(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0131702
(43) 공개일자 2020년11월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *G06F 16/901* (2019.01)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/0643 (2013.01)
G06F 16/901 (2019.01)
(21) 출원번호 10-2019-0056639
(22) 출원일자 2019년05월14일
심사청구일자 2019년05월14일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
이범식
광주광역시 남구 제석로80번길 5, 102동 903호
사랄라 기미레
광주광역시 동구 지호로 16, 301호
(74) 대리인
허용록

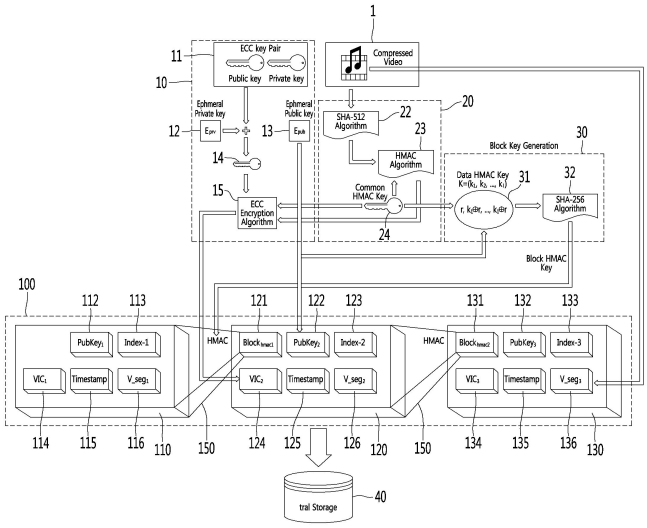
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **블럭체인장치, 블럭체인제공장치, 블럭체인화방법, 및 블럭체인의 데이터구조**

(57) 요 약

본 발명에 따른 블럭체인제공장치에는, 디지털 정보를 암호화하는 정보암호화부; 상기 정보암호화부의 암호화에 사용된 키를 암호화하는 키암호화부; 블럭체인에 포함되는 블럭의 생성에 사용되는 블럭키를 생성하는 블럭키 생성부; 및 상기 블럭체인에 포함되는 현재블럭을 생성할 때, 상기 블럭키를 이용하여 상기 현재블럭의 이전에 있는 블럭의 정보를 암호화하여, 상기 현재블럭에 저장하는 블럭작용부가 포함된다.

대 표 도



(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/0894 (2013.01)
H04L 9/3066 (2013.01)
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711073388
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	SW중심대학
연구과제명	SW중심대학(조선대)
기 여 율	1/1
과제수행기관명	조선대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

디지털 정보를 암호화하는 정보암호화부;

상기 정보암호화부의 암호화에 사용된 키를 암호화하는 키암호화부;

블럭체인에 포함되는 블럭의 생성에 사용되는 블럭키를 생성하는 블럭키 생성부; 및

상기 블럭체인에 포함되는 현재블럭을 생성할 때, 상기 블럭키를 이용하여 상기 현재블럭의 이전에 있는 블럭의 정보를 암호화하여, 상기 현재블럭에 저장하는 블럭작용부가 포함되는 블럭체인제공장치.

청구항 2

제 1 항에 있어서,

상기 블럭키는 상기 정보암호화부의 암호화에 사용된 키를 사용하는 블럭체인제공장치.

청구항 3

제 1 항에 있어서,

상기 이전블럭의 정보는 해쉬되어 상기 현재블럭에 포함되는 블럭체인제공장치.

청구항 4

제 1 항에 있어서,

상기 키 암호화부는,

상기 정보암호화부의 암호화에 사용된 키, 및 상기 정보암호화부에서 암호화된 메시지인증코드를, 함께 암호화하는 블럭체인제공장치.

청구항 5

제 1 항에 있어서,

상기 키 암호화부는 타원곡선암호화방식으로 암호화하는 블럭체인제공장치.

청구항 6

제 1 항에 있어서,

상기 정보암호화부에는,

상기 디지털 정보를 암호화하여 상기 디지털 정보의 해쉬데이터을 제공하는 제 1 정보암호화부; 및

공통키를 이용하여 상기 디지털 정보의 해쉬데이터에 대한 메시지인증코드를 제공하는 제 2 정보암호화부가 포함되는 블럭체인제공장치.

