(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년12월05일
(11) 등록번호 10-1925463
(24) 등록일자 2018년11월29일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 17/30* (2006.01)
(52) CPC특허분류
G06F 21/6218 (2013.01)
G06F 17/30097 (2013.01)
(21) 출원번호 10-2017-0180406
(22) 출원일자 2017년12월27일
심사청구일자 2017년12월27일
(56) 선행기술조사문헌
KR1020160118028 A*
L. Baird, "The Swirlds Hashgraph Consensus Algorithm - Fair, Fast, Byzantine Fault Tolerance"(2016.)*
KR101735708 B1*
Y. Liu, Y. Xiao, "A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks", Radioengineering Journal, Vol. 22, No. 4(2013.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 뷰노
서울특별시 서초구 강남대로 507 , 6층(반포동, 신태양빌딩)
(72) 발명자
강주영
경기도 용인시 수지구 풍덕천로22번길 67, 201동 1303호 (풍덕천동, 정자뜰마을태영데시앙2차아파트)
(74) 대리인
특허법인영비

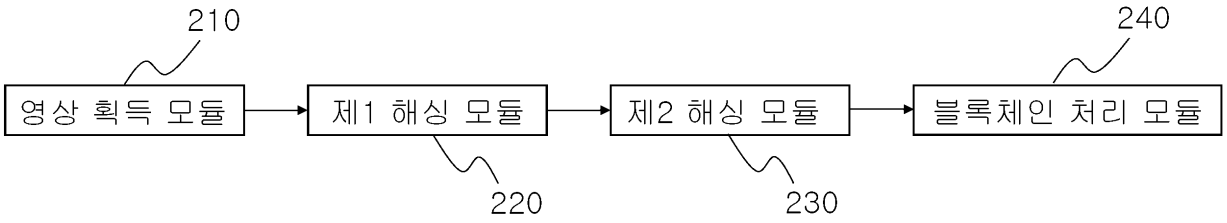
전체 청구항 수 : 총 4 항 심사관 : 정성훈

(54) 발명의 명칭 **영상 해시값 등록 및 검증 방법, 및 이를 이용한 장치**

(57) 요 약

본 발명은 영상의 해시값을 등록하는 방법과 그 해시값이 기 등록된 해시값과 비교하여 유효한지 여부를 검증하는 방법 및 이를 이용한 장치에 관한 것이다. 구체적으로, 본 발명에 따른 영상 해시값 검증 서버는, 특정 영상에 대한 검증 요청이 획득되면, 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 산출된 제1 영상 해시값에 기초한 값 및 소정의 분산 데이터베이스에 등록된 값을 참조로 하여 상기 특정 영상에 대한 검증을 수행하거나 수행하도록 지원한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/6209 (2013.01)

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

영상의 해시값을 검증하는 방법에 있어서,

(a) 특정 영상에 대한 검증 요청이 획득되면, 서버가, (i) 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 제1 영상 해시값을 생성하는 프로세스, 및 (ii) 상기 해시 함수를 이용하여 상기 특정 영상에 대응되는 비교 대상 영상의 제2 영상 해시값을 생성 또는 획득하는 프로세스를 수행하는 단계로서, 상기 변형은, 영상 포맷 변환(image format conversion), 압축(compression), 회전, 확대, 축소 및 블러링(blurring) 중 적어도 하나를 포함하는 단계;

(b) 생성된 상기 제1 영상 해시값과 상기 제2 영상 해시값에 기초하여, 상기 서버가, 상기 특정 영상과 상기 비교 대상 영상의 동일성을 검증하는 단계로서, 상기 제1 영상 해시값과 상기 제2 영상 해시값의 거리를 산출하고, 산출된 상기 거리가 소정의 임계값보다 크면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일하지 않은 것으로 판정하며, 상기 거리가 소정의 임계값보다 작으면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일한 것으로 판정하는 단계;

(c) 상기 거리가 소정의 임계값보다 작으면, 상기 제2 영상 해시값에 기초하여 산출된 제1 등록 해시값이 소정의 분산 데이터베이스에 등록된 위치를 나타내는 대응되는 트랜잭션 식별자(transaction identifier)를 참조하고, 참조된 상기 트랜잭션 식별자를 이용하여 소정의 분산 데이터베이스에 등록된 제2 등록 해시값을 획득하는 단계로서,

상기 제1 등록 해시값은 상기 제2 영상 해시값 및 특정 사용자의 고유 식별 정보를 포함하는 영상 식별 정보로부터 상기 특정 사용자의 개인키(private key)에 의한 인코딩 또는 서명을 거쳐 상기 소정의 분산 데이터베이스에 저장된 해시값인, 단계; 및

(d) 상기 제1 등록 해시값과 상기 제2 등록 해시값이 동일하면, 상기 서버가, 상기 특정 영상이 검증된 것으로 판정하고, 상기 제1 등록 해시값과 상기 제2 등록 해시값이 상이하거나 상기 제2 등록 해시값이 상기 분산 데이터베이스로부터 획득되지 않으면, 상기 서버가, 상기 특정 영상이 검증되지 않은 것으로 판정하는 단계

를 포함하는 영상 해시값 검증 방법.

청구항 7

삭제

청구항 8

삭제

청구항 9

제6항에 있어서,

상기 (c) 단계는,

상기 특정 영상과 상기 비교 대상 영상이 동일하지 않으면, 상기 서버가, 상기 특정 영상이 검증되지 않은 것으로 판정하는 것을 특징으로 하는 영상 해시값 검증 방법.

청구항 10

컴퓨팅 장치로 하여금, 제6항 또는 제9항의 방법을 수행하도록 구현된 명령어(instructions)를 포함하는, 기계 판독 가능한 비일시적 기록 매체에 저장된, 컴퓨터 프로그램.

청구항 11

삭제

청구항 12

특정 영상에 대한 검증 요청을 획득하는 통신부; 및

상기 검증 요청이 획득되면, 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 제1 영상 해시값을 생성하는 프로세스, 및 (ii) 상기 해시 함수를 이용하여 상기 특정 영상에 대응되는 비교 대상 영상의 제2 영상 해시값을 생성 또는 획득하는 프로세스를 수행하는 프로세서

를 포함하되,

상기 변형은,

영상 포맷 변환(image format conversion), 압축(compression), 회전, 확대, 축소 및 블러링(blurring) 중 적어도 하나를 포함하고,

상기 프로세서는,

생성된 상기 제1 영상 해시값과 상기 제2 영상 해시값에 기초하여, 상기 특정 영상과 상기 비교 대상 영상의 동일성을 검증하되, 상기 제1 영상 해시값과 상기 제2 영상 해시값의 거리를 산출하고, 산출된 상기 거리가 소정의 임계값보다 크면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일하지 않은 것으로 판정하며, 상기 거리가 소정의 임계값보다 작으면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일한 것으로 판정하고,

