사도 거리를 발견하도록 사용된다. 비디오 콘텐츠 내의 다양한 변경은 모션 타임 시리즈에서 많은 다중 복잡성을 불러 일으킨다. (오프셋, 진폭 및 위상 스케일링, 와핑(warping), 폐색으로 인해 왜곡될 수 있는) 이러한 변경에 의해 타임 시리즈는 빈번하게 상이한 양의 정점과 저점을 갖게 된다. 동적 타임 와핑(dynamic time warping) 같은, 일반적으로 사용되는 유사도 측정 기법이나, 몇몇 정점과 저점의 부분적인 정렬을 제공하는 것은 이러한 문제를 완전하게 해결하지 못한다. 모션 타임 시리즈 매칭의 다양한 복잡성을 차단하기 위하여, 복잡성-불변 거리 측정(complexity-invariant distance measure) 알고리즘이 두 타임 시리즈 간의 복잡성 차이를 결정하기 위해 현존하는 거리 측정에 대한 교정 팩터로서 사용된다. 복잡성-불변 거리 측정 알고리즘에 대한 추가적인 정보는, 예를 들면, 그 내용이 전체적으로 본 출원에서 참조 문헌으로 인용되는, Batista et al., A complexity-Invariant Distance Measure for Time Series, Proceedings of Society of Industrial and Applied mathematics(SIAM) Conference on Data Mining, April 28-30, 2011, Mesa, Arizona, pp. 699-710을 참조하라.

[0031] 복잡도-불변 거리 측정 알고리즘은 비디오 변환에 의해 이입되는 노이즈에 대하여 충분히 강건한 것으로 실험에 의해 발견되었다. 공식으로,

[0032] $Q=\{\{\theta_{i,j}:0\le i\le f\}:0\le j<b\}$ 과 $C=\{\{\tau_{i,j}:0\le i\le g\}:0\le j<b\}$

[0033] (g≥f라고 가정)이 주어지고, 두 개의 대응하는 타임 시리즈 Q_j, C_j 간의 거리 D는 각 히스토그램 빈 j, $0 \le j < b$, (여기서 b는 빈의 총 개수)에 대하여 다음과 같이 계산될 수 있다.

[0034] $$D(Q_jC_j)=\min\{D_{CIV}(Q_j,C_{i\ldots i+f-1,j}):0\le i\le g-f\}$$

[0035] 최저는 $C_{i\ldots i+f-1,j}=\{\tau_{i,j}:i^*\le i\le i^*+f\}$ 일때 발생하며, 여기서 i^*는 최소화 시간적 얼라인먼트 오프셋, $0\le i^*\le g-f$ 이다.

[0036] 복잡성-불변 거리 D_{CIV} 는 다음 식과 같이 계산될 수 있다.

[0037] $$D_{CIV}(Q_j, C_j) = \frac{\max\{K(Q_j), K(C_j)\}}{\min\{K(Q_j), K(C_j)\}} D_E(Q_j, C_j)$$

[0038] 여기서 D_E는 유클리드 거리이고, $K(Q_j)$는 히스토그램 빈 j에 대한 타임 시리즈 $Q_j=\{\theta_{i,j}:0\le i\le f\}$ 에

대한 복잡성의 척도(measure)이다. 예를 들면, $K(Q_j)$는

[0039] $$K(Q_j) = \sqrt{\sum_{i=0}^{f-2} (\theta_{i,j} - \theta_{i+1,j})^2}$$

[0040] 로 정의 될 수 있다. 유사하게, $K(C_j)$는 히스토그램 빈 j에 대한 대응하는 타임 시리즈 $C_j=\{\tau_{i,j}:0\leq i\leq g\}$ 에 대한 복잡도의 척도이며 유사한 표기법을 사용하여 정의될 수 있다.

[0041] 직관적으로, $K(Q_j)$는 시리즈의 도함수의 평균제곱근(RMS)을 측정하여, 더 큰 분산을 갖는 시리즈에 더 많은 가중을 부여한다. b 타임 시리즈 거리는 각 대응하는 쌍에 대하여 계산될 수 있다. 마침내, 대응하는 쌍에 대한 점수 △(Q,C)가 계산될 수 있다. 점수 △(Q,C)는 특정 임계값 d와 거리의 평균을 넘는 타임 시리즈 거리의 수를 포함하는 튜플(tuple)이다. 예를 들면,

[0042] $$\text{distance} = \{D(Q_j, C_j):0 \leq j < b \text{ and } D(Q_j, C_j) > d\}$$ 에 대하여

[0043] $$\Delta(Q, C) = \left(|\text{distance}|, \frac{\sum \text{distance}}{|\text{distance}|}\right)$$ 이다.

[0044] 방법은 경험적으로 결정될 수 있는 *d* 에 지나치게 민감하지 않다. 대응하는 쌍에 대한 점수 △는 |distance| (내림차순)와 평균 거리(오름차순)에 의하여 랭킹될 수 있다. 매칭 비디오들은 평균 거리 0을 갖는 b 매칭 타임 시리즈를 가질 것이다.

[0045] 시간적인 와핑(warping) 없는 상이한 길이의 두 개의 타임 시리즈를 비교할 때, 타임 시리즈는 정렬되어야 한다. 이것은 선형으로 될 수 있지만, 선형 기법은 느리고 불충분하다. 좀 더 효율적인 비교를 위하여, 주 경사(major inclines) 매칭 프로세스가 두 개의 시간 시리즈 간의 시간적 오프셋을 빠르게 계산하도록 사용되어 수신한 비디오 지문과 새로운 비디오 지문을 동기화할 수 있다. 주 경사 매칭 기법은 각 타임 시리즈에 대하여 선형 세그멘테이션을 사용하여 히스토그램의 시간적 자취의 근사치를 산출한 다음, 더 긴 거리나 더 깊은 높이를 갖는 주 경사를 선형 세그먼트로부터 추출한다. 두 개의 주 경사는, 만일 이들이 유사한 길이와 높이를 갖는다면 유사하다. 두 개의 주 경사의 유사도는 비교되는 히스토그램 간의 잠재적인 얼라인먼트를 나타낸다. 잠재적인 얼라인먼트 위치에 기초하여, 비교 비디오 지문 간의 복잡성-불변 유사도 거리가 산출될 수 있다. 만일 유사도 거리가 미리 결정된 임계값보다 작다면, (또한, 디지털 서명도 매치한다면) 두 개의 비디오 지문은 복잡성-불변 매치로 간주되어 비디오 콘텐츠가 인증된다. 만일 유사도 거리가 미리 결정된 임계값보다 작지 않다면, 수신한 비디오 콘텐츠는 진본이 아닌 것으로 간주된다.

[0046] 좀더 상세하게, 주 경사 매칭 기법은 선형 세그멘테이션 단계를 적용하는데, 이는 타임 시리즈를 선형 세그먼트의 시퀀스로 압축함으로써 타임 시리즈에 대한 근사치를 산출하는 상향(bottom-up) 세그멘테이션 알고리즘을 사용할 수 있다. 상향 세그멘테이션 알고리즘에 대한 추가적인 정보는, 그 내용이 전체적으로 본 출원에서 참조문헌으로 인용되는, Keogh et al., An Online Algorithm for Segmenting Time Series, Procedings of IEEEE International Conference on Data Mining, Nov. 29 - Dec. 2, 2001, pp 289-296를 참조하라.

[0047] 각 세그먼트는 상호 비교될 수 있다. 상술한 것처럼, 두 개의 선형 세그먼트는 더 짧은 것을 더 긴 것에 대하여 슬라이딩하고 이들 사이의 복잡성-불변 거리를 계산함으로써, 비교될 수 있다. 그러나, 얼라인먼트는 진폭에 대해서 "더 높고" 그리고/또는 타임에 대해서 "더 긴" 선형 세그먼트를 선택함으로써 축소되거나 단순화될 수 있다. 선택된 세그먼트는 주 경사로 불릴 수 있다. 주 경사 매칭 프로세스의 예가 도 3 내지 도 5에 도시된다.

[0048] 좀 더 상세하게, 주 경사를 발견하는 단계는 선형 세그먼트의 시퀀스를 길이 ρ의 동일한 인터벌로 시간에 따라 분할하는 단계를 포함한다. 만일 시작 시간점이 인터벌 내에 있다면 선형 세그먼트는 인터벌 내로 고려된다. 각 인터벌로부터, z 선형 세그먼트는 가장 큰 높이와 주어진 임계 길이*(1)*를 넘는 길이를 갖도록 선택된다. 상이한 길이의 비디오에서, 더 짧은 비디오의 주 경사는 더 긴 비디오에 의해 버려질 것이다. 따라서, 더 짧은 비디오에 적합한 길이 ρ를 선택하는 것이 좋다.

[0049] 일단, 주 경사들이 계산되면, 이들은 쌍으로 비교된다. 만일 이들이 유사한 길이와 높이(과도하게 제한적이지 않는 한, 정확한 거리 척도가 결정적인 것은 아니다)를 갖는다면, 두 개의 주 경사가 유사하다고 간주 된다. 두 개의 주 경사의 유사도는 비교되는 타임 시리즈의 가능한 얼라인먼트 위치, i^*를 나타낸다. 복잡성-불변 거리는 이들의 얼라인먼트 위치에 따라 계산된다. 전체적인 비교 시간은 계산이 이들의 위치에 한정되기 때문에 감소된다.

[0050] 도 1과 도 6을 참조하면, 송신기와 수신기 측에서 수행되는 비디오 지문 추출의 표본 실시예는 동일한 비디오 지문 채취 알고리즘을 활용한다. 직관적으로, 각 측에서 비디오 지문은 비디오의 가장 돌출된 특징의 모션 궤적을 시간에 걸쳐서 캡처하려고 한다. 이것은 광 흐름 방향 히스토그램(histograms of orientations of optical flow (HOOF)) 알고리즘을 사용하여 특징을 추출함으로써 수행된다. HOOF 알고리즘에 대한 추가적인 정보는, 전체적으로 그 내용이 본 출원에서 참조문헌으로 인용되는, Chaudhry et al., Histograms of Oriented Optical/Flow and Binet-Cauchy Kernals on Nonlinear Dynamical Systems for the Recognition of Human Actions, IEEE Conference on Computer Vision and Pattern Recognition, 2009, pp. 1932-1939를 참조하라.

[0051] 도 7을 참조하면, 비디오 지문 채취 알고리즘의 표본 실시예는 비디오 콘텐츠 Q를 f개의 단일하게 샘플링된 프레임 $Q = \{q_0, q_1, \ldots, q_{f-1}\}$의 시퀀스로서 표현되는 입력으로서 받아들인다. 광 흐름의 방향 히스토그램은 각 연속되는 프레임 쌍 q_i, q_{i+1} 에 대하여 생성될 수 있다. 프레임 q_i 내의 돌출 국소 특징(즉, 키 포인트)은, FAST 같은, 특징 검출기 알고리즘을 사용하여 검출될 수 있다. 프레임 q_i로부터 q_{i+1}로의 키 포인트의 광 흐름은 루카스-카나데(Lucas-Kande) 알고리즘을 적용하여 계산될 수 있다. 실질적인 범위 내의 크기를 갖는 궤적이 유지될 수 있다. 동일한 가중치로 유지되는 궤적의 방향은 b 빈들로 비닝되고(binning), 히스토그램은 정규화될 것이다. 예를 들면, 8 개의 빈이 선택되어, b = 8 빈이 될 것이다. 동일한 가중치로 비닝하는 것은 크기에 의한 가중에 비해서 좀 더 강건한 비디오 지문을 생산하는데, 이는 잘못 계산되는 궤적이 (좀더 많은) 정확한 궤적에 의해서 약화되기 때문이다.

[0052] 각 연속 프레임 쌍$\{q_i, q_{i+1}\}$에 대하여, 히스토그램 : $\{\Theta_{ij}: 0 \le j < b\}$이 존재하며, 여기서 Θ_{ij}는 주어진 방향으로 이동하는 키 포인트의 수를 기록한다. 검출된 키 포인트, 그들의 광 흐름 및 광 흐름의 방향 히스토그램를 갖는 프레임의 예가 도 2에 주어진다. 빈은 시간에 걸쳐 집계되어 b 타임 시리즈를 포함하는 (각 방향 빈에 대하여 하나의) 최종 비디오 지문을 생성한다.