청구항 7

제 6 항에 있어서,

상기 제 1 정보암호화부는 SHA-512 알고리즘을 이용하여 해쉬하는 블럭체인제공장치.

청구항 8

제 6 항에 있어서,

상기 키 암호화부에는,

메인개인키/메인공개키 페어; 및

상기 해쉬데이터, 및 상기 메시지인증코드를 함께, 소정의 비밀키를 이용하요 암호화하여 인증코드를 출력하는 타원곡선암호화부가 포함되는 블럭체인제공장치.

청구항 9

제 8 항에 있어서,

상기 비밀키는, 상기 메인개인키/메인공개키 패어에서 공급되는 메인공개키와 일시 개인키로부터 산출되는 블럭체인제공장치.

청구항 10

제 8 항에 있어서,

상기 키 암호화부는 일시 공개키를 상기 현재블럭에 제공되는 블럭체인제공장치.

청구항 11

제 10 항에 있어서,

상기 블럭키 생성부에는,

상기 일시 공개키를 시드값으로 상기 공통키를 랜덤해쉬한 해쉬데이터를 출력하는 제 1 블럭키 암호화부; 및

상기 해쉬데이터를 이용하여 상기 블럭키를 출력하는 제 2 블럭키 암호화부가 포함되는 블럭체인제공장치.

청구항 12

제 1 항에 있어서,

상기 블럭작용부는,

상기 블럭키를 이용하여 시계열 상으로 상기 현재블럭의 앞에 있는 블럭의 정보를 해쉬하여 해쉬값을 상기 현재블럭에 저장하는 블럭체인제공장치.

청구항 13

제 1 항에 있어서,

상기 블럭작용부는,

상기 블럭체인에 포함되는 현재블럭을 생성할 때, 상기 블럭키를 이용하여 상기 현재블럭의 직근 이전에 있는 블럭의 정보를 암호화하여, 상기 현재블럭에 저장하는 블럭체인제공장치.

청구항 14

디지털 정보의 각 세그먼트의 암호화에 사용되는 공통키를 해쉬하여 제공되는 블럭키를 이용하여, 각 블럭을 생성하는 블럭체인제공장치; 및

상기 블럭체인제공장치에 의해서 제공되는 블럭체인을 저장하는 메모리가 포함되는 블럭체인장치.

청구항 15

제 14 항에 있어서,

상기 블럭키는, 현재 생성되는 블럭의 이전에 있는 블럭의 정보를 해쉬하는 키값으로 사용되고, 해쉬된 해쉬값은 현재 생성되는 블럭에 저장되는 블럭체인장치.

청구항 16

제 14 항에 있어서,

상기 메모리는 단일의 중앙저장소인 블럭체인장치.

청구항 17

블럭이 연결되는 블럭체인의 데이터구조이고,

상기 블럭에는, 적어도 하나의 현재블럭, 및 시계열 상으로 상기 현재블럭의 앞에 놓이는 이전블럭이 포함되고,

상기 현재블럭에는,

상기 이전블럭의 해쉬값(Blockhmac), 상기 현재블럭을 위한 일시적 공개키(Ephemral public key), 상기 현재블럭의 색인(Index), 상기 현재블럭의 암호화 키값(VIC: Video Integrity Code), 상기 현재블럭을 위한 비디오 세그먼트(V_seg), 및 상기 현재블럭의 비디오 세그먼트를 위한 타임 스탬프(Timestamp)가 포함되는 블럭체인의 데이터구조.

청구항 18

제 17 항에 있어서,

상기 이전블럭이 상기 블럭체인의 가장 앞에 놓이는 블럭인 경우에는, 해당하는 이전블럭이 생성되는 시점을 이전이라고 할 때,

이전 시점의 일시적 공개키(Ephemral public key), 상기 이전블럭의 색인(Index), 상기 이전블럭의 암호화 키값(VIC: Video Integrity Code), 상기 이전블럭을 위한 비디오 세그먼트(V_seg), 및 상기 이전블럭의 비디오 세그먼트를 위한 타임 스탬프(Timestamp)가 포함되는 블럭체인의 데이터구조.