상기 특정 영상과 상기 비교 대상 영상이 동일하면, 상기 제2 영상 해시값에 기초하여 산출된 제1 등록 해시값에 대응되는 트랜잭션 식별자(transaction identifier)를 참조하고, 참조된 상기 트랜잭션 식별자를 이용하여 소정의 분산 데이터베이스에 등록된 제2 등록 해시값을 획득하되, 상기 제1 등록 해시값은 상기 제2 영상 해시값 및 특정 사용자의 고유 식별 정보를 포함하는 영상 식별 정보로부터 상기 특정 사용자의 개인키(private key)에 의한 인코딩 또는 서명을 거쳐 상기 소정의 분산 데이터베이스에 저장된 해시값이고,

상기 제1 등록 해시값과 상기 제2 등록 해시값이 동일하면, 상기 특정 영상이 검증된 것으로 판정하고, 상기 제1 등록 해시값과 상기 제2 등록 해시값이 상이하거나 상기 제2 등록 해시값이 상기 분산 데이터베이스로부터 획득되지 않으면, 상기 특정 영상이 검증되지 않은 것으로 판정하는 것을 특징으로 하는 영상 해시값 검증 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 영상의 해시값을 등록하는 방법과 그 해시값이 기 등록된 해시값과 비교하여 유효한지 여부를 검증하

는 방법 및 이를 이용한 장치에 관한 것이다. 구체적으로, 본 발명에 따른 영상 해시값 검증 서버는, 특정 영상에 대한 검증 요청이 획득되면, 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 산출된 제1 영상 해시값에 기초한 값 및 소정의 분산 데이터베이스에 등록된 값을 참조로 하여 상기 특정 영상에 대한 검증을 수행하거나 수행하도록 지원한다.

배 경 기 술

[0002] 네트워크 기술의 발달로 인하여 다양한 영상들이 네트워크 상에서 송수신되고 있다. 그런데, 이러한 영상은 종종 쉽게 위변조되어 그 가치가 훼손되는 일이 비일비재한데, 영상의 진위 여부나 품질 고하가 매우 중요한 분야에서는 그러한 위변조를 방지하는 것이 중요한 문제가 된다.

[0003] 예를 들어, 영상으로 된 전자화 계약서나 의료 영상에 있어서는 법률관계의 존부와 그 내용, 환자의 목숨이 좌우될 정도로 그 진실성과 품질이 중요하게 다뤄질 수 있다. 특히 2016년 5월 29일 개정 대한민국 형사소송법의 제313조 등에 따르면, 정보저장매체에 저장된 문자, 사진, 영상 등의 정보도 진술서로서의 효력이 인정될 수 있으며, 심지어 진술서의 작성자가 그 진술서의 성립을 부인하는 경우에도 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있게 되었다.

[0004] 다만, 종래에 문서의 내용과 관련하여는 블록체인을 활용하여 그 위변조를 방지하는 기술이 존재했다. 예를 들어 대한민국 등록특허공보 제10-1735708호를 참조하면, 파일의 해시값을 블록체인 데이터베이스에 올려, 그 파일 내용 자체의 위변조를 방지하는 기술이 개시되어 있다.

[0005] 그런데, 이 종래 기술에 따르면 영상으로 된 데이터의 경우에 이와 같은 종래 기술을 그대로 적용하면 영상의 크기 조절(resizing), 포맷 변환은 영상의 본질적인 내용을 바꾸는 것이 아님에도 불구하고 위변조된 것으로 판정하는 단점이 있다.

[0006] 따라서 본 발명에서는 이러한 종래 기술의 단점을 극복하고 영상 포맷 변환(image format conversion), 압축(compression), 회전, 확대, 축소 및 블러링(blurring) 등의 변화에 무관하게 영상의 위변조를 가려낼 수 있는 영상의 해시값 등록 및 검증 방법, 및 이를 이용한 장치를 제안하고자 한다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) KR 10-1735708 B

비특허문헌

[0008] (비특허문헌 0001) YuLing LIU, Yong XIAO. A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks

(비특허문헌 0002) Leemon Baird, The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, May 31, 2016

발명의 내용

해결하려는 과제

[0009] 본 발명은 합의 알고리즘(consensus algorithm)에 기반한 분산(decentralized) 데이터베이스에 영상의 해시값을 기록하여 그 영상의 등록 및 검증을 수행할 수 있는 방법을 제공함으로써 법률적으로 효력 있고, 수학적으로도 검증 가능한 방식으로 영상의 위변조를 방지하는 것을 목적으로 한다.

[0010] 또한, 본 발명은 영상에 대한 몇몇 변경을 허용함으로써 영상의 본질적 내용이 바뀌지 않았음에도 사소한 변화에 위변조된 것으로 판정하는 문제점을 해결함으로써 그 영상의 제공 주체가 다양한 형태{모드(mode), 포맷(format), 해상도(resolution) 등}로 그 영상을 제공할 수 있는 편의를 제공하는 것을 목적으로 한다.

[0011] 이와 같이 본 발명은 합의 알고리즘 기술을 이용하여 계약서의 스캔본, 의료 영상 등 다양한 종류의 영상에 대하여 위변조를 방지함으로써 영상을 주고받는 당사자들 간의 신뢰를 유지할 수 있는 암호학적 입증 방법을 제시하는 것을 목적으로 한다.

과제의 해결 수단

[0012] 상기한 바와 같은 본 발명의 목적을 달성하고, 후술하는 본 발명의 특징적인 효과를 실현하기 위한 본 발명의 특징적인 구성은 하기와 같다.

[0013] 본 발명의 일 태양에 따르면, 영상 해시값 등록 방법이 제공되는바, 그 방법에 따르면, 특정 영상에 대한 등록 요청이 획득되면, 서버가, 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 산출된 영상 해시값에 기초한 값을 소정의 분산 데이터베이스에 등록하거나 등록하도록 지원한다.

[0014] 본 발명의 다른 태양에 따르면, 영상 해시값 검증 방법이 제공되는바, 그 방법에 따르면, 특정 영상에 대한 검증 요청이 획득되면, 서버가, 상기 특정 영상에 적용되는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 해시 함수를 이용하여 상기 특정 영상으로부터 산출된 제1 영상 해시값에 기초한 값 및 소정의 분산 데이터베이스에 등록된 값을 참조로 하여 상기 특정 영상에 대한 검증을 수행하거나 수행하도록 지원한다.

[0015] 본 발명의 또 다른 태양에 따르면, 전술한 방법들을 수행하도록 구현된 명령어(instructions)를 포함하는, 기계 판독 가능한 비일시적 기록 매체에 저장된, 컴퓨터 프로그램도 제공된다.

[0016] 또한, 본 발명의 다른 일 태양에 따르면, 전술한 방법들을 수행하는 컴퓨팅 장치인 영상 해시값 등록 서버 및 영상 해시값 검증 서버도 제공된다.

발명의 효과

[0017] 본 발명에 의하면, 합의 알고리즘에 기반한 분산 데이터베이스에 영상에 관한 해시값이 기록되어 영상의 위변조가 방지되는 효과가 있다.