[0053] $$\{\{\theta i,j: 0 \le i < f\}: \theta i,j: 0 \le j < b\}$$

[0054] 매칭은 지문 생성에 비하면 계산적으로 비싸지 않은 것으로 여겨지며, 이는, 앞서 설명한, 송신기 측으로부터 수신한 비디오 지문을 수신기 측에서 생성된 비디오 지문과 비교하는 기술 덕분이다.

[0055] 국소 특징 검출기는 추가적인 계산 비용에도 불구하고 단일하게 샘플링된 점들 대신에 국소 특징을 추적하도록 선택될 수 있는데, 이는 1) 결과적인 광 흐름이 좀더 신뢰할만하고, 2) 비디오 내의 각 프레임의 가장 돌출된 특징의 모션이 가장 결정적인 부분이라는 직관에 일치하기 때문이다.

[0056] 스케일-불변 특징 변환(SIFT) 알고리즘, 가속된 로버스트 특징(SURF) 알고리즘 및 FAST를 포함하여, 다양한 현존하는 국소 특징 검출기 알고리즘이 비교되었다. SIFT 알고리즘에 대한 추가적인 정보는, 그 내용이 전체적으로 본 출원에서 참조문서로서 인용되는, Lowe, Distinctive Image Features from Scale-Invariant Keypoints, International Journal of Computer Vision, Vol. 60, Issue 2, November, 2004, pp. 91-110을 참조하라. SURF 알고리즘에 대한 추가적인 정보는, 그 내용이 전체적으로 본 출원에서 참조문서로서 인용되는, Speeded Up Robust Features, Computer Vision and Image Understanding, Vol. 110, Issue 3, June, 2008, pp. 346-359를 참조하라.

[0057] FAST는 (직접적인 픽셀 비교를 통해 컴퓨팅되므로) 훨씬 더 빠르게 수행되고 더 많은 키 포인트를 생성하기 때문에 SIFT와 SURF에 우선하여 선택되었다. 추가적인 키 포인트는 부정확한 키 포인트 트래킹의 효과를 약화시키기 때문에 유리하다. 비록 FAST는 덜 강건하지만, 그럼에도 불구 하고 프레임에서 프레임으로의 미미한 변화를 추적하기에 충분하다.

[0058] 본 출원에서 설명되는 다양한 방법과 장치는 효율적인 실시간 비디오 인증을 가능하게 하는 강건한 컴팩트 비디오 지문 기술을 제공함으로써 감시 비디오와 다른 타입의 비디오 콘텐츠의 콘텐츠 변경과 인간이 개입된 공격에 대하여 방어한다. 감시 비디오는, 예를 들면, 공공의 안전과 가정 보안에 있어서 더 크고 중요한 역할을 수행한

다. 이는 특히 공공의 안전과 최초의 응답자 통신을 위해 사용될 수 있는 LTE 모바일 비디오의 보안에 시기 적절하고 적합하다. 본 출원에서 설명되는 방법은 또한 법률 집행이나 범죄인 기소에 대한 증거로서 사용될 수 있는 기록 비디오를 인증하도록 사용될 수 있다. 비디오 지문 추출 기법은 포맷 및 코덱-모듈을 준용한다.

[0059] 예를 들면, 속도와 정밀도와 관련하여 여기 설명되는 방법의 강건함과 효력을 입증하기 위하여, 공중에게 가용한 비디오 데이터베이스인, MUSLE VCD 벤치마크가 성능 비교 분석을 수행하기 위하여 사용되었다. 데이터베이스는 총 80 시간의 길이를 갖는 101 개의 비디오로 구성된다. 이 데이터베이스는, 스포츠 프로그램, 다큐멘터리, 만화 영화, 홈 비디오, 옛 흑백영화, 광고 등과 같은, 다양한 프로그램의 비디오를 제공한다. MUSCLE VCD 벤치마크는 일련의 지상 검증 자료(ground truth data) ST1을 포함하는데, 이는 통합하여 2시간 30분의 지속시간을 갖는 15개의 쿼리를 포함한다. 그들은 5분에서 1시간 길이의 비디오 카피이다. 쿼리 비디오는 크기 변경, 재-인코딩, 앵글 녹화, 컬러 특징의 크로핑과 변경, 확대 및 축소, 노이즈의 추가, 블러링 및 자막의 변경 등을 포함하는, 과도한 변형을 겪었다. 모든 쿼리 비디오에 대한 서명을 생성하고, 데이터베이스에서 이들을 검색하기에 필요한 시간을 포함하여, 총 쿼리 시간이 측정된다. 테스트 기계는 16G 램의 2.26GHz에서 수행되는 인텔 제온 쿼드-코어 프로세서이다. 도 8을 참조하면, 프로세스가 고도로 정확하게 ST1 내의 모든 쿼리를 검색하는 데에 10분 미만을 사용한다는 것을 보여준다. 증명 팀이 획득한 최고 점수를 위한 시간은 44분이 소요되었다. 비디오 콘텐츠 인증에 대하여, 돌출 특징점의 이동 궤적에 기초한 비디오 지문을 사용하여 주 경사 얼라인먼트에 따라 비디오 지문을 매칭하는 것은 여기 설명되는 방법을 사용하면 실행가능하며 실용적이다.

[0060] 본 출원에서 설명되는 다양한 방법과 장치는 비디오 감시 시스템을 위한 비디오 콘텐츠 인증을 제공하도록 구현될 수 있다. 본 출원에서 설명되는 비디오 인증 프로세스는 비디오 지문을 계산하는 어떤 알고리즘과도 결합하여 사용될 수 있다. 이것은 프로세스가 프로세스의 다양한 단계를 위하여 구현될 수 있는 다양한 알고리즘과 관련하여 얼마나 강건한지를 증명한다. 프로세스는 또한 현존하는 비디오 인증 기술과 관련된 비디오 콘텐츠 인증을 위하여 컴팩트 비디오 지문을 제공한다.

[0061] 비디오 콘텐츠를 인증하는 프로세스의 다른 표본 실시예가, 감시에 사용되어 적용가능한 방법을 설명하기 위하여 비디오 지문의 정확성의 맥락에서 설명된다. 전반적인 프로세스는 미디어 인증 방법의 콘텐츠-기반의 카테고리에 속하지만, 이전의 방법보다 더 상위 레벨의 특징을 사용한다. 국소 돌출 특징은 샘플링된 프레임으로부터 비디오 콘텐츠 내에서 감지되어 이러한 특징의 모션의 궤적이 시간에 걸쳐서 모션 타임 시리즈로서 캡처된다. 모션은 압축 코딩(예를 들면, MPEC-4)으로부터 단기(2-프레임) 모션 벡터에 대해서 사용되었다. 더 상위 레벨 특징은 일반적으로 지나치게 높은 계산 부하를 야기하는 것으로 생각될 수 있지만, 그러나, 더 상위 레벨 특징은 이미 대역폭과 잘못된 경고의 에러율을 감소시키도록 사용되고 있다. (싱글 또는 2-프레임 방법보다) 좀 더 강건한 이러한 특징은 이미 계산되기 때문에, 인증을 위한 사용은 추가적인 계산 비용을 갖지 않는다. 샘플링된 프레임의 비디오 지문은 빈 값의 특정 수이며, 이는 국소 특징의 모션 궤적의 방향을 빈들로 비닝함으로써 획득된다. 예를 들면, 8 개의 빈들이 표본적인 구현에서 사용될 수 있다.

[0062] 인증 기법은 강건한 해시 대신에 해시-매칭을 위한 강건한 방법을 사용한다. 공식으로, 지문의 시퀀스는 다음식으로 표현되며,

[0063] $$F = \{\{f_{i,j} : 0 \le i < m\} : 0 \le j < B\}$$,

[0064] 여기서 F는 지문의 시퀀스이고, f는 샘플링된 프레임의 지문이고, m은 샘플링된 프레임 시퀀스의 길이이고, B는 빈의 총수이다. 각 프레임 지문은 디지털로 서명된다(해싱되고 개인키로 암호화된다). 이것은 비디오 왜곡에 강건하지는 않지만, 그러나 디지털 서명에 부가하여, 온전한(즉, 암호화되지 않은) 디지털 지문이 수신기로의 전송 내에 포함된다. 비디오 콘텐츠를 인증하기 위하여, 수신기는 공중 시드(seed)를 사용하여 비디오 지문을 해시하고, H_1'을 획득한다. 디지털 서명은 공개키를 사용하여 복호화된다. 결과 해시 H_2'는 H_1'과 비교된다. 수신한 비디오에 대한 비디오 지문은 F_1'을 획득하도록 계산된다. 계산된 비디오 지문 F_1'는 수신한 비디오 지문 F_2'와 비교된다. 만일 $H_1' = H_2'$이고 유사도 거리 $D(F_1', F_2') \le$ dist라면, 대응하는 비디오 콘텐츠 프레임이 인증되며, 여기서 dist는 거리 임계값이다.

[0065] 비디오 지문은 타임 시리즈로 표현되기 때문에, $D(F_1', F_2')$는 타임 시리즈들 간의 거리를 측정함으로써 산출될 수 있다. 스케일링, 트랜스코딩 및 패킷 손실 등으로 인한, 비디오 전송에서의 다양한 변경은 타임 시리즈 내의 다중 복잡성을 유발한다. (오프셋, 진폭 및 위상 스케일링 등에 의해 왜곡될 수 있는) 결과하는 타임 시리즈들은 빈번하게 상이한 양의 최고점과 최저점을 갖는다. 비디오 지문의 매칭에서의 다양한 복잡성을 저지하기 위하

여, 바티스트(Batista)의 복잡성-불변 거리 측정이 구현될 수 있다. 복잡성-불변 거리 측정은 두 개의 타임 시리즈 간의 복잡성 차이를 존재하는 거리 척도에 대한 교정 팩터로서 사용한다. 복잡성-불변 거리 D_{CIV}는 다음 식과 같이 계산될 수 있다.

[0066] $$D_{CIV}(F_{1j}, F_{2j}) = \frac{\max\{K(F_{1j}), K(F_{2j})\}}{\min\{K(F_{1j}), K(F_{2j})\}} D_E(F_{1j}, F_{2j})$$

[0067] $$K(F_j) = \sqrt{\sum_{i=0}^{m-2} (f_{i,j} - f_{i+1,j})^2}$$

[0068] 여기서 F_{1j}와 F_{2j}는 히스토그램 빈 j에 대한 두 개의 타임 시리즈이고, D_E는 유클리드 거리이고, $K(F_j)$는 타임 시리즈의 복잡성의 척도이다. 직관적으로 $K(F_j)$는 시리즈의 도함수의 RMS를 측정하여, 더 큰 분산을 갖는 시리즈에 더 많은 가중치를 준다.

[0069] 유사도 거리를 B 타임 시리즈에 대하여 획득한 후에, 비교된 지문 쌍에 대한 점수 $\triangle(F_1, F_2)$가 계산될 수 있다. 점수 $\triangle(F_1, F_2)$는 특정 임계값 dist를 넘는 타임 시리즈 거리들의 수와 그 거리들의 평균을 포함하는 튜플이다. 즉,

[0070] $D_{total} = \{D_{CIV}(F_{1j}, F_{2j}): 0 \le j < B, \text{ and } D_{CIV}(F_{1j}, F_{2j}) > dist\}$ 에 대해서

[0071] $$\Delta(F_1, F_2) = \left(|D_{total}|, \frac{\sum D_{total}}{|D_{total}|} \right)$$ 이다.

[0072] 방법은 경험적으로 결정될 수 있는 dist에 지나치게 민감하지 않다. 두 개의 동일한 비디오는 평균 거리 0으로 매칭된 모든 빈을 갖는다.

[0073] 도 9를 참조하면, 비디오 콘텐츠를 인증하는 프로세스(900)의 표본 실시예는 (902)에서 시작하며, 여기서 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠가 통신 네트워크 내의 수신 노드에서 전송 노드로부터 수신된다. 다음으로, 수신노드에서 프로세스는 디지털 서명이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여 보호되지 않은 비디오 지문을 검증한다(904). (906)에서, 프로세스는 수신 노드에서 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 보호되지 않은 비디오 콘텐츠를 검증한다. 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증되면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서 후속 사용을 위하여 인증된다.

[0074] 프로세스(900)의 다른 실시예에서, 디지털 서명이 수신 노드로의 전송을 위하여 보호되지 않은 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다. 본 실시예에서, 프로세스(900)는 또한 수신 노드에서 디지털 서명을 보호되지 않은 비디오 콘텐츠로부터 분리하는 단계를 포함한다.