청구항 19

제 17 항에 있어서,

상기 이전블럭의 해쉬값은, 각 블럭마다 다른 블럭키가 이전블럭의 해쉬를 위한 키값으로 사용되는 블럭체인의 데이터 구조.

청구항 20

블럭화 작용이 수행되는 현재블럭의 앞에 있는 어느 블럭의 정보가 해쉬되는 키값으로 블럭키를 사용하는 것; 및

상기 어느 블럭의 정보가 해쉬된 해쉬값은 상기 현재블럭에 저장되는 것이 포함되고,

상기 블럭키는 ,디지털 정보의 각 세그먼트의 암호화에 사용되는 공통키를 해쉬하여 제공되는 블럭체인화방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 데이터를 블럭체인에 기반하여 저장하는 장치, 방법, 및 데이터 구조에 관한 것이다.

배 경 기 술

[0002] 일반적인 의미에서 블럭체인은, 노드 상호 간의 트랜잭션으로 생성된 데이터가, 블럭들이 체인(chain) 형태로 연결되어 모인 것을 의미한다. 상기 블럭체인은, 이전블럭에 다음 블럭을 연이어 암호화하고, 과반수가 넘는 사용자가 동의한 데이터를 실제 데이터로 인정하기 때문에, 한번 기록된 데이터는 위조 또는 변조가 불가능하다.

[0003] 블럭체인의 대표적인 응용사례는 암호화폐의 거래 과정을 기록하는 분산화된 전자 화폐인 비트코인(bitcoin)이 있다.

[0004] 한편, 전자기술의 발달로 인하여 디지털 데이터의 위조 및 변조가 가능한 영역이 확대됨과 함께, 법원에 제출되는 디지털 증거자료의 증거능력을 확인할 수 있는 방법에 대한 수요가 증가하고 있다. 상기 디지털 증거자료는 극히 작은 일 부분이라도 위조 또는 변조가 되면, 증거능력이 상실되는 특징이 있다.

[0005] 데이터의 위조 및 변조를 검증하는 기술 예로는 서버에 저장되는 데이터를 블럭체인으로 저장하는 공개특허 10-2018-0089682, 블럭체인 기반의 데이터의 무결성을 검증하는 전자 장치 및 방법이 있다. 상기 종래기술에도 불

구하고, 상기 디지털 증거자료의 위조 및 변조를 방지하고 이를 검증하는 기술의 발전은 더디기만 하다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 공개특허 10-2018-0089682, 블럭체인 기반의 데이터의 무결성을 검증하는 전자 장치 및 방법

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기되는 배경에서 제안되는 것으로서, 디지털 증거자료의 위조 또는 변조를 정확하게 검증할 수 있는 블럭체인장치, 블럭체인제공장치, 블럭체인화방법, 및 블럭체인의 데이터구조를 제안한다.

[0008] 본 발명은, 하나의 디지털 증거자료 중의 극히 작은 부분이라도 위조 또는 변조가 불가능한 블럭체인장치, 블럭체인제공장치, 블럭체인화방법, 및 블럭체인의 데이터구조를 제안한다.

과제의 해결 수단

[0009] 본 발명에 따른 블럭체인제공장치에는, 디지털 정보를 암호화하는 정보암호화부; 상기 정보암호화부의 암호화에 사용된 키를 암호화하는 키암호화부; 블럭체인에 포함되는 블럭의 생성에 사용되는 블럭키를 생성하는 블럭키 생성부; 및 상기 블럭체인에 포함되는 현재블럭을 생성할 때, 상기 블럭키를 이용하여 상기 현재블럭의 이전에 있는 블럭의 정보를 암호화하여, 상기 현재블럭에 저장하는 블럭작용부가 포함된다. 본 발명에 따르면 시계열로 구분되는 각 블럭에 저장되는 디지털 데이터의 위변조를 방지할 수 있고, 증거자료의 위변조사실을 검증할 수 있다.