[0018] 또한, 본 발명에 의하면, 영상의 본질적 내용이 바뀌지 않는 몇몇 변경에도 불구하고 그 영상의 해시값이 불변이거나 크게 변하지 않는 저항성이 있으므로 그 영상의 제공 주체가 다양한 형태{모드(mode), 포맷(format), 해상도(resolution) 등} 로 그 영상을 제공할 수 있는 편의의 효과가 있다.

[0019] 그리고 본 발명에 의하면, 다양한 종류의 영상에 대하여 위변조를 방지함으로써 영상을 주고받는 당사자들 간에 해당 영상에 대한 신뢰가 유지될 수 있는 효과가 있다.

[0020] 합의 알고리즘에 기반한 분산 데이터베이스에 접근 가능한 컴퓨팅 장치라면 무엇이든 본 발명의 효과를 향유할 수 있으므로, 본 발명의 방법이 특정 운영체제(operating system) 등의 플랫폼에 종속되지 않음은 물론이다.

도면의 간단한 설명

[0021] 본 발명의 실시예의 설명에 이용되기 위하여 첨부된 아래 도면들은 본 발명의 실시예들 중 단지 일부일 뿐이며, 본 발명이 속한 기술분야의 통상의 기술자에게 있어서는 발명적 작업이 이루어짐 없이 이 도면들에 기초하여 다른 도면들이 얻어질 수 있다.

도 1은 본 발명에 따른 영상 해시값 등록 방법 및 영상 해시값 검증 방법을 수행하는 서버의 예시적 구성을 개략적으로 도시한 개념도이다.

도 2는 본 발명에 따른 영상 해시값 등록 방법 및 영상 해시값 검증 방법을 수행하는 서버의 하드웨어 또는 소프트웨어 구성요소를 도시한 예시적 블록도이다.

도 3은 본 발명에 따른 영상 해시값 등록 방법의 일 실시예를 나타낸 흐름도이다.

도 4는 본 발명에 따른 영상 해시값 검증 방법의 일 실시예를 나타낸 흐름도이다.

도 5는 본 발명의 따른 영상 해시값 검증 방법에 있어서 해시값의 비교를 통하여 특정 영상과 비교 대상 영상 간의 동일성을 검증하는 단계를 더 구체화한 실시예를 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 후술하는 본 발명에 대한 상세한 설명은, 본 발명의 목적들, 기술적 해법들 및 장점들을 분명하게 하기 위하여 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 통상의 기술자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다.

[0023] 본 발명의 상세한 설명 및 청구항들에 걸쳐 이용된 "영상" 또는 "영상 데이터"라는 용어는 이산적 영상 요소들(예컨대, 2차원 영상에 있어서는 픽셀, 3차원 영상에 있어서는 복셀)로 구성된 다차원 데이터를 지칭한다.

[0024] 그리고 본 발명의 상세한 설명 및 청구항들에 걸쳐, '포함하다'라는 단어 및 그 변형은 다른 기술적 특징들, 부가물들, 구성요소들 또는 단계들을 제외하는 것으로 의도된 것이 아니다. 또한, '하나' 또는 '한'은 하나 이상의 의미로 쓰인 것이며, '또 다른'은 적어도 두 번째 이상으로 한정된다.

[0025] 또한 본 발명의 상세한 설명 및 청구항들에 걸쳐 이용된 A "에 기초한 값"이라는 표현은, (i) A 자체, (ii) A를 포함하는 값, 또는 (iii) 상기 (i) 또는 (ii)로부터 가공된 값을 지칭한다.

[0026] 통상의 기술자에게 본 발명의 다른 목적들, 장점들 및 특성들이 일부는 본 설명서로부터, 그리고 일부는 본 발명의 실시로부터 드러날 것이다. 아래의 예시 및 도면은 실례로서 제공되며, 본 발명을 한정하는 것으로 의도된 것이 아니다. 따라서, 특정 구조나 기능에 관하여 본 명세서에 개시된 상세 사항들은 한정하는 의미로 해석되어서는 아니되고, 단지 통상의 기술자가 실질적으로 적합한 임의의 상세 구조들로써 본 발명을 다양하게 실시하도록 지침을 제공하는 대표적인 기초 자료로 해석되어야 할 것이다.

[0027] 더욱이 본 발명은 본 명세서에 표시된 실시예들의 모든 가능한 조합들을 망라한다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 사상 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 사상 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0028] 본 명세서에서 달리 표시되거나 분명히 문맥에 모순되지 않는 한, 단수로 지칭된 항목은, 그 문맥에서 달리 요구되지 않는 한, 복수의 것을 아우른다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0029] 이제 각 실시예에 대한 설명을 위하여 본 명세서에서 사용되는 표현식을 다음과 같이 정의한다. ':'의 왼쪽은 표현식을 나타내며, 오른쪽의 표현식의 정의를 나타낸다.

[0030] PrivX: X의 개인키(private key)

[0031] PubX: X의 공개키(public key)

[0032] SigPrivX(Y): PrivX를 이용하여 Y를 ECDSA 또는 RSA 서명한 출력값

[0033] VerPubX(Y): PubX를 이용한 SigPrivX(Y) 검증의 출력값(참 또는 거짓)

[0034] EncPrivX(Y): PrivX를 이용하여 Y의 ECC 또는 RSA 인코딩(암호화)한 출력값

[0035] DecPubX(Y): PubX를 이용하여 Y의 ECC 또는 RSA 디코딩(복호화)한 출력값

[0036] $Hash_1(Y)$: 제1 해시 함수의 Y에 대한 출력값

[0037] $Hash_2(Y)$: 제2 해시 함수의 Y에 대한 출력값, 예컨대 triple_SHA256(Y)

[0038] 이하, 통상의 기술자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 바람직한 실시예들에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0039] 도 1은 본 발명에 따른 영상 해시값 등록 방법 및 영상 해시값 검증 방법을 수행하는 서버의 예시적 구성을 개략적으로 도시한 개념도이다.

[0040] 도 1을 참조하면, 본 발명의 일 실시예에 따른 컴퓨팅 장치인 서버(100)는, 통신부(110) 및 프로세서(120)를 포

함하며, 상기 통신부(110)를 통하여 외부 컴퓨팅 장치(미도시)와 직간접적으로 통신할 수 있다.

[0041] 구체적으로, 상기 서버(100)는, 전형적인 컴퓨터 하드웨어(예컨대, 컴퓨터 프로세서, 메모리, 스토리지, 입력 장치 및 출력 장치, 기타 기존의 컴퓨팅 장치의 구성요소들을 포함할 수 있는 장치; 라우터, 스위치 등과 같은 전자 통신 장치; 네트워크 부착 스토리지(NAS; network-attached storage) 및 스토리지 영역 네트워크(SAN; storage area network)와 같은 전자 정보 스토리지 시스템)와 컴퓨터 소프트웨어(즉, 컴퓨팅 장치로 하여금 특정의 방식으로 기능하게 하는 명령어들)의 조합을 이용하여 원하는 시스템 성능을 달성하는 것일 수 있다.