[0075] 프로세스(900)의 또 다른 실시예에서, 보호되지 않은 비디오 지문이 수신 노드로의 전송을 위하여 보호되지 않은 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다. 본 실시예에서, 프로세스(900)는 또한 수신 노드에서 보호되지 않은 비디오 지문을 보호되지 않은 비디오 콘텐츠로부터 분리하는 단계를 포함한다.

[0076] 프로세스(900)의 또 다른 실시예에서, 만일 보호되지 않은 비디오 지문이 수신 노드에 의해 검증되지 않는다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서 후속 사용을 위하여 인증되지 않는다. 프로세스(900)의 또 다른 실시예에서, 만일 수신 노드에 의해, 보호되지 않은 비디오 지문은 검증되고 그리고 보호되지 않은 비디오 콘텐츠는 검증되지 않는다면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서의 후속 사용을 위하여 인증되지 않는다.

[0077] 프로세스(900)의 또 다른 실시예에서, 디지털 서명과 보호되지 않은 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드에서 수신된다. 프로세스(900)의 또 다른 실시예에서, 보호되지 않은 지문과

보호되지 않은 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드에서 수신된다.

[0078] 다양한 실시예에서, 보호되지 않은 비디오 지문은 최초의 비디오 지문의 수신 버전이다. 최초의 비디오 지문은, 전송 노드에 의한 최초의 비디오 지문의 전송에 앞서, 지문 채취 알고리즘을 사용하여 최초의 비디오 콘텐츠로부터 도출될 수 있다. 디지털 서명은, 전송 노드에 의한 디지털 서명의 전송에 앞서, 암호화 알고리즘과 개인키를 사용하여 최초의 해시값으로터 생성된다. 최초의 해시값은 최초의 해시값의 암호화에 앞서서 해싱 알고리즘을 사용하여 최초의 비디오 지문으로부터 도출될 수 있다. 보호되지 않은 비디오 콘텐츠는 최초의 비디오 콘텐츠의 수신 버전이다.

[0079] 도 9와 도 10을 참조하면, 비디오 콘텐츠를 인증하는 프로세스(1000)의 다른 표본 실시예는 도 9의 프로세스(900)를 보호되지 않은 비디오 지문을 검증하는 것(904)과 관련하여 확장된다. 본 실시예에서, 프로세스(1000)는 도 9의 (904)에서 (1002)로 진행되며, 여기서 디지털 서명이 복호 알고리즘과 공개키를 사용하여 수신 노드에서 복호되어 최초의 해시값과 관련된 복호 해시값을 획득한다. 다음으로, 보호되지 않은 비디오 지문은 해싱 알고리즘을 사용하여 수신 노드에서 처리되어 최초의 해시값과 관련된 새로운 해시값을 획득한다(1004). (1006)에서, 새로운 해시값은 수신 노드에서 복호 해시값에 비교되고, 만일 새로운 해시값이 복호 해시값과 매칭된다면, 보호되지 않은 비디오 지문이 검증된다. 본 실시예에서, 프로세스(1000)는 (1006) 이후에 (906)으로 복귀한다. 프로세스(1000)의 또 다른 실시예에서, 만일, 새로운 해시값이 복호 해시값에 매칭되지 않는다면, 보호되지 않은 비디오 지문은 검증되지 않는다.

[0080] 도 9 내지 도 11을 참조하면, 비디오 콘텐츠를 인증하는 프로세스(1100)의 다른 표본 실시예는, 해싱 알고리즘을 사용하는 것(1004)과 관련하여, 도 10의 프로세스(1000)를 확장한다. 본 실시예에서, 프로세스(1100)는 도 10의 (1004)에서 (1102)로 진행되고, 여기서 해싱 알고리즘이 보호되지 않은 비디오 지문을 표현하는 데이터의 정렬에 적용되어 새로운 해시값을 설정하는 체크섬 값을 결정한다. 본 실시예에서, 프로세스(1100)는 (1102)후에 (1006)으로 반환된다.

[0081] 도 9와 도 12를 참조하면, 비디오 콘텐츠를 인증하는 프로세스(1200)의 다른 표본 실시예는, 보호되지 않은 비디오 콘텐츠를 검증하는 것(906)과 관련하여, 도 9의 프로세스(900)를 확장한다. 본 실시예에서, 프로세스(1200)는 도 9의 (906)에서 (1202)로 진행되어, 새로운 비디오 지문이 지문 채취 알고리즘을 사용하여 보호되지 않은 비디오 콘텐츠를 처리함으로써 수신 노드에서 생성된다. 다음으로, 프로세스는 복잡성-불변 거리 측정 알고리즘을 사용하여 수신 노드에서 보호되지 않은 비디오 지문과 새로운 비디오 지문 간의 거리 메트릭을 결정한다(1204). (1206)에서, 거리 메트릭이 수신 노드에서 미리 결정된 임계값과 비교되고, 만일 거리 메트릭이 미리 결정된 임계값을 초과하지 않는다면 보호되지 않은 비디오 콘텐츠가 검증된다. 프로세스(1200)의 다른 실시예에서, 만일 거리 메트릭이 미리 결정된 임계값을 초과한다면, 보호되지 않은 비디오 콘텐츠는 검증되지 않는다.

[0082] 도 9, 도 12 및 도 13을 참조하면, 비디오 콘텐츠를 인증하는 프로세스(1300)의 다른 표본 실시예는, 지문 채취 알고리즘을 사용하는 것(1202)과 관련하여, 도 12의 프로세스(1200)를 확장한다. 본 실시예에서, 프로세스(1300)는 도 12의 (1202)에서 (1302)로 진행되어, 비디오 프레임의 샘플이 보호되지 않은 비디오 콘텐츠로부터 선택되고 연결된 시간 시퀀스로 정렬된다. 다음으로, 돌출 특징점이 각 샘플 비디오 프레임에서 검출된다(1304). (1306)에서, 광 흐름의 각도 방향이 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의 각 돌출점에 대해서 계산된다. 다음으로, 각 샘플 비디오 프레임의 돌출 특징점에 대한 각도 방향은 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈으로 분배된다(1308). (1310)에서, 각 샘플 비디오 프레임들에 대한 각 각도 레인지 내의 값들은 연결된 시간 시퀀스에 걸쳐 연결되어 각 각도 레인지 빈에 대한 히스토그램을 형성한다. 다음으로, 각도 레인지 빈들에 대한 일련의 히스토그램이 정규화되어, 새로운 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성한다(1312).

[0083] 다른 실시예에서, 새로운 비디오 지문을 설정하기 위하여 지문 채취 알고리즘을 사용하는 것과 관련하여, 프로세스(1300)는 또한 선형 세그멘테이션 알고리즘을 사용하여 각 모션 타임 시리즈를 압축하여 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하는 단계를 포함한다. 본 실시예에서, 주 경사는 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여 각 압축된 모션 타임 시리즈로부터 추출되어 추출된 주 경사에 의해 표현되는 새로운 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다.

[0084] 다시 도 9와 12를 참조하면, 프로세스(1200)의 다른 실시예에서, 최초의 비디오 지문, 보호되지 않은 비디오 지문 및 새로운 비디오 지문은 각각 대응하는 히스토그램을 선형 세그먼트의 시퀀스로 축소시키고 선형 세그먼트의 시퀀스로부터 주 경사를 추출함으로써 형성된 대응하는 일련의 모션 타임 시리즈를 포함한다. 본

실시예에서, 복잡성-불변 거리 측정 알고리즘을 사용하는 것과 관련하여, 프로세스(1200)는 보호되지 않은 비디오 지문의 각 모션 타임 시리즈를 새로운 비디오 지문의 대응하는 모션 타임 시리즈와 페어링하는 단계를 포함한다. 각 페어링된 모션 타임 시리즈는 대응하는 페어링된 모션 타임 시리즈 내의 유사한 주 경사의 식별에 적어도 부분적으로 기초하여 정렬된다. 각 정렬된 모션 타임 시리즈 간의 거리 척도는 복잡성-불변 거리 측정 알고리즘을 사용하여 결정된다.

[0085] 프로세스(1200)의 또 다른 실시예에서, 최초의 비디오 지문, 보호되지 않은 비디오 지문 및 새로운 비디오 지문은 각각 대응하는 히스토그램에 의해 형성된 대응하는 일련의 모션 타임 시리즈를 포함한다. 본 실시예에서, 복잡성-불변 거리 측정 알고리즘을 사용하는 것과 관련하여, 프로세스(1200)는 보호되지 않은 비디오 지문의 각 모션 타임 시리즈를 선형 세그멘테이션 알고리즘을 사용하여 압축하여, 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하는 단계를 포함한다. 주 경사는 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여 보호되지 않은 비디오 지문의 각 압축된 모션 타임 시리즈로부터 추출되어, 추출된 주 경사에 의해 표현되는 보호되지 않은 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다. 새로운 비디오 지문의 각 모션 타임 시리즈는 선형 세그멘테이션 알고리즘을 사용하여 압축되고 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환한다. 주 경사는 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여 새로운 비디오 지문의 각 압축된 모션 타임 시리즈로부터 추출되어, 추출된 주 경사에 의해 표현되는 새로운 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다. 보호되지 않은 비디오 지문의 각 모션 타임 시리즈는 새로운 비디오 지문의 대응하는 모션 타임 시리즈와 페어링된다. 각 페어링된 모션 타임 시리즈는 대응하는 페어링된 모션 타임 시리즈 내의 유사한 주 경사들의 식별에 적어도 부분적으로 기초하여 정렬된다. 각 정렬된 모션 타임 시리즈들 간의 거리는 복잡성-불변 거리 측정 알고리즘을 사용하여 결정된다.

[0086] 도 14를 참조하면, 비디오 콘텐츠를 인증하는 수신 노드(1400)의 일 표본 실시예는 입력 모듈(1402), 지문 검증 모듈(1404), 콘텐츠 검증 모듈(1406), 컨트롤러 모듈(1408)을 포함한다. 입력 모듈(1402)은 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠를 전송 노드(1410)로부터 통신 네트워크(1412)를 통해 수신하도록 구성된다. 전송 노드(1410)는 통신 네트워크(1412) 내의 네트워크 노드일 수 있고, 또는 통신 네트워크(1412)에 접속을 갖는 사용자나 컴퓨팅 장치일 수 있다. 통신 네트워크(1412)는 다양한 타입의 네트워크 아키텍처, 통신 프로토콜 및 적합하게 조합된 기술을 포함하는 하이브리드 통신 네트워크일 수 있다. 지문 검증 모듈(1404)은 디지털 서명이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여 보호되지 않은 비디오 지문을 검증하도록 구성된다. 콘텐츠 검증 모듈(1406)은 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 보호되지 않은 비디오 콘텐츠를 검증하도록 구성된다. 컨트롤러 모듈(1408)은 입력 모듈(1402), 지문 검증 모듈(1404) 및 콘텐츠 검증 모듈(1406)과 동작가능하게 통신하고, 또한 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증된다면, 보호되지 않은 비디오 콘텐츠가 후속 사용을 위해 인증되도록, 동작을 제어하도록 구성된다.

[0087] 수신 노드(1400)의 다른 실시예에서, 디지털 서명은 전송을 위하여 보호되지 않은 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 또는 뒤에 첨부된다. 본 실시예에서, 수신 노드(1400)는 입력 모듈(1402) 및 컨트롤러 모듈(1408)과 동작가능하게 통신하는 비디오 프로세싱 모듈을 포함한다. 비디오 프로세싱 모듈은 디지털 서명을 보호되지 않은 비디오 콘텐츠로부터 분리하도록 구성된다.

[0088] 수신 노드(1400)의 다른 실시예에서, 보호되지 않은 비디오 지문은 전송을 위하여 보호되지 않은 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 또는 뒤에 첨부된다. 본 실시예에서, 수신 노드(1400)는 또한 입력 모듈(1402) 및 컨트롤러 모듈(1408)과 동작가능하게 통신하는 비디오 프로세싱 모듈을 포함한다. 비디오 프로세싱 모듈은 보호되지 않은 비디오 지문을 보호되지 않은 비디오 콘텐츠로부터 분리하도록 구성된다.