[0010] 상기 블럭키는 상기 정보암호화부의 암호화에 사용된 키를 사용함으로써, 단일의 암호화된 키를 반복하여 사용할 수 있으므로 엔코딩과 검증의 시간이 줄어들고, 메모리를 작게 차지할 수 있다.

[0011] 상기 이전블럭의 정보는 해쉬되어 상기 현재블럭에 포함됨으로써, 암호화의 성능을 더 높일 수 있다.

[0012] 상기 키 암호화부는, 상기 정보암호화부의 암호화에 사용된 키, 및 상기 정보암호화부에서 암호화된 메시지인증코드를, 함께 암호화함으로써, 프로세싱 시간을 줄일 수 있고, 위변조의 가능성을 더욱 감소시킬 수 있다.

[0013] 상기 키 암호화부는 타원곡선암호화방식으로 암호화함으로써, 더 다양한 암호를 만들어 낼 수 있고, 데이터 처리시간을 줄이고, 키 값이 늘어나는 것에 대한 부담이 크게 줄어들 수 있다.

[0014] 상기 정보암호화부에는, 상기 디지털 정보를 암호화하여 상기 디지털 정보의 해쉬데이터을 제공하는 제 1 정보암호화부; 및 공통키를 이용하여 상기 디지털 정보의 해쉬데이터에 대한 메시지인증코드를 제공하는 제 2 정보암호화부가 포함된다. 이에 따르면, 더 어려운 암호를 만들어 낼 수 있다.

[0015] 상기 제 1 정보암호화부는 SHA-512 알고리즘을 이용하여 높은 수준의 보안을 구현할 수 있다.

[0016] 상기 키 암호화부에는, 메인개인키/메인공개키 페어; 및 상기 해쉬데이터, 및 상기 메시지인증코드를 함께, 소정의 비밀키를 이용하여 암호화하여 인증코드를 출력하는 타원곡선암호화부가 포함되어, 복제가 어려운 암호화키를 생성할 수 있다.

[0017] 상기 비밀키는, 상기 메인개인키/메인공개키 페어에서 공급되는 메인공개키와 일시 개인키로부터 산출되어, 더 어려운 암호화를 위한 키를 제공할 수 있다.

[0018] 상기 키 암호화부는 일시 공개키를 상기 현재블럭에 제공하여, 검증 시에 신속하게 사용하도록 할 수 있다.

[0019] 상기 블럭키 생성부에는, 상기 일시 공개키를 시드값으로 상기 공통키를 랜덤해쉬한 해쉬데이터를 출력하는 제 1 블럭키 암호화부; 및 상기 해쉬데이터를 이용하여 상기 블럭키를 출력하는 제 2 블럭키 암호화부가 포함된다. 이에 따르면, 공통키로부터 생성되는 블럭키를 제공하여 이를 블럭작용부의 키값으로 사용하여, 더 안전하게 신속한 디지털처리가 가능하다.

[0020] 상기 블럭작용부는, 상기 블럭키를 이용하여 시계열 상으로 상기 현재블럭의 앞에 있는 블럭의 정보를 해쉬하여

해쉬값을 상기 현재블럭에 저장한다. 이에 따르면 이전블럭의 정보를 현재블럭의 정보로서 포함할 수 있기 때문에, 위변조가 불가능해진다.

[0021] 상기 블럭작용부는, 상기 블럭체인에 포함되는 현재블럭을 생성할 때, 상기 블럭키를 이용하여 상기 현재블럭의 직근 이전에 있는 블럭의 정보를 암호화하여, 상기 현재블럭에 저장할 수 있다. 이에 따르면, 현재블럭과 이전블럭이 시계열로 서로 붙어 있기 때문에 신속하게 디지털 정보를 검증할 수 있다.

[0022] 본 발명의 블럭체인장치에는, 디지털 정보의 각 세그먼트의 암호화에 사용되는 공통키를 해쉬하여 제공되는 블럭키를 이용하여, 각 블럭을 생성하는 블럭체인제공장치; 및 상기 블럭체인제공장치에 의해서 제공되는 블럭체인을 저장하는 메모리가 포함된다. 본 발명에 따르면, 블럭키를 활용하여 블럭의 정보를 위변조로부터 보호할 수 있다.