[0042] 이와 같은 서버의 통신부(110)는 연동되는 타 컴퓨팅 장치와 요청과 응답을 송수신할 수 있는바, 일 예시로서 그러한 요청과 응답은 동일한 TCP(transmission control protocol) 세션(session)에 의하여 이루어질 수 있지만, 이에 한정되지는 않는바, 예컨대 UDP(user datagram protocol) 데이터그램(datagram)으로서 송수신될 수도 있을 것이다. 덧붙여, 넓은 의미에서 상기 통신부(110)는 명령어 또는 지시 등을 전달받기 위한 키보드, 마우스, 기타 외부 입력장치, 프린터, 디스플레이, 기타 외부 출력장치를 포함할 수 있다.

[0043] 또한, 서버의 프로세서(120)는 MPU(micro processing unit), CPU(central processing unit), GPU(graphics processing unit) 또는 TPU(tensor processing unit), 캐시 메모리(cache memory), 데이터 버스(data bus) 등의 하드웨어 구성을 포함할 수 있다. 또한, 운영체제, 특정 목적을 수행하는 애플리케이션의 소프트웨어 구성을 더 포함할 수도 있다.

[0044] 도 2는 본 발명에 따른 영상 해시값 등록 방법 및 영상 해시값 검증 방법을 수행하는 서버의 하드웨어 또는 소프트웨어 구성요소를 도시한 예시적 블록도이다.

[0045] 도 2를 참조하여 본 발명에 따른 방법 및 장치의 구성을 개관하면, 서버(100)는 그 일 구성요소로서 영상 획득 모듈(210)을 포함할 수 있다. 이와 같은 영상 획득 모듈(210)은 상기 서버(100)에 포함된 통신부(110), 또는 상기 통신부(110) 및 프로세서(120)의 연동에 의하여 구현될 수 있음은 통상의 기술자가 이해할 수 있을 것이다.

[0046] 도 2를 참조하면, 영상 획득 모듈(210)은, 특정 영상에 대한 등록 요청 또는 검증 요청을 획득할 수 있는데, 그 특정 영상의 등록 또는 검증을 위하여 그 특정 영상의 데이터가 아울러 획득된다.

[0047] 다음으로, 특정 영상의 데이터는, 상기 획득된 요청에 따라 제1 해싱 모듈(220)에 전달될 수 있는데, 상기 프로세서(120)에 의하여 구현될 수 있는 제1 해싱 모듈(220)은, 해시 함수를 이용하여 상기 특정 영상의 영상 해시값을 생성할 수 있다. 여기에서 이용되는 해시 함수는 상기 특정 영상에 적용될 수 있는 적어도 하나의 변형에 대하여 불변(invariant)이거나 저항성(resistant to)이 있는 것이 특징이다. 달리 말하자면, 상기 적어도 하나의 변형이 상기 특정 영상에 적용되더라도 상기 특정 영상의 영상 해시값이 변화되지 않거나 그 변화의 정도가 미미하다. 예를 들어, 이 변화의 정도는 해시값 사이의 거리, 예컨대 해밍 거리(Hamming distance)로 측정될 수 있다. 여기에서 적어도 하나의 변형이란, 영상 포맷 변환(image format conversion), 압축(compression), 회전, 확대, 축소 및 블러링(blurring)일 수 있다.

[0048] 그 다음, 생성된 영상 해시값은, 제2 해싱 모듈(230)에 전달될 수 있는데, 상기 프로세서(120)에 의하여 구현될 수 있는 제2 해싱 모듈(230)은, 제2 해시 함수를 이용하여 영상 해시값 및 상기 영상의 등록을 요청한 특정 사용자의 고유 식별 정보를 포함하는 영상 식별 정보의 적어도 일부가 상기 특정 사용자의 개인키(private key)로 인코딩된 값으로부터 등록 해시값을 산출할 수 있다.

[0049] 산출된 등록 해시값은, 통신부(110)를 통하여 외부 노드들과 연동되는 데이터베이스 처리 모듈(240), 예컨대 블록체인 처리 모듈에 전달될 수 있는데, 프로세서(120) 및 통신부(110)의 연동에 의하여 구현될 수 있는 데이터베이스 처리 모듈(240)은, 등록 해시값을 이용하여 도 3과 관련하여 상세히 후술할 등록 또는 검증을 수행할 수 있다. 여기에서 외부 노드들은 합의 알고리즘에 기반한 분산 데이터베이스를 구성하는 다수의 컴퓨팅 장치들을 지칭한다. 본 명세서에서 설명되는 합의 알고리즘에 기반한 분산 데이터베이스는 개별 컴퓨팅 장치가 하나의 노드를 이루고 있는 분산 시스템으로서, 복수의 노드로 이루어진 분산 시스템을 지칭한다. 예컨대, 비트코인 등의 암호 화폐의 거래에 이용되는 블록체인 데이터베이스의 경우에는 이를 처리하는 서버가 현재 전세계적으로 분산된 다수의 노드를 가지는 거대한 분산 시스템으로 이루어져 있다.

[0050] 본 발명에서 언급되는 분산 데이터베이스는 크게 다음 2가지 문제를 해결하는 것을 조건으로 한다.

[0051] 첫 번째, 분산 데이터베이스는 합의 문제를 해결하여야 하며, 이를 위한 합의 알고리즘은 3가지 조건을 만족하여야 한다. 그 3가지 조건은, i) 모든 프로세스가 같은 값을 결정하는 것이며, ii) 그 결정된 데이터는 특정

프로세스에 의하여 제안된 것이어야 하고, iii) 모든 시스템의 상태는 0이나 1로 결정되어야 한다는 것이다. 즉, 모두 1이거나 0인지를 판단할 수 있어야 한다. 이들 조건을 만족시키는 알고리즘을 합의 알고리즘이라고 한다.

[0052] 두 번째, 분산 데이터베이스는 비잔틴 장군 문제(Byzantine General Problem)를 해결하여야 한다. 즉, 악의적인 노드가 분산 데이터베이스에 참여한 상황에서도 전체 시스템은 신뢰도 있는 서비스를 제공하여야 한다는 것이다.

[0053] 본 발명에서는 이 2가지 문제를 해결할 수 있는 분산 데이터베이스를 이용하며, 이 중 잘 알려진 것은 비트코인 등의 암호 화폐가 활용하는 블록체인이다. 그러나 통상의 기술자는 분산 데이터베이스가 이에 한정되지 않으며, 예컨대 비특허문헌 2: Leemon Baird, The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, May 31, 2016에 개시된 해시그래프(hash graph)와 같은 타 분산 데이터베이스에도 적용 가능하다는 점을 이해할 수 있을 것이다.

[0054] 데이터베이스 처리 모듈(240)은 서버(100)가 보유, 저장 또는 취급하는 데이터들을 분산 관리 및 상호 검증되는 분산 데이터베이스에 기입하고 비교 검증하는 등, 취급 대상인 데이터를 분산 데이터베이스에 연관시키는 작용, 즉 앵커링(anchoring)을 수행한다고 할 수 있다.