[0089] 수신 노드(1400)의 또 다른 실시예에서, 만일 보호되지 않은 비디오 지문이 지문 검증 모듈(1404)에 의해 검증되지 않는다면, 컨트롤러 모듈(1408)은, 보호되지 않은 비디오 콘텐츠가 후속 사용을 위하여 인증되지 않도록, 하는 방식으로 구성된다. 수신 노드(1400)의 또 다른 실시예에서, 만일 보호되지 않은 비디오 지문은 지문 검증 모듈(1404)에 의해 검증되고, 그리고 보호되지 않은 비디오 콘텐츠는 콘텐츠 검증 모듈(1406)에 의해 검증되지 않는다면, 컨트롤러 모듈(1408)은 보호되지 않은 비디오 콘텐츠가 수신 노드에서의 후속 사용을 위하여 인증되지 않도록, 하는 방식으로 구성된다.

[0090] 수신 노드(1400)의 또 다른 실시예에서, 디지털 서명과 보호되지 않은 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 입력 모듈(1402)에 의해 수신된다. 수신 노드(1400)의 또 다른 실시예에서, 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 입력 모듈(1402)에 의해 수신된다.

[0091] 수신 노드(1400)의 다양한 실시예에서, 보호되지 않은 지문은 최초의 비디오 지문의 수신 버전이다. 최초의 비디오 지문은, 전송 노드(1410)에 의한 최초의 비디오 지문의 전송에 앞서, 지문 채취 알고리즘을 사용하여 최초의 비디오 콘텐츠로부터 도출될 수 있다. 디지털 서명은, 전송 노드(1410)에 의한 디지털 서명의 전송에 앞서, 암호화 알고리즘과 개인키를 사용하여 최초의 해시값으로터 생성된다. 최초의 해시값은 최초의 해시값의 암호화에 앞서서 해싱 알고리즘을 사용하여 최초의 비디오 지문으로부터 도출될 수 있다. 보호되지 않은 비디오 콘텐츠는 최초의 비디오 콘텐츠의 수신 버전이다.

[0092] 도 15를 참조하면, 지문 검증 모듈(1404)의 표본 실시예는, 컨트롤러 모듈(1408)과 연관하여 보호되지 않은 비디오 지문을 검증하기 위하여, 복호 서브모듈(1502), 해싱 서브모듈(1504), 비교기 서브모듈(1506) 및 프로세서 서브모듈(1508)을 포함한다. 복호 서브모듈(1502)은 디지털 서명을 복호 알고리즘과 공개키를 사용하여 복호하여 최초의 해시값과 관련된 복호 해시값을 획득하도록 구성된다. 해싱 서브모듈(1504)은 보호되지 않은 비디오 지문을 해싱 알고리즘을 사용하여 처리하여 최초의 해시값과 관련된 새로운 해시값을 획득하도록 구성된다. 비교기 서브모듈(1506)은 새로운 해시값을 복호 해시값과 비교하여, 만일 새로운 해시값이 복호 해시값과 매칭된다면, 보호되지 않은 비디오 지문이 검증되도록 하는 방식으로 구성된다. 프로세서 서브모듈(1508)은 복호 서브모듈(1502), 해싱 서브모듈(1504), 비교기 서브모듈(1506)과 동작가능하게 통신한다. 프로세서 서브모듈(1508)은 디지털 서명, 보호되지 않은 비디오 지문, 새로운 해시값 및 복호 해시값 중의 하나 이상을 복호하고, 처리하고, 비교하는 것과 관련된 동작을 제어하도록 구성된다. 지문 검증 모듈(1404)의 다른 표본 실시예에서, 만일, 새로운 해시값이 복호 해시값에 매칭되지 않는다면, 비교기 서브모듈(1506)은 보호되지 않은 비디오 지문이 검증되지 않도록 하는 방식으로 구성된다.

[0093] 지문 검증 모듈(1404)의 또 다른 표본 실시예에서, 해싱 알고리즘의 사용과 관련하여, 해싱 서브모듈(1502)은 보호되지 않은 비디오 지문을 표현하는 데이터의 정렬에 해싱 알고리즘을 적용하여 새로운 해시값을 설정하는 체크섬 값을 결정하도록 구성된다.

[0094] 도 16을 참조하면, 콘텐츠 검증 모듈(1406)의 표본 실시예는, 컨트롤러 모듈(1408)과 연관하여 보호되지 않은 비디오 지문을 검증하기 위하여, 지문 채취 서브모듈(1602), 측정 서브모듈(1604), 비교기 서브모듈(1606) 및 프로세서 서브모듈(1608)을 포함한다. 지문 채취 서브모듈(1602)은 지문 채취 알고리즘을 사용하여 보호되지 않은 비디오 콘텐츠를 처리함으로써 새로운 비디오 지문을 생성하도록 구성된다. 측정 서브모듈(1604)은 복잡성-불변 거리 측정 알고리즘을 사용하여 보호되지 않은 비디오 지문과 새로운 비디오 지문 간의 거리 메트릭을 결정하도록 구성된다. 비교기 서브모듈(1606)은, 만일 거리 메트릭이 미리 결정된 임계값을 초과하지 않는다면 보호되지 않은 비디오 콘텐츠가 검증되도록, 거리 메트릭을 미리 결정된 임계값과 비교하도록 구성된다. 프로세서 서브모듈(1608)은 지문 채취 서브모듈(1602), 측정 서브모듈(1604), 비교기 서브모듈(1606)과 동작가능하게 통신한다. 프로세서 서브모듈(1608)은 새로운 비디오 지문, 보호되지 않은 비디오 콘텐츠, 거리 메트릭, 보호되지 않은 비디오 지문 및 미리 결정된 임계값 중의 하나 이상을 생성하고, 결정하고, 비교하는 것과 관련된 동작을 제어하도록 구성된다. 콘텐츠 검증 모듈(1406)의 다른 실시예에서, 만일 거리 메트릭이 미리 결정된 임계값을 초과한다면, 비교기 서브모듈(1606)은 보호되지 않은 비디오 콘텐츠가 검증되지 않도록 하는 방식으로 구성된다.

[0095] 콘텐츠 검증 모듈(1406)의 또 다른 표본 실시예에서, 지문 채취 서브모듈(1602)은 비디오 프레임의 샘플을 보호되지 않은 비디오 콘텐츠로부터 선택하고, 샘플 비디오 프레임을 연결된 시간 시퀀스로 정렬하도록 구성된다. 지문 채취 서브모듈(1602)은 또한 각 샘플 비디오 프레임 내의 돌출 특징점을 검출하도록 구성된다. 지문 채취 서브모듈(1602)은 각 샘플 비디오 프레임 내의 각 돌출 특징점에 대한 광 흐름의 각도 방향을, 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여, 계산하도록 구성된다. 추가적으로 지문 채취 서브모듈(1602)은 각 샘플 비디오 프레임의 돌출 특징점에 대한 각도 방향을 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈으로 분배한다. 지문 채취 서브모듈(1602)은 또한 각 샘플 비디오 프레임들에 대한 각 각도 레인지 내의 값들을 연결된 시간 시퀀스에 걸쳐 연결하여 각 각도 레인지 빈에 대한 히스토그램을 형성한다. 지문 채취 서브모듈(1602)은 또한 각도 레인지 빈들에 대한 일련의 히스토그램을 정규화하여, 새로운 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성하도록 구성된다.

[0096] 콘텐츠 검증 모듈(1406)의 또 다른 실시예에서, 새로운 비디오 지문을 설정하기 위하여 지문 채취 알고리즘을 사용하는 것과 관련하여, 지문 채취 서브모듈(1602)은 선형 세그멘테이션 알고리즘을 사용하여 각 모션 타임 시리즈를 압축하여 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하도록 구성된다. 지문 채취 서브모듈(1602)은 또한 주 경사를, 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여, 각 압축된 모션 타임 시리즈로부터 추출하고, 추출된 주 경사에 의해 표현되는 새로운 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성하도록 구성된다.

[0097] 콘텐츠 검증 모듈(1406)의 또 다른 실시예에서, 최초의 비디오 지문, 보호되지 않은 비디오 지문 및 새로운 비디오 지문은 각각 대응하는 히스토그램을 선형 세그먼트의 시퀀스로 축소하고 선형 세그먼트의 시퀀스로부터 주 경사를 추출함으로써 형성된 대응하는 일련의 모션 타임 시리즈를 포함한다. 본 실시예에서, 복잡성-불변 거리 측정 알고리즘을 사용하는 것과 관련하여, 측정 서브모듈(1604)은 보호되지 않은 비디오 지문의 각 모션 타임 시리즈를 새로운 비디오 지문의 대응하는 모션 타임 시리즈와 페어링하도록 구성된다. 측정 서브모듈(1604)은 또한 각 페어링된 모션 타임 시리즈를 대응하는 페어링된 모션 타임 시리즈 내의 유사한 주 경사의 식별에 적어도 부분적으로 기초하여 정렬한다. 측정 서브모듈(1604)은 또한 각 정렬된 모션 타임 시리즈 간의 거리 척도를 복잡성-불변 거리 측정 알고리즘을 사용하여 결정하도록 구성된다.

[0098] 콘텐츠 검증 모듈(1406)의 또 다른 실시예에서, 최초의 비디오 지문, 보호되지 않은 비디오 지문 및 새로운 비디오 지문은 각각 대응하는 히스토그램에 의해 형성된 대응하는 일련의 모션 타임 시리즈를 포함한다. 본 실시예에서, 복잡성-불변 거리 측정 알고리즘의 사용과 관련하여, 측정 서브모듈(1604)은 보호되지 않은 비디오 지문의 각 모션 타임 시리즈를 선형 세그멘테이션 알고리즘을 사용하여 압축하여, 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하도록 구성된다. 측정 서브모듈(1604)은 또한 주 경사를, 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여, 보호되지 않은 비디오 지문의 각 압축된 모션 타임 시리즈로부터 추출하고, 추출된 주 경사에 의해 표현되는 보호되지 않은 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성하도록 구성된다. 측정 서브모듈(1604)은 또한 선형 세그멘테이션 알고리즘을 사용하여 새로운 비디오 지문의 각 모션 타임 시리즈를 압축하여, 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하도록 구성된다. 또한, 측정 서브모듈(1604)은 주 경사를, 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여, 새로운 비디오 지문의 각 압축된 모션 타임 시리즈로부터 추출하고, 추출된 주 경사에 의해 표현되는 새로운 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다. 측정 서브모듈(1604)은 또한 보호되지 않은 비디오 지문의 각 모션 타임 시리즈를 새로운 비디오 지문의 대응하는 모션 타임 시리즈와 페어링한다. 측정 서브모듈(1604)은 또한 각 페어링된 모션 타임 시리즈를 페어링된 모션 타임 시리즈 내의 유사한 주 경사들의 식별에 적어도 부분적으로 기초하여 정렬하도록 구성된다. 추가로, 측정 서브모듈(1604)은 각 정렬된 모션 타임 시리즈들 간의 거리 척도를 복잡성-불변 거리 측정 알고리즘을 사용하여 결정한다.

[0099] 도 17을 참조하면, 비디오 콘텐츠를 인증하는 프로세스(1700)의 다른 표본 실시예가 (1702)에서 시작하고, 여기서 비디오 콘텐츠가 소스 장치로부터 수신된다. 다음으로, 비디오 지문이 지문 채취 알고리즘을 사용하여 비디오 콘텐츠를 처리함으로써 생성된다(1704). (1706)에서, 비디오 지문은 최초의 해시값을 획득하기 위하여 해싱 알고리즘을 사용하여 처리된다. 다음으로, 최초의 해시값이 암호화 알고리즘과 개인키를 사용하여 암호화되고 최초의 해시값과 관련된 디지털 서명을 획득한다(1708). (1710)에서, 디지털 서명, 비디오 지문 및 비디오 콘텐츠는 전송 노드의 저장 장치 내에 적어도 일시적으로 저장된다. 다음으로, 디지털 서명, 비디오 지문 및 비디오 콘텐츠가 전송 노드로부터 하나 이상의 통신 세션 내의 일 통신 네트워크 내의 수신 노드로 전송된다(1712).

[0100] 다른 실시예에서, 해싱 알고리즘의 사용과 관련하여, 프로세스(1700)는 또한 해싱 알고리즘을 비디오 지문을 표현하는 데이터의 정렬에 적용하여, 최초의 해시값을 설정하는 체크섬 값을 결정하는 단계를 포함한다.

[0101] 프로세스(1700)의 또 다른 실시예에서, 수신 노드는, 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 전송 노드로부터 수신한 후에, 복호 해시값이 수신한 비디오 지문과 일치하는지 여부를 결정하여 수신한 비디오 지문을 검증할 수 있다. 본 실시예에서, 수신 노드는 또한 수신한 비디오 지문이 수신한 비디오 콘텐츠와 일치하는지 여부를 결정하여, 수신한 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 수신한 비디오 콘텐츠를 검증할 수 있다. 또 다른 실시예에서,만일 수신한 비디오 지문과 수신한 비디오 콘텐츠가 수신 노드에 의해 검증되면, 수신한 비디오 콘텐츠는 수신 노드에서 후속 사용을 위하여 인증된다. 또 다른 실시예에서, 만일 수신한 비디오 지문이 수신 노드에 의해 검증되지 않는다면, 수신한 비디오 콘텐츠는 수신 노드에서 후속 사용

을 위하여 인증되지 않는다. 또 다른 실시예에서, 만일 수신 노드에 의해, 수신한 비디오 지문은 검증되고 그리고 수신한 비디오 콘텐츠는 검증되지 않는다면, 수신한 비디오 콘텐츠는 수신 노드에서의 후속 사용을 위하여 인증되지 않는다.

[0102] 프로세스(1700)의 또 다른 실시예에서, 디지털 서명과 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드로 전송된다. 프로세스(1700)의 또 다른 실시예에서, 비디오 지문과 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드로 전송된다.

[0103] 프로세스(1700)의 다른 실시예에서, 디지털 서명은 수신 노드로의 전송을 위하여 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다. 프로세스(1700)의 또 다른 실시예에서, 비디오 지문은 수신 노드로의 전송을 위하여 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다.

[0104] 도 17과 도 18을 참조하면, 비디오를 인증하는 프로세스(1800)의 다른 표본 실시예는 도 17의 프로세스(1700)를 지문 채취 알고리즘의 사용(1704)과 관련하여 확장된다. 본 실시예에서, 프로세스(1800)는 도 17의 (1704)에서 (1802)로 진행되며, 여기서 비디오 프레임의 샘플이 비디오 콘텐츠로부터 선택되고 연결된 시간 시퀀스로 정렬된다. 다음으로, 돌출 특징점이 각 샘플 비디오 프레임에서 검출된다(1804). (1806)에서, 광 흐름의 각도 방향이 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의 각 돌출점에 대해서 계산된다. 다음으로, 각 샘플 비디오 프레임의 돌출 특징점에 대한 각도 방향이 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈으로 분배된다(1808). (1810)에서, 각 샘플 비디오 프레임들에 대한 각 각도 레인지 내의 값들은 연결된 시간 시퀀스에 걸쳐 연결되어 각 각도 레인지 빈에 대한 히스토그램을 형성한다. 다음으로, 각도 레인지 빈들에 대한 일련의 히스토그램이 정규화되어, 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성한다(1812). 본 실시예에서, 프로세스(1800)는 (1812) 이후에 (1706)으로 복귀한다.

[0105] 다른 실시예에서, 새로운 비디오 지문을 설정하기 위하여 지문 채취 알고리즘을 사용하는 것과 관련하여, 프로세스(1800)는 또한 선형 세그멘테이션 알고리즘을 사용하여 각 모션 타임 시리즈를 압축하고 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하는 단계를 포함한다. 본 실시예에서, 주 경사는 타임 특징과 진폭 특징 중 적어도 한 특징에 대하여 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여 각 압축된 모션 타임 시리즈로부터 추출되어, 추출된 주 경사에 의해 표현되는 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다.

[0106] 도 19를 참조하면, 비디오 콘텐츠를 인증하는 전송 노드(1900)의 일 실시예는 입력 모듈(1902), 지문 채취 모듈(1904), 해싱 모듈(1906), 암호화 모듈(1908), 저장 장치(1910), 출력 모듈(1912), 컨트롤러 모듈(1914)을 포함한다. 입력 모듈(1902)은 비디오 콘텐츠를 소스 장치(1916)로부터 수신하도록 구성된다. 지문 채취 모듈(1904)은 지문 채취 알고리즘을 사용하여 비디오 콘텐츠를 처리함으로써 비디오 지문을 생성하도록 구성된다. 해싱 모듈(1906)은 비디오 지문을 해싱 알고리즘을 사용하여 처리하여 최초의 해시값을 획득하도록 구성된다. 암호화 모듈(1908)은 암호화 알고리즘과 개인키를 사용하여 최초의 해시값을 암호화하여, 최초의 해시값과 관련된 디지털 서명을 획득하도록 구성된다. 저장 장치(1910)는 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 적어도 일시적으로 저장하도록 구성된다. 출력 모듈(1912)은 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 하나 이상의 통신 세션 내의 일 통신 네트워크(1920) 내의 수신 노드(1918)로 전송하도록 구성된다. 컨트롤러 모듈(1914)은 입력 모듈(1902), 지문 채취 모듈(1904), 해싱 모듈(1906), 암호화 모듈(1908), 저장 장치(1910), 출력 모듈(1912)과 동작가능하게 통신하고, 하나 이상의 비디오 콘텐츠, 비디오 지문 및 디지털 서명을 수신하고, 생성하고, 처리하고, 암호화하고, 저장하고 또한 전송하는 것과 연관된 동작을 제어하도록 구성된다.

[0107] 전송 노드(1900)는 통신 네트워크(1920) 내의 네트워크 노드일 수 있고, 또는 통신 네트워크(1920)에 접속을 갖는 사용자나 컴퓨팅 장치일 수 있다. 유사하게, 소스 장치(1916)는 통신 네트워크(1920) 내의 네트워크 노드일 수 있고, 또는 통신 네트워크(1920)에 접속을 갖는 사용자나 컴퓨팅 장치일 수 있다. 예를 들면, 소스 장치(1916)는 비디오 캡처 장치(예를 들면, 비디오 카메라)나, 비디오 저장 장치(예를 들면, 비디오 콘텐츠 서버)나, 또는 둘 다일 수 있다. 전송 노드(1900)와 소스 장치(1916)는 상이한 위치에 있거나, 상호 관련되거나(예를 들면, 보안 시스템), 또는 동일한 장치(예를 들면, 모바일 스테이션, 랩톱 컴퓨터, 등) 내에 결합될 수 있다.

[0108] 전송 노드(1900)의 다른 실시예에서, 해싱 알고리즘의 사용과 관련하여, 해싱 모듈(1906)은 해싱 알고리즘을 비디오 지문을 표현하는 데이터의 정렬에 적용하여 최초의 해시값을 설정하는 체크섬 값을 결정하도록 구성될 수 있다.

[0109] 전송 노드(1900)의 또 다른 실시예에서, 수신 노드(1918)는, 디지털 서명, 비디오 지문 및 비디오 콘텐츠를 전송 노드(1900)로부터 수신한 후에, 복호 해시값이 수신한 비디오 지문과 일치하는지 여부를 결정하여 수신한 비디오 지문을 검증할 수 있다. 본 실시예에서, 수신 노드(1918)는 또한 수신한 비디오 지문이 수신한 비디오 콘텐츠와 일치하는지 여부를 결정하여, 수신한 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 수신한 비디오 콘텐츠를 검증할 수 있다. 추가적인 실시예에서, 만일 수신한 비디오 지문과 수신한 비디오 콘텐츠가 수신 노드에 의해 검증되면, 수신한 비디오 콘텐츠는 수신 노드(1918)에서 후속 사용을 위하여 인증된다. 다른 추가적인 실시예에서, 만일 수신한 비디오 지문이 수신 노드에 의해 검증되지 않는다면, 수신한 비디오 콘텐츠는 수신 노드(1918)에서 후속 사용을 위하여 인증되지 않는다. 또 다른 추가적인 실시예에서, 만일 수신 노드에 의해, 수신한 비디오 지문은 검증되고 그리고 수신한 비디오 콘텐츠는 검증되지 않는다면, 수신한 비디오 콘텐츠는 수신 노드(1918)에서의 후속 사용을 위하여 인증되지 않는다.

[0110] 전송 노드(1900)의 또 다른 실시예에서, 디지털 서명과 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드로 전송된다. 전송 노드(1900)의 또 다른 실시예에서, 비디오 지문과 비디오 콘텐츠는 상이한 통신 경로를 통해 별도의 통신 세션 내의 수신 노드로 전송된다.

[0111] 전송 노드(1900)의 또 다른 실시예에서, 디지털 서명은 수신 노드로의 전송을 위하여 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다. 전송 노드(1900)의 또 다른 실시예에서, 비디오 지문은 수신 노드로의 전송을 위하여 비디오 콘텐츠와 함께 앞에 첨부되거나, 삽입되거나, 뒤에 첨부된다.

[0112] 전송 노드(1900)의 또 다른 실시예에서, 지문 채취 알고리즘의 사용과 관련하여, 지문 채취 모듈(1904)은 비디오 프레임의 샘플을 비디오 콘텐츠로부터 선택하여, 샘플 비디오 프레임을 연결된 시간 시퀀스로 정렬하도록 구성된다. 지문 채취 모듈(1904)은 또한 돌출 특징점을 각 샘플 비디오 프레임에서 검출한다. 지문 채취 모듈(1904)은 또한 각 샘플 비디오 프레임 내의 각 돌출 특징점에 대한 광 흐름의 각도 방향을 연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여 계산하도록 구성된다. 추가적으로, 지문 채취 모듈(1904)은 각 샘플 비디오 프레임의 돌출 특징점에 대한 각도 방향을 각 샘플 비디오 프레임에 대한 대응하는 각도 레인지 빈으로 분배한다. 지문 채취 모듈(1904)은 또한 각 샘플 비디오 프레임들에 대한 각 각도 레인지 내의 값들을 연결된 시간 시퀀스에 걸쳐 연결하여 각 각도 레인지 빈에 대한 히스토그램을 형성한다. 지문 채취 모듈(1904)은 또한 각도 레인지 빈들에 대한 일련의 히스토그램을 정규화하여, 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성하도록 구성된다.

[0113] 전송 노드(1900)의 추가적인 실시예에서, 새로운 비디오 지문을 설정하기 위하여 지문 채취 알고리즘을 사용하는 것과 관련하여, 지문 채취 모듈(1904)은 또한 선형 세그멘테이션 알고리즘을 사용하여 각 모션 타임 시리즈를 압축하여 대응하는 히스토그램을 선형 세그먼트의 대응하는 시퀀스로 변환하도록 구성된다. 본 실시예에서, 지문 채취 모듈(1904)은 또한 주 경사를, 타임 특징과 진폭 특징 중 적어도 한 특징에 대한 미리 결정된 임계값보다 더 큰 선형 세그먼트를 선택하는 것에 적어도 부분적으로 기초하여 각 압축된 모션 타임 시리즈로부터 추출하여, 추출된 주 경사에 의해 표현되는 비디오 지문에 대한 대응하는 일련의 모션 타임 시리즈를 형성한다.

[0114] 도 9 내지 도 16을 다시 참조하면, 비-일시적 컴퓨터-판독가능한 매체의 표본 실시예는, 제1 컴퓨터에서 수행될 때, 컴퓨터-제어되는 수신 노드(1400)가 비디오 콘텐츠를 인증하는 프로세스(예를 들면, 900, 1000, 1100, 1200, 1300)를 수행하도록 유발한다. 일 표본 실시예에서, 프로세스는, 디지털 서명, 보호되지 않은 비디오 지문 및 보호되지 않은 비디오 콘텐츠를 전송 노드로부터 통신 네트워크 내의 수신 노드에서 수신한 후에, 수신 노드에서, 복호 해시값이 보호되지 않은 비디오 지문과 일치하는지 여부를 결정하여 보호되지 않은 비디오 지문을 검증하는 단계를 포함한다. 프로세스는 또한, 수신 노드에서, 보호되지 않은 비디오 지문이 보호되지 않은 비디오 콘텐츠와 일치하는지 여부를 결정하여, 보호되지 않은 비디오 콘텐츠 내의 미리 결정된 손실 한도를 감내하는 방식으로 보호되지 않은 비디오 콘텐츠를 검증하는 단계를 포함한다. 만일 보호되지 않은 비디오 지문과 보호되지 않은 비디오 콘텐츠가 검증되면, 보호되지 않은 비디오 콘텐츠는 수신 노드에서의 후속 사용을 위하여 인증된다.