[0055] 도 2에 나타난 구성요소들은 설명의 편의상 하나의 컴퓨팅 장치(예컨대, single standalone workstation)에서 실현되는 것으로 예시되었으나, 본 발명의 방법을 수행하는 컴퓨팅 장치인 서버(100)는 복수로 구성될 수도 있을 것이다.

[0056] 이제 본 발명에 따른 영상 해시값 등록 방법의 일 실시예를 도 3을 참조하여 구체적으로 설명하기로 한다. 도 3은 본 발명에 따른 영상 해시값 등록 방법의 일 실시예를 나타낸 흐름도이다.

[0057] 도 3을 참조하면, 본 발명에 따른 영상 해시값 등록 방법은, 앞서 도 2를 참조하여 설명한 바와 같이, 우선, 특정 영상 A에 대한 등록 요청이 서버(100)에서 획득(S305)되면, 서버(100)가, 해시 함수 $Hash_1$를 이용하여 특정 영상 A의 영상 해시값 $Hash_1(A)$을 생성하거나 서버(100)에 연동되는 타 장치로 하여금 생성하도록 지원(S310)하는 단계(S305, S310)를 포함한다.

[0058] 여기에서 상기 변형은, 영상 포맷 변환, (JPEG 등의) 압축, 회전, 확대, 축소 및 블러링을 포함하나 이에 한정하지 않음이 이해될 수 있을 것이다. 이와 같은 변형에는 평행이동(translation), 저역통과 필터(low-pass filter), 중앙값 필터(median filter), 가우시안 노이즈(Gaussian noise) 등등이 포함될 수도 있다.

[0059] 이와 같은 변형에 대하여 불변이거나 저항성이 있는 해시 함수의 일 예시는 비특허문헌 1: YuLing LIU, Yong XIAO. A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks에 개시된 바와 같다. 예를 들어 해시 함수는 소정의 비밀키에 기초하여 해시 생성에 필요한 특징 추출을 수행할 수 있다. 소정의 비밀키가 이용되는 경우에, 비밀키가 상이하면 전혀 다른 영상 해시값이 생성될 수 있다.

[0060] 한편, 영상 해시값은 상기 영상에 대응되도록 서버(100)에 의하여 보유될 수 있으며, 등록 요청의 주체, 즉, 사용자에게 제공될 수도 있다. 영상의 제공 주체인 사용자는 영상을 타 주체에 제공할 때, 영상의 검증에 대한 편의를 제공하기 위하여 영상 해시값을 제공할 수 있다.

[0061] 도 3을 참조하면, 본 발명에 따른 영상 해시값 등록 방법은, 단계(S305, S310) 다음으로, 상기 서버(100)가, 상기 영상 해시값에 기초하여 산출(S315)된 등록 해시값을 소정의 분산 데이터베이스에 등록하거나 등록하도록 지원(S320)하는 단계(S315, S320)를 더 포함한다.

[0062] 여기에서 등록 해시값은, 상기 영상 해시값 $Hash_1(A)$ 및 특정 사용자 U의 고유 식별 정보 P를 포함하는 영상 식별 정보 $B_{i=1,\cdots,n}$의 적어도 일부가 상기 특정 사용자 U의 개인키(private key) PrivU로 인코딩된 값 C으로부터 제2 해시 함수($Hash_2$)를 이용하여 산출된 해시값 $Hash_2(C)$일 수 있다. 예를 들어, 상기 인코딩된 값 C은 영상 해시값 $Hash_1(A)$을 개인키 PrivU로 인코딩한 값인 $EncPrivU(Hash_1(A))$에 상기 고유 식별 정보 P를 스트링 연결(string concatenation)한 값일 수 있다.

[0063] 대안으로서, 상기 개인키 PrivU로 인코딩하는 대신에 상기 개인키 PrivU로 서명하는 방식이 이용될 수도 있을 것이다. 예컨대 $EncPrivU(Hash_1(A))$에 P를 스트링 연결한 값 대신에 $SigPrivU(Hash_1(A))$에 P를 스트링 연결한 값이 이용될 수 있다.

[0064] 서버(100)는 등록 해시값을 분산 데이터베이스에 등록할 뿐만 아니라, 바람직하게는 그 등록 해시값의 원시 정보(raw data)를 보유할 수 있는바, 예컨대, 제2 등록 해시값이 $Hash_2(C)$이고 C는 영상 A에 대하여 $EncPrivU(Hash_1(A))$에 고유 식별 정보 P를 스트링 연결한 값인 경우에 그 C값을 보유할 수 있고, 추후 이를 통하여 서버(100)에서 보유한 영상 A의 해시값이 진실(genuine)된 것인지를 검증할 수 있을 것이다.

[0065] 여기에서 제2 해시 함수는 전술한 해시 함수, 즉 영상 해시값을 생성하는 제1 해시 함수와는 상이한 것일 수 있는바, 제2 해시 함수는 영상이 아닌 string에 적용되는 통상적인 해시 함수로서, 예컨대 triple_SHA256, MD5 등일 수 있다.

[0066] 한편, 사용자의 고유 식별 정보 P라고 함은, 사용자의 성명 또는 명칭 등 사용자의 개인 정보를 포함하는 것일 수 있으나, 그러한 개인 정보로부터 가공된 값 또는 사용자를 식별하기 위하여 임의로 부여된 영숫자열(alphanumeric string)일 수 있는바, 이와 같은 고유 식별 정보 P가 사용자의 신원을 나타내는 다른 정보로부터 생성되지 않을 수도 있다는 점은 물론이다. 이러한 사용자의 고유 식별 정보 P는 영상과 관련하여 영상의 제공 주체인 사용자로부터 영상의 이용 주체에게 제공될 것으로 의도되는 정보이다. 따라서 후술하는 영상 해시값 검증 방법에서 검증을 요청하는 영상의 이용 주체는 영상의 제공 주체인 사용자의 고유 식별 정보 P를 알고 있거나 용이하게 획득할 수 있음이 전제된다.

[0067] 단계(S315)에서 인코딩된 값에 대해서는 상기 개인키에 대응되는 공개키(public key)에 의한 디코딩을 통하여 그 진위를 판정할 수 있으며, 서명된 값에 대해서는 상기 공개키에 의한 서명 검증(signature verification)을 통하여 그 진위를 판정할 수 있는바, 이는 후술할 영상 해시값 검증 방법에서 이용된다.

[0068] 단계(S320)에서 등록 해시값은, 예컨대, 비트코인의 OP_RETURN 스크립트 코드에 기입되는 메시지로서 비트코인의 블록체인 데이터베이스에 등록될 수 있는데, 이는 하나의 예시에 지나지 않고, 분산 데이터베이스의 유형마다 상이한 방식이 이용될 수 있을 것이다.