[0115] 다양한 추가적인 실시예에서, 비-일시적 컴퓨터-판독가능한 메모리에 저장되는 제1 명령은, 제1 컴퓨터에서 수행될 때, 컴퓨터-제어되는 수신 노드(1400)가 앞에서 설명한 비디오 콘텐츠를 인증하는 프로세스(900, 1100, 1200, 1300)와 연관된 기능의 다양한 조합을 수행하게 한다. 즉, 앞에서 설명한 다양한 특징은 비-일시적 컴퓨터-판독가능한 매체 내에 저장되는 제1 프로그램 명령에 의한 적합한 조합으로 구현될 수 있다. 앞서 설명된 수신 노드(1400)의 어느 적합한 모듈이나 서브모듈은 대응하는 프로그램 명령과 연관되는 대응하는 컴퓨터와 비-일시적 컴퓨터-판독가능한 매체를 포함할 수 있다. 대안으로, 대응하는 프로그램 명령과 연관되는 대응하는 컴

퓨터와 비-일시적 컴퓨터-판독가능한 매체는 개별적이거나 또는 컴포넌트로 결합되어, 앞에서 설명한 수신 노드(1400)의 모듈이나 서브모듈의 적합한 조합과 동작가능하게 통신할 수 있다.

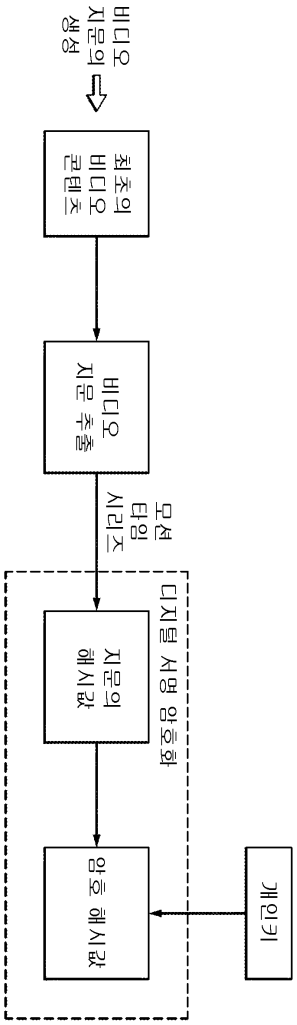
[0116] 도 17 내지 도 19를 다시 참조하면, 제2 명령을 저장하는 비-일시적 컴퓨터-판독가능한 매체의 표본 실시예는, 제2 컴퓨터에서 수행될 때, 컴퓨터-제어되는 전송 노드(1900)가 비디오 콘텐츠를 인증하는 프로세스(예를 들면, 1700, 1800)를 수행하도록 유발한다. 일 표본 실시예에서, 프로세스는, 비디오 콘텐츠를 소스 장치로부터 수신한 후에, 지문 알고리즘을 사용하여 비디오 콘텐츠를 처리함으로써 비디오 지문을 생성하는 단계를 포함한다. 비디오 지문은 해싱 알고리즘을 사용하여 처리되어 최초의 해시값을 획득한다. 최초의 해시값은 최초의 해시값과 관련된 디지털 서명을 획득하기 위하여 암호화 알고리즘과 개인키를 사용하여 암호화된다. 디지털 서명, 비디오 지문 및 비디오 콘텐츠는 전송 노드의 저장 장치 내에 적어도 일시적으로 저장된다. 디지털 서명, 비디오 지문 및 비디오 콘텐츠는 전송 노드로부터 하나 이상의 통신 세션에서 일 통신 네트워크 내의 수신 노드로 전송된다.

[0117] 다양한 추가적인 실시예에서, 비-일시적 컴퓨터-판독가능한 메모리에 저장되는 제1 명령은, 제1 컴퓨터에서 수행될 때, 컴퓨터-제어되는 전송 노드(1900)가 앞에서 설명한 비디오 콘텐츠를 인증하는 프로세스(1700, 1800)와 연관된 기능의 다양한 조합을 수행하게 한다. 즉, 앞에서 설명한 다양한 특징은 비-일시적 컴퓨터-판독가능한 매체 내에 저장되는 제1 프로그램 명령에 의한 적합한 조합으로 구현될 수 있다. 앞서 설명된 전송 노드(1900)의 어느 적합한 모듈은 대응하는 프로그램 명령과 연관되는 대응하는 컴퓨터와 비-일시적 컴퓨터-판독가능한 매체를 포함할 수 있다. 대안으로, 대응하는 프로그램 명령과 연관되는 대응하는 컴퓨터와 비-일시적 컴퓨터-판독가능한 매체는 개별적이거나 또는 컴포넌트로 결합되어, 앞에서 설명한 전송 노드(1900)의 모듈의 적합한 조합과 동작가능하게 통신할 수 있다.

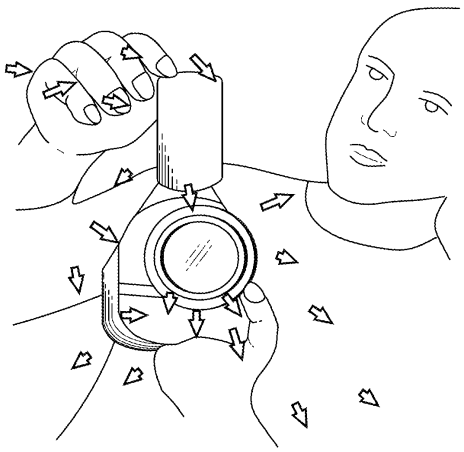
[0118] 앞의 설명은 단지 본 발명의 특정 실시예의 개시를 제공하는 것이고 이에 한정하기 위한 목적이 아니다. 따라서, 본 발명은 위에 설명한 실시예에 한정되지 않는다. 오히려, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명의 영역에 속하는 다른 실시예를 고안할 수 있음이 인정된다.

도면

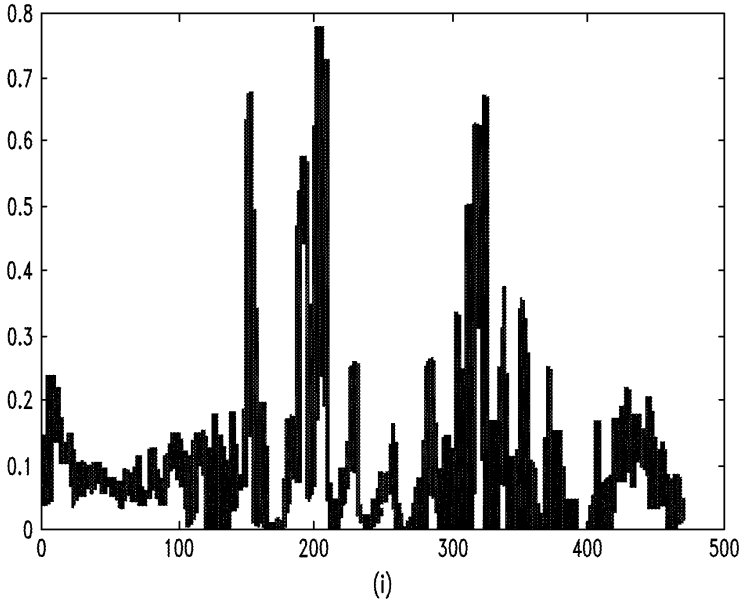
도면1


비디오 지문의 생성
최초의 비디오 콘텐츠
비디오 지문 추출
모션 타임 시리즈
디지털 서명 암호화
지문의 해시값
암호 해시값
개인키

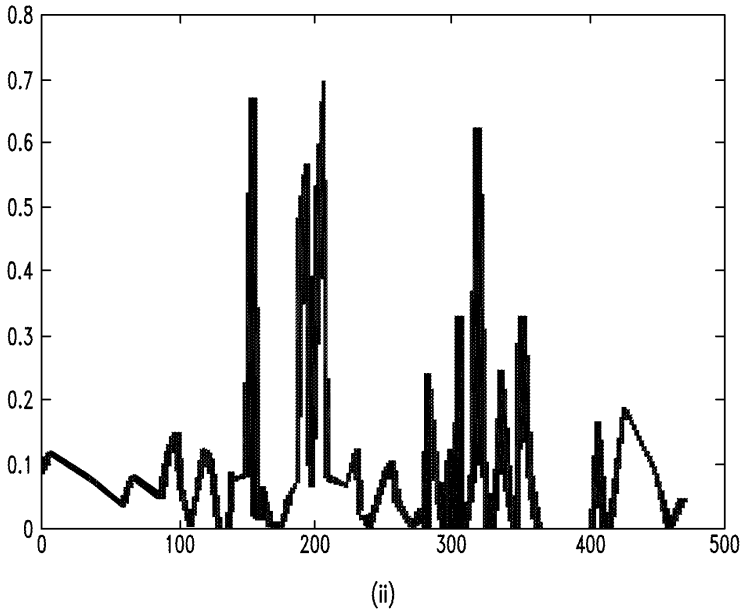
도면2



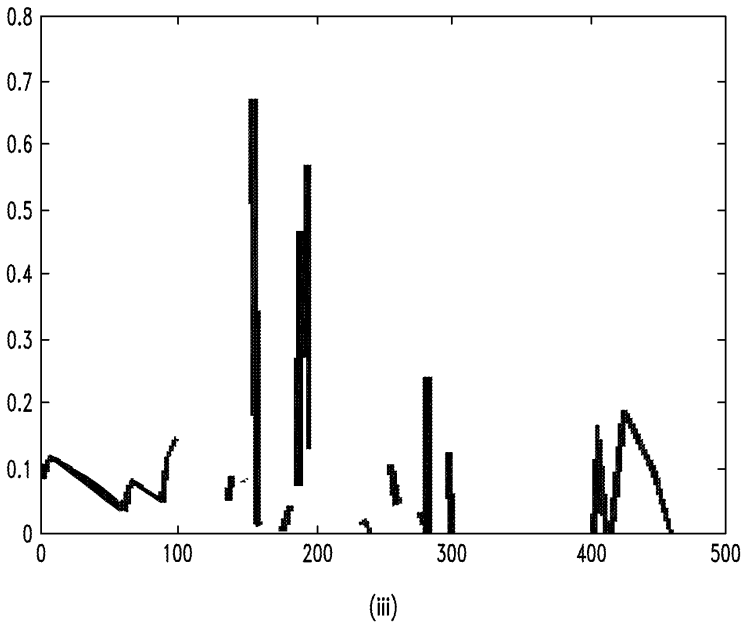
도면3


0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
100
200
300
400
500
(i)

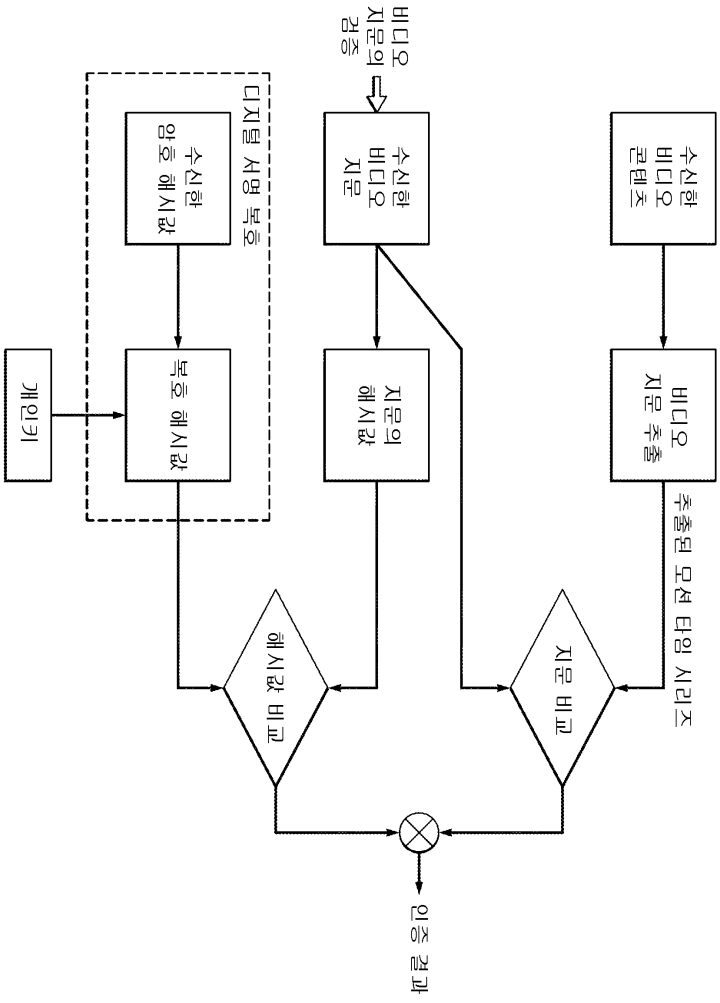
도면4


0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
100
200
300
400
500
(ii)

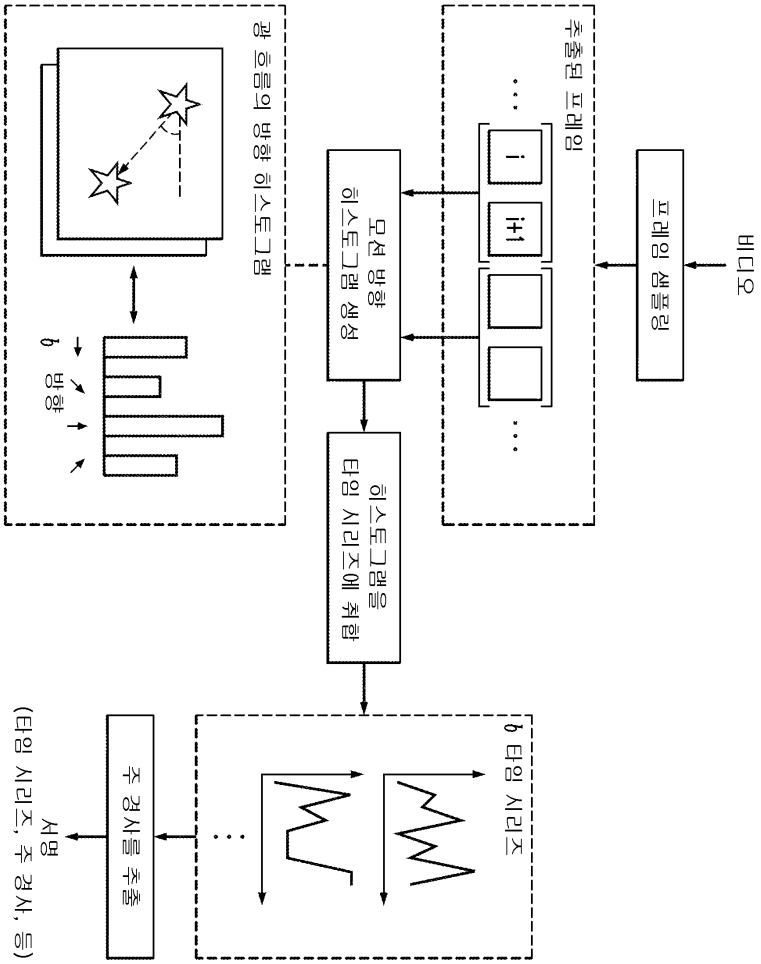
도면5


0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
100
200
300
400
500
(iii)

도면6


비디오 지문의 검출
디지털 서명 복호
수신한 암호 해시값
개인키
복호 해시값
수신한 비디오 지문
지문의 해시값
수신한 비디오 콘텐츠
비디오 지문 추출
추출된 모션 타임 시리즈
해시값 비교
지문 비교
인증 결과

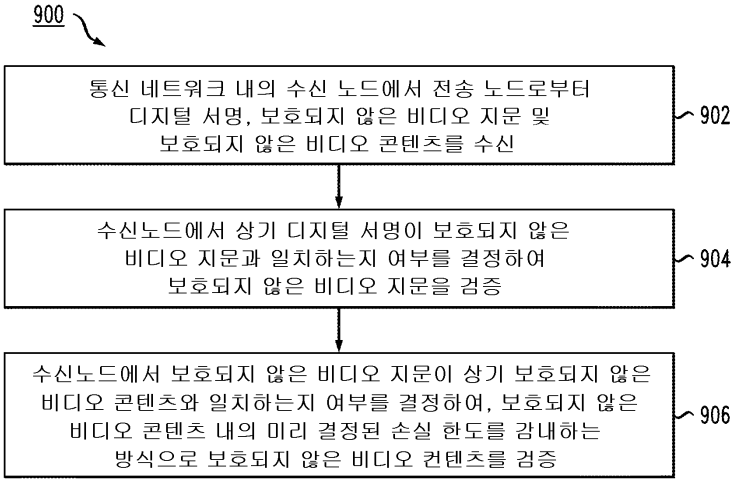
도면7



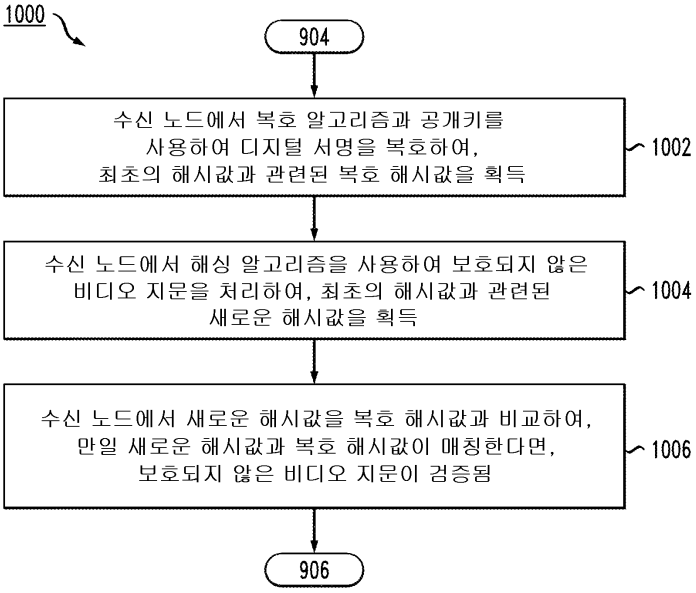
도면8

팀	정확도	질의 시간
ADVESTIGO	0.86	64 min
중국 과학원 - 1	0.46	41 min
중국 과학원 - 2	0.53	14 min
홍콩시티 대학교	0.66	45 min
IBM - 1	0.86	44 min
IBM - 2	0.73	68 min
IBM - 3	0.8	99 min
우리의 접근방법	1.0	<10 min

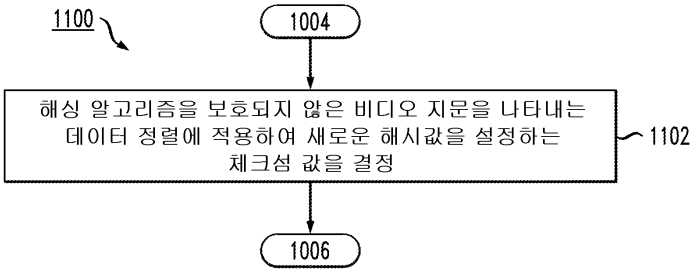
도면9



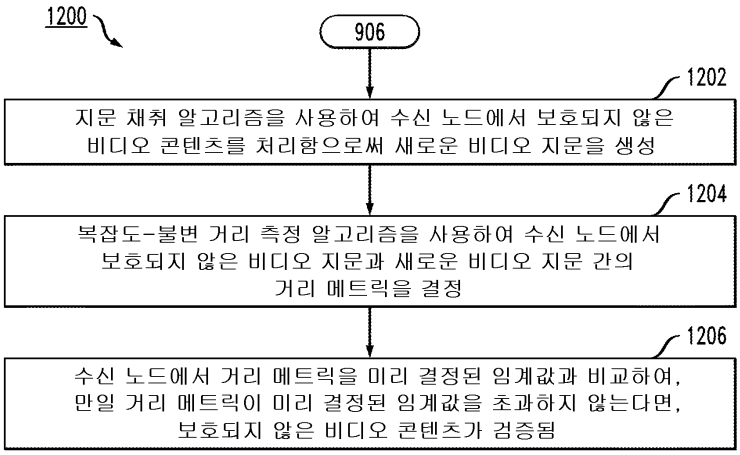
도면10



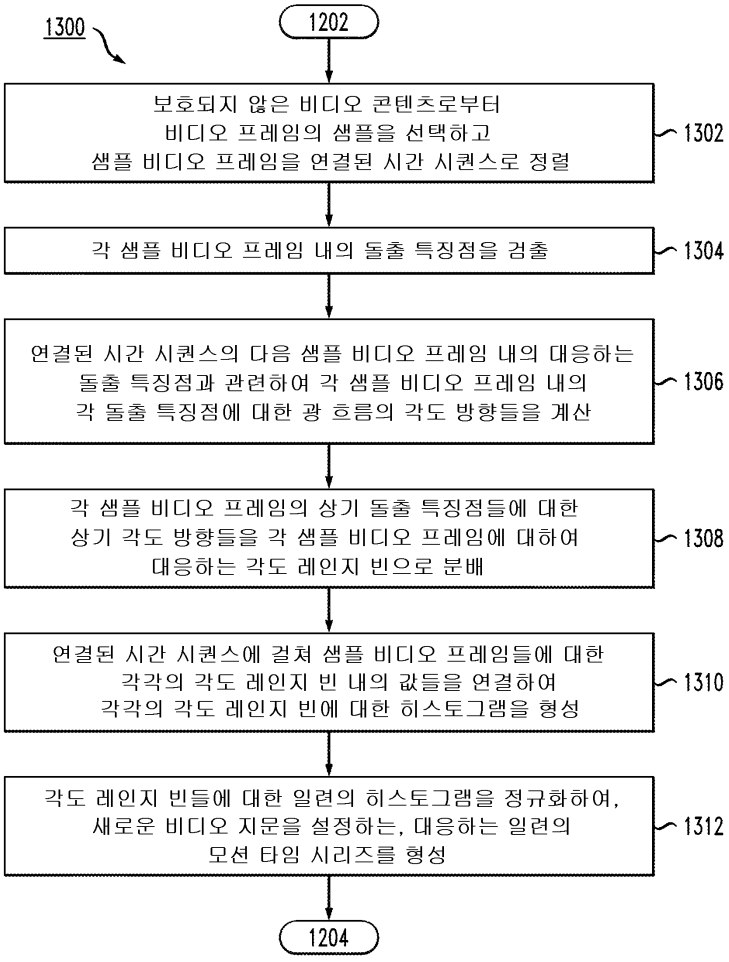
도면11



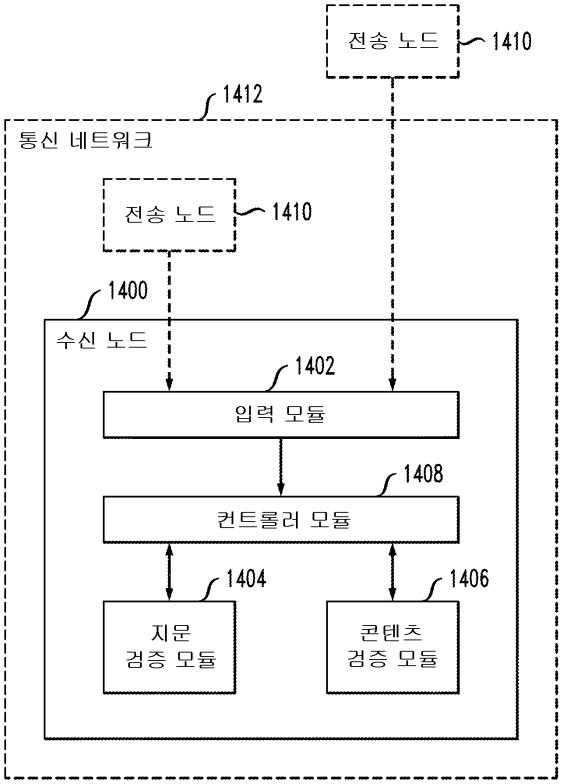
도면12


1200
906
1202
지문 채취 알고리즘을 사용하여 수신 노드에서 보호되지 않은 비디오 콘텐츠를 처리함으로써 새로운 비디오 지문을 생성
1204
복잡도-불변 거리 측정 알고리즘을 사용하여 수신 노드에서 보호되지 않은 비디오 지문과 새로운 비디오 지문 간의 거리 메트릭을 결정
1206
수신 노드에서 거리 메트릭을 미리 결정된 임계값과 비교하여, 만일 거리 메트릭이 미리 결정된 임계값을 초과하지 않는다면, 보호되지 않은 비디오 콘텐츠가 검증됨