[0069] 다시 도 3을 참조하면, 단계(S315, S320) 후에, 발명에 따른 영상 해시값 등록 방법은, 상기 서버(100)가, 상기 등록 해시값이 상기 소정의 분산 데이터베이스에 등록된 위치를 나타내는 트랜잭션 식별자(transaction identifier)를 획득하거나 획득하도록 지원하는 단계(S330)를 더 포함한다. 이 단계(S330)는 단계(S320)와 동시에 수행되거나 이시에 수행될 수 있는데, 이시에 수행되는 경우에는 단계(S320)가 수행된 후에 단계(S330)가 수행되거나 단계(S330)가 수행된 후에 단계(S320)가 수행될 수 있다. 이와 같은 트랜잭션 식별자는 상기 영상 및/또는 상기 영상으로부터 산출된 값, 예컨대, 상기 등록 해시값에 대응되도록 서버(100)에 의하여 보유될 수 있다. 이 트랜잭션 식별자는 서버(100)에 의하여 보유될 수 있을 뿐만 아니라 등록 요청의 주체, 즉, 사용자에게 제공될 수도 있다. 영상의 제공 주체인 사용자는 영상을 타 주체에 제공할 때, 영상과 함께 이 트랜잭션 식별자를 제공함으로써 영상이 위변조되지 않았음을 보장할 수 있는바, 이를 검증하기 위한 방법은 다음과 같다.

[0070] 즉, 본 발명에 따르면 영상 해시값에 대한 검증 방법도 제공되는데, 특정 영상의 영상 해시값에 대한 검증은 본 발명의 영상 해시값 등록 방법에 따라 소정의 분산 데이터베이스에 비교 대상 영상의 영상 해시값이 등록된 상태에서 수행된다.

[0071] 도 4는 본 발명에 따른 영상 해시값 검증 방법의 일 실시예를 나타낸 흐름도이다.

[0072] 도 4를 참조하면, 본 발명에 따른 영상 해시값 검증 방법은, 우선, 특정 영상에 대한 검증 요청이 획득(S405)되면, 서버(100)가, (i) 해시 함수를 이용하여 상기 특정 영상의 제1 영상 해시값을 생성하는 프로세스(S410-1; 미도시), 및 (ii) 상기 해시 함수를 이용하여 상기 특정 영상에 대응되는 비교 대상 영상의 제2 영상 해시값을 생성 또는 획득하는 프로세스(S410-2; 미도시)를 수행하거나 수행하도록 지원하는 단계(S410)를 포함한다. 여기에서 해시 함수는 전술한 제1 해시 함수와 동일한 것이다.

[0073] 프로세스(S410-2)에서의 제2 영상 해시값은 검증 요청과 함께 획득되는 비교 대상 영상에 제1 해시 함수를 적용하여 생성된 값일 수 있으나, 검증을 요청하는 주체가 제2 영상 해시값을 알고 있는 때에는 검증 요청과 함께 획득되는 값일 수도 있다.

[0074] 다음으로, 본 발명에 따른 영상 해시값 검증 방법은, 상기 제1 영상 해시값과 상기 제2 영상 해시값에 기초하여, 서버(100)가, 상기 특정 영상과 상기 비교 대상 영상의 동일성을 검증하거나 검증하도록 지원하는 단계(S420)를 더 포함한다.

[0075] 단계(S420)의 일 실시예에서는, 상기 서버(100)가, 상기 서버가, 상기 제1 영상 해시값과 상기 제2 영상 해시값

의 거리를 산출하거나 산출하도록 지원하고, 산출된 상기 거리가 소정의 임계값보다 크면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일하지 않은 것으로 판정하며, 상기 거리가 소정의 임계값보다 작으면, 상기 제1 영상 해시값과 상기 제2 영상 해시값이 동일한 것으로 판정할 수 있다. 여기에서 거리(distance)는 예컨대 해밍 거리(Hamming distance)일 수 있다.

[0076] 도 5는 본 발명의 따른 영상 해시값 검증 방법에 있어서 해시값의 비교를 통하여 특정 영상과 비교 대상 영상 간의 동일성을 검증하는 단계(S420)를 더 구체화한 실시예를 나타낸 흐름도이다.

[0077] 도 5를 참조하여 영상 해시값의 생성 과정을 다시 살펴보면, 우선 영상이 입력되면, 비밀키에 기초한 상기 영상의 특징 추출이 수행됨으로써 영상 해시값이 생성된다(예컨대 비특허문헌 1 참조). 제1 영상 해시값과 제2 영상 해시값 모두가 이와 같은 방식으로 생성될 수 있다. 이 제1 영상 해시값과 제2 영상 해시값 간의 해밍 거리가 전술한 소정의 임계값보다 크면 영상이 서로 동일하지 않아 검증이 실패한 것으로 판정되며, 임계값보다 작으면 영상이 실질적으로 동일하여 검증이 성공한 것으로 판정되는 것이다.

[0078] 단계(S420)에서 상기 특정 영상과 상기 비교 대상 영상이 동일하면, 본 발명에 따른 영상 해시값 검증 방법은, 서버(100)가, 상기 제2 영상 해시값에 기초하여 산출된 제1 등록 해시값에 대응되는 트랜잭션 식별자(transaction identifier)를 참조하거나 참조하도록 지원하고, 참조된 상기 트랜잭션 식별자를 이용하여 소정의 분산 데이터베이스(blockchain)에 등록된 제2 등록 해시값을 획득하거나 획득하도록 지원하는 단계(S430)를 더 포함한다.

[0079] 여기에서 트랜잭션 식별자의 참조는, 검증 요청의 주체에 의하여 서버에 제공된 트랜잭션 식별자를 참조하는 것일 수 있으며, 대안으로서, 검증 요청의 주체로부터 제2 영상 해시값이 서버(100)에 제공되면, 그 제2 영상 해시값에 대하여 산출한 등록 해시값에 대응되도록 서버(100)에서 보유하고 있는 트랜잭션 식별자를 참조하는 것일 수도 있다.

[0080] 어떤 경우에라도 트랜잭션 식별자는 기 등록된 것이어야 하는바, 그렇지 않으면, 분산 데이터베이스에 대한 검증 요청 주체의 열람에 의하여 조작(부정행위) 여부가 드러날 것이다.

[0081] 또한, 서버(100)가 등록 해시값의 원시 정보 C를 보유한 경우에는, 이를 통하여 영상 해시값이 진실된 것인지를 검증할 수 있다. 예를 들어 영상 A에 대한 등록 해시값이 $Hash_2(C)$이고 C는 $EncPrivU(Hash_1(A))$에 등록 주체의 고유 식별 정보 P를 스트링 연결한 값인 경우에, $EncPrivU(Hash_1(A))$를 공개키 PubU에 의하여 디코딩한 결과 $DecPubU(EncPrivU(Hash_1(A)))$인 $Hash_1(A)$이 영상 해시값과 동일한 것인지를 판정함으로써 그 영상 해시값이 진실된 것인지 확인할 수 있다.