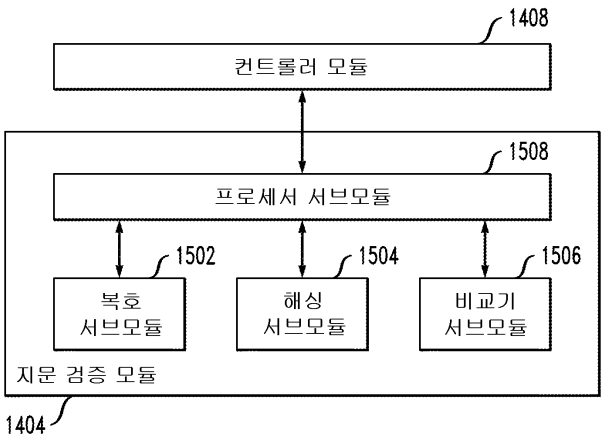
도면13


1300
1202
보호되지 않은 비디오 콘텐츠로부터 비디오 프레임의 샘플을 선택하고 샘플 비디오 프레임을 연결된 시간 시퀀스로 정렬
1302
각 샘플 비디오 프레임 내의 돌출 특징점을 검출
1304
연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는 돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의 각 돌출 특징점에 대한 광 흐름의 각도 방향들을 계산
1306
각 샘플 비디오 프레임의 상기 돌출 특징점들에 대한 상기 각도 방향들을 각 샘플 비디오 프레임에 대하여 대응하는 각도 레인지 빈으로 분배
1308
연결된 시간 시퀀스에 걸쳐 샘플 비디오 프레임들에 대한 각각의 각도 레인지 빈 내의 값들을 연결하여 각각의 각도 레인지 빈에 대한 히스토그램을 형성
1310
각도 레인지 빈들에 대한 일련의 히스토그램을 정규화하여, 새로운 비디오 지문을 설정하는, 대응하는 일련의 모션 타임 시리즈를 형성
1312
1204

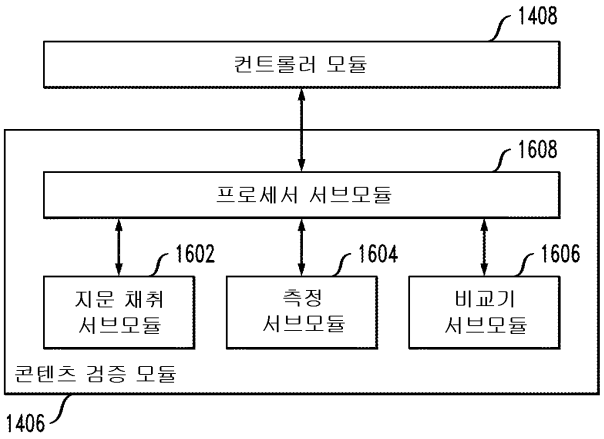
도면14


전송 노드
1410
1412
통신 네트워크
전송 노드
1410
1400
수신 노드
1402
입력 모듈
1408
컨트롤러 모듈
1404
1406
지문
검증 모듈
콘텐츠
검증 모듈

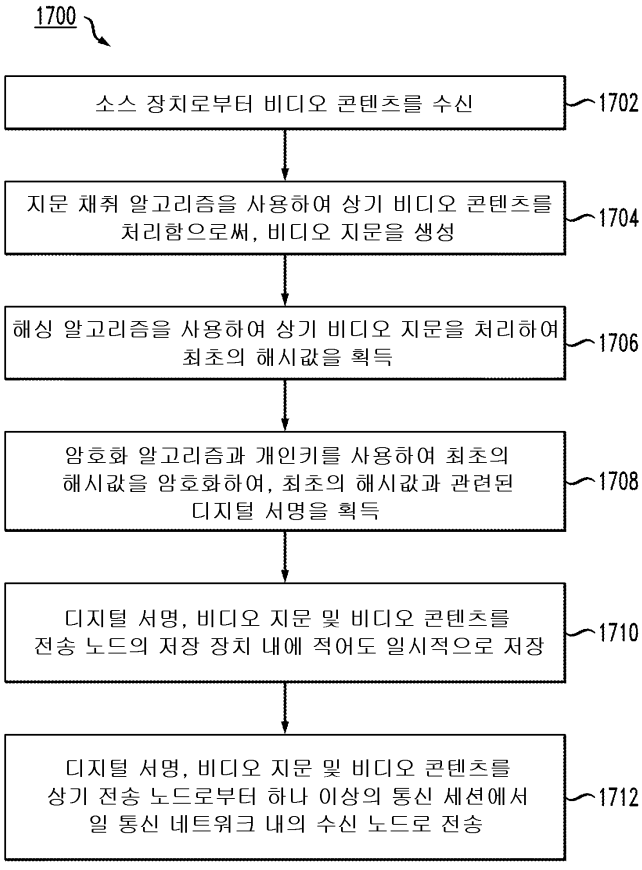
도면15


1408
컨트롤러 모듈
1508
프로세서 서브모듈
1502
1504
1506
복호
서브모듈
해싱
서브모듈
비교기
서브모듈
지문 검증 모듈
1404

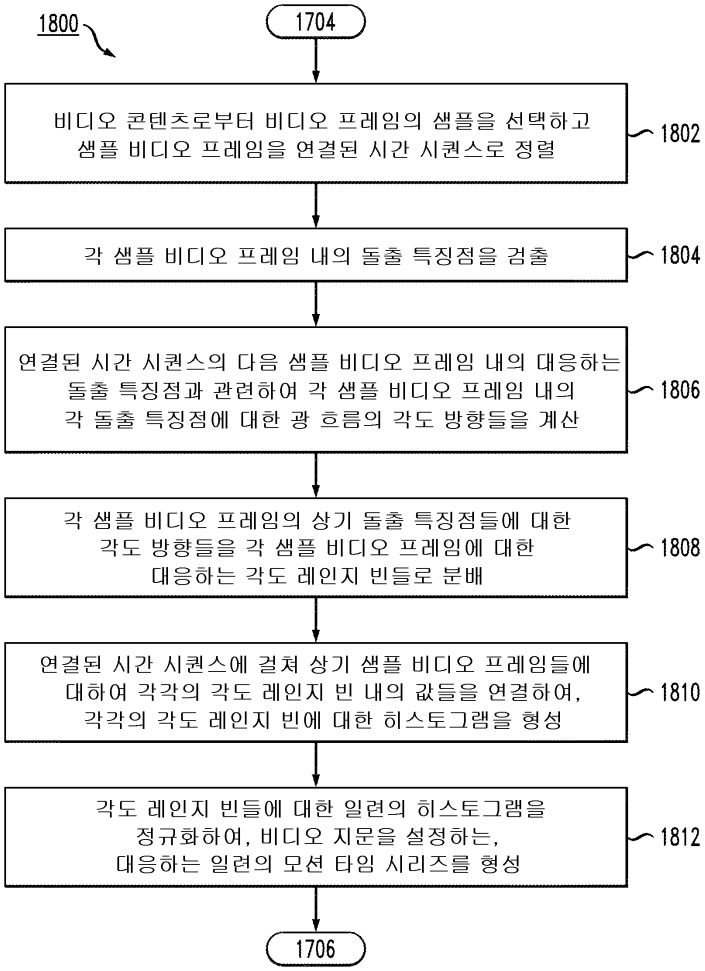
도면16


1408
컨트롤러 모듈
1608
프로세서 서브모듈
1602
1604
1606
지문 채취 서브모듈
측정 서브모듈
비교기 서브모듈
콘텐츠 검증 모듈
1406

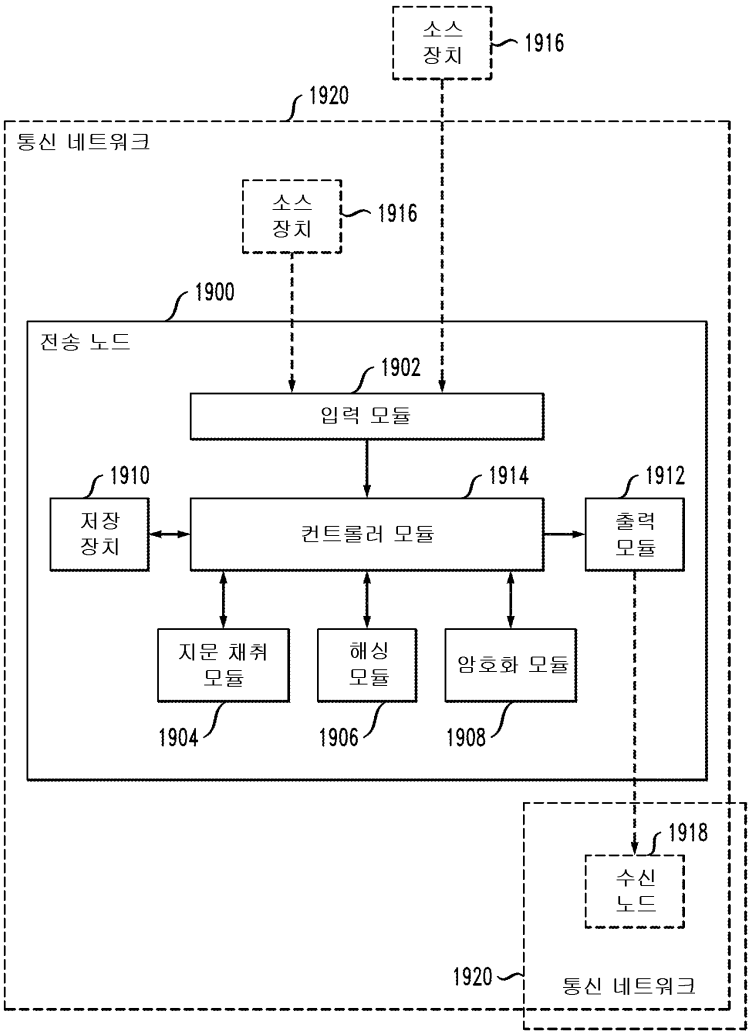
도면17


1700
소스 장치로부터 비디오 콘텐츠를 수신
1702
지문 채취 알고리즘을 사용하여 상기 비디오 콘텐츠를 처리함으로써, 비디오 지문을 생성
1704
해싱 알고리즘을 사용하여 상기 비디오 지문을 처리하여 최초의 해시값을 획득
1706
암호화 알고리즘과 개인키를 사용하여 최초의 해시값을 암호화하여, 최초의 해시값과 관련된 디지털 서명을 획득
1708
디지털 서명, 비디오 지문 및 비디오 콘텐츠를 전송 노드의 저장 장치 내에 적어도 일시적으로 저장
1710
디지털 서명, 비디오 지문 및 비디오 콘텐츠를 상기 전송 노드로부터 하나 이상의 통신 세션에서 일 통신 네트워크 내의 수신 노드로 전송
1712

도면18


1800
1704
비디오 콘텐츠로부터 비디오 프레임의 샘플을 선택하고
샘플 비디오 프레임을 연결된 시간 시퀀스로 정렬
1802
각 샘플 비디오 프레임 내의 돌출 특징점을 검출
1804
연결된 시간 시퀀스의 다음 샘플 비디오 프레임 내의 대응하는
돌출 특징점과 관련하여 각 샘플 비디오 프레임 내의
각 돌출 특징점에 대한 광 흐름의 각도 방향들을 계산
1806
각 샘플 비디오 프레임의 상기 돌출 특징점들에 대한
각도 방향들을 각 샘플 비디오 프레임에 대한
대응하는 각도 레인지 빈들로 분배
1808
연결된 시간 시퀀스에 걸쳐 상기 샘플 비디오 프레임들에
대하여 각각의 각도 레인지 빈 내의 값들을 연결하여,
각각의 각도 레인지 빈에 대한 히스토그램을 형성
1810
각도 레인지 빈들에 대한 일련의 히스토그램을
정규화하여, 비디오 지문을 설정하는,
대응하는 일련의 모션 타임 시리즈를 형성
1812
1706

도면19


소스 장치
1916
1920
통신 네트워크
소스 장치
1916
1900
전송 노드
1902
입력 모듈
1910
저장 장치
1914
컨트롤러 모듈
1912
출력 모듈
지문 채취 모듈
해싱 모듈
암호화 모듈
1904
1906
1908
1918
수신 노드
1920
통신 네트워크