[0082] 대안으로서, C가 $SigPrivU(Hash_1(A))$에 P를 스트링 연결한 값인 경우에, $SigPrivU(Hash_1(A))$를 공개키 PubU에 의하여 서명을 검증한 결과 $VerPubU(SigPrivU(Hash_1(A)))$의 불값(Boolean value)이 참인지 여부를 판정함으로써 그 영상 해시값이 진실된 것인지를 확인할 수 있다.

[0083] C에 고유 식별 정보 P가 반영되어 있으며, P가 위변조되면 C가 달라져 결과적으로 등록 해시값이 변경되므로, 고유 식별 정보의 위변조 여부도 함께 검증될 수 있다.

[0084] 한편, 단계(S420)에서 상기 특정 영상과 상기 비교 대상 영상이 동일하지 않은 것으로 판정되면, 상기 서버(100)가, 상기 특정 영상은 검증되지 않은 것으로 판정, 즉, 위변조된 것으로 판정하고 종료될 수 있다.

[0085] 다시 도 4를 참조하면, 본 발명에 따른 영상 해시값 검증 방법은, 단계(S430)의 수행 후에, 상기 제1 등록 해시값과 상기 제2 등록 해시값이 동일하면, 서버(100)가, 상기 특정 영상이 검증된 것으로 판정하거나 판정하도록 지원하고, 상기 제1 등록 해시값과 상기 제2 등록 해시값이 상이하거나 상기 제2 등록 해시값이 상기 분산 데이터베이스로부터으로부터 획득되지 않으면, 서버(100)가, 상기 특정 영상이 검증되지 않은 것으로 판정하거나 판정하도록 지원하는 단계(S440)를 더 포함한다.

[0086] 전술한 단계들을 통해 검증 요청의 주체는 특정 영상과 비교 대상 영상이 동일한지 여부를 검증할 수 있는바, 분산 데이터베이스에서 보유되는 정보인 제2 등록 해시값에 의한 비교를 통하여 검증 결과의 조작이 배제된다.

[0087] 즉, 본 발명은 전술한 모든 실시예들에 걸쳐, 법률적인 효력을 가지는 검증이 영상의 형식으로 된 정보에 대하여 가능하게 되는 효과가 있다. 상기 실시예들로써 여기에서 설명된 기술의 이점은, 서로 다른 포맷으로 되거나 영상의 크기와 무관하게 일정 범위 내에서 변형된 영상에 대해서도 영상의 동일성을 가려낼 수 있게 되어 영

상의 제공 주체가 다양한 형태로 영상을 제공할 수 있으며, 이를 제공받는 주체도 그 영상의 위변조 여부를 전문가의 도움 없이 손쉽게 판정할 수 있게 되며, 그 결과도 분산 데이터베이스에 의하여 진정성이 보장된다는 점이다.

[0088] 위 실시예의 설명에 기초하여 해당 기술분야의 통상의 기술자는, 본 발명의 방법 및/또는 프로세스들, 그리고 그 단계들이 하드웨어, 소프트웨어 또는 특정 용례에 적합한 하드웨어 및 소프트웨어의 임의의 조합으로 실현될 수 있다는 점을 명확하게 이해할 수 있다. 상기 하드웨어는 범용 컴퓨터 및/또는 전용 컴퓨팅 장치 또는 특정 컴퓨팅 장치 또는 특정 컴퓨팅 장치의 특별한 모습 또는 구성요소를 포함할 수 있다. 상기 프로세스들은 내부 및/또는 외부 메모리를 가지는, 하나 이상의 마이크로프로세서, 마이크로컨트롤러, 임베디드 마이크로컨트롤러, 프로그래머블 디지털 신호 프로세서 또는 기타 프로그래머블 장치에 의하여 실현될 수 있다. 게다가, 혹은 대안으로서, 상기 프로세스들은 주문형 집적회로(application specific integrated circuit; ASIC), 프로그래머블 게이트 어레이(programmable gate array), 프로그래머블 어레이 로직(Programmable Array Logic; PAL) 또는 전자 신호들을 처리하기 위해 구성될 수 있는 임의의 다른 장치 또는 장치들의 조합으로 실시될 수 있다. 더욱이 본 발명의 기술적 해법의 대상물 또는 선행 기술들에 기여하는 부분들은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 기계 판독 가능한 기록 매체에 기록될 수 있다. 상기 기계 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 기계 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 통상의 기술자에게 공지되어 사용 가능한 것일 수도 있다. 기계 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD, Blu-ray와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 전술한 장치들 중 어느 하나뿐만 아니라 프로세서, 프로세서 아키텍처 또는 상이한 하드웨어 및 소프트웨어의 조합들의 이종 조합, 또는 다른 어떤 프로그램 명령어들을 실행할 수 있는 기계 상에서 실행되기 위하여 저장 및 컴파일 또는 인터프리트될 수 있는, C와 같은 구조적 프로그래밍 언어, C++ 같은 객체지향적 프로그래밍 언어 또는 고급 또는 저급 프로그래밍 언어(어셈블리어, 하드웨어 기술 언어들 및 데이터베이스 프로그래밍 언어 및 기술들)를 사용하여 만들어질 수 있는바, 기계어 코드, 바이트코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 이에 포함된다.

[0089] 따라서 본 발명에 따른 일 태양에서는, 앞서 설명된 방법 및 그 조합들이 하나 이상의 컴퓨팅 장치들에 의하여 수행될 때, 그 방법 및 방법의 조합들이 각 단계들을 수행하는 실행 가능한 코드로서 실시될 수 있다. 다른 일 태양에서는, 상기 방법은 상기 단계들을 수행하는 시스템들로서 실시될 수 있고, 방법들은 장치들에 걸쳐 여러 가지 방법으로 분산되거나 모든 기능들이 하나의 전용, 독립형 장치 또는 다른 하드웨어에 통합될 수 있다. 또 다른 일 태양에서는, 위에서 설명한 프로세스들과 연관된 단계들을 수행하는 수단들은 앞서 설명한 임의의 하드웨어 및/또는 소프트웨어를 포함할 수 있다. 그러한 모든 순차 결합 및 조합들은 본 개시서의 범위 내에 속하도록 의도된 것이다.

[0090] 예를 들어, 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다. 상기 하드웨어 장치는, 프로그램 명령어를 저장하기 위한 ROM/RAM 등과 같은 메모리와 결합되고 상기 메모리에 저장된 명령어들을 실행하도록 구성되는 MPU, CPU, GPU, TPU와 같은 프로세서를 포함할 수 있으며, 외부 장치와 신호를 주고 받을 수 있는 통신부를 포함할 수 있다. 덧붙여, 상기 하드웨어 장치는 개발자들에 의하여 작성된 명령어들을 전달받기 위한 키보드, 마우스, 기타 외부 입력장치를 포함할 수 있다.

[0091] 이상에서 본 발명이 구체적인 구성요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나, 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명이 상기 실시예들에 한정되는 것은 아니며, 본 발명이 속하는 기술분야에서 통상적인 지식을 가진 사람이라면 이러한 기재로부터 다양한 수정 및 변형을 꾀할 수 있다.

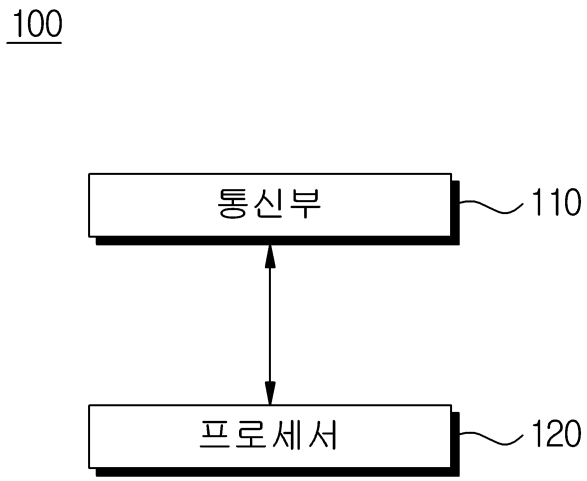
[0092] 따라서, 본 발명의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하게 또는 등가적으로 변형된 모든 것들은 본 발명의 사상의 범주에 속한다고 할 것이다.

[0093] 그와 같이 균등하게 또는 등가적으로 변형된 것에는, 예컨대 본 발명에 따른 방법을 실시한 것과 동일한 결과를 낼 수 있는, 논리적으로 동치(logically equivalent)인 방법이 포함될 것인바, 본 발명의 진의 및 범위는 전술

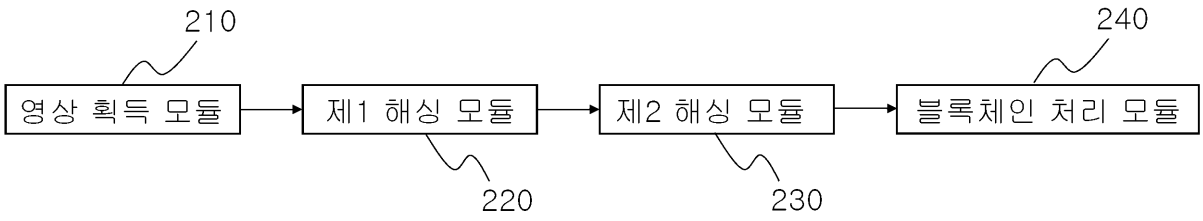
한 예시들에 의하여 제한되어서는 아니되며, 법률에 의하여 허용 가능한 가장 넓은 의미로 이해되어야 한다.

도면

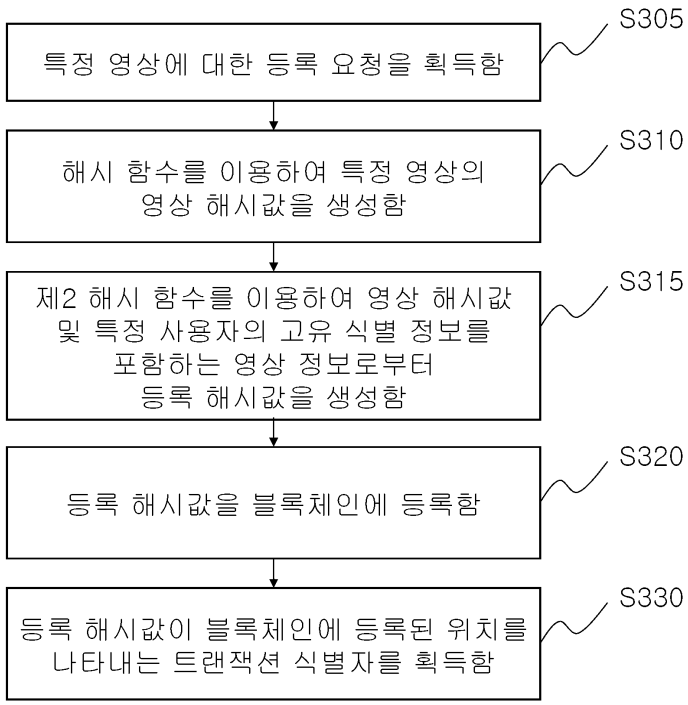
도면1



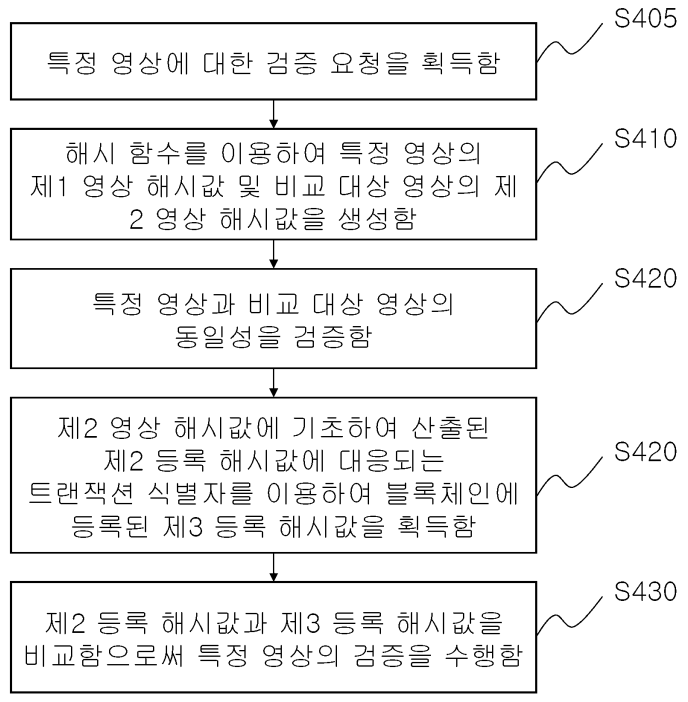
도면2



도면3


특정 영상에 대한 등록 요청을 획득함
S305
해시 함수를 이용하여 특정 영상의 영상 해시값을 생성함
S310
제2 해시 함수를 이용하여 영상 해시값 및 특정 사용자의 고유 식별 정보를 포함하는 영상 정보로부터 등록 해시값을 생성함
S315
등록 해시값을 블록체인에 등록함
S320
등록 해시값이 블록체인에 등록된 위치를 나타내는 트랜잭션 식별자를 획득함
S330

도면4


특정 영상에 대한 검증 요청을 획득함
S405
해시 함수를 이용하여 특정 영상의 제1 영상 해시값 및 비교 대상 영상의 제2 영상 해시값을 생성함
S410
특정 영상과 비교 대상 영상의 동일성을 검증함
S420
제2 영상 해시값에 기초하여 산출된 제2 등록 해시값에 대응되는 트랜잭션 식별자를 이용하여 블록체인에 등록된 제3 등록 해시값을 획득함
S420
제2 등록 해시값과 제3 등록 해시값을 비교함으로써 특정 영상의 검증을 수행함
S430

도면5