[0023] 상기 블럭키는, 현재 생성되는 블럭의 이전에 있는 블럭의 정보를 해쉬하는 키값으로 사용되고, 해쉬된 해쉬값은 현재 생성되는 블럭에 저장된다. 이에 따르면, 블럭간에 서로 정보를 공유하여 더 안전하게 증거자료로서 활용하는 디지털 정보를 보호할 수 있다.

[0024] 상기 메모리는 단일의 중앙저장소가 됨으로써, 증거자료로서의 활용성을 더욱 높일 수 있다.

[0025] 본 발명에 따른 블럭체인의 데이터구조는, 블럭이 연결되는 블럭체인의 데이터구조이고, 상기 블럭에는, 적어도 하나의 현재블럭, 및 시계열 상으로 상기 현재블럭의 앞에 놓이는 이전블럭이 포함되고, 상기 현재블럭에는, 상기 이전블럭의 해쉬값(Blockhmac), 상기 현재블럭을 위한 일시적 공개키(Ephemral public key), 상기 현재블럭의 색인(Index), 상기 현재블럭의 암호화 키값(VIC: Video Integrity Code), 상기 현재블럭을 위한 비디오 세그먼트(V_seg), 및 상기 현재블럭의 비디오 세그먼트를 위한 타임 스탬프(Timestamp)가 포함된다. 본 발명에 따르면, 외부의 위변조에 강건한 증거자료를 얻을 수 있다. 물론, 위변조가 된 사실의 검증을 신속하게 수행할 수도 있다.

[0026] 상기 이전블럭이 상기 블럭체인의 가장 앞에 놓이는 블럭인 경우에는, 해당하는 이전블럭이 생성되는 시점을 이전이라고 할 때, 이전 시점의 일시적 공개키(Ephemral public key), 상기 이전블럭의 색인(Index), 상기 이전블럭의 암호화 키값(VIC: Video Integrity Code), 상기 이전블럭을 위한 비디오 세그먼트(V_seg), 및 상기 이전블럭의 비디오 세그먼트를 위한 타임 스탬프(Timestamp)가 포함된다. 이에 따르면, 이전블럭에 대해서도 암호화가 수행되어 보호할 수 있다.

[0027] 상기 이전블럭의 해쉬값은, 각 블럭마다 다른 블럭키가 이전블럭의 해쉬를 위한 키값으로 사용됨으로써, 안전하게 디지털 증거자료를 블럭체인으로 보호할 수 있다

[0028] 본 발명에 따른 블럭체인화방법에는, 블럭화 작용이 수행되는 현재블럭의 앞에 있는 어느 블럭의 정보가 해쉬되는 키값으로 블럭키를 사용하는 것; 및 상기 어느 블럭의 정보가 해쉬된 해쉬값은 상기 현재블럭에 저장되는 것이 포함되고, 상기 블럭키는 ,디지털 정보의 각 세그먼트의 암호화에 사용되는 공통키를 해쉬하여 제공되는 것을 특징으로 한다. 이에 따르면, 블럭체인을 통하여 디지털 정보인 증거자료를 위변조로부터 안전하게 보호하고, 위변조 사실을 편리하게 검증할 수도 있다.

발명의 효과

[0029] 본 발명에 따르면, 디지털 증거자료의 위조 또는 변조를 정확하게 검증할 수 있고, 이에 따라서, 하나의 디지털 증거자료 중의 극히 작은 부분이라도 위조 또는 변조가 불가능한 장점이 있다.

[0030] 본 발명에 따르면, 신속하게 암호화처리를 수행하고, 적은 용량의 메모리로 암호화를 수행할 수 있다.

[0031] 본 발명에 따르면, 대용량의 디지털 증거자료를 안전하게 보호할 수 있다.

도면의 간단한 설명

[0032] 도 1은 실시예에 따른 블럭체인장치를 개시하는 도면.

도 2는 실시예의 블럭체인장치에서 위변조가 불가능한 이유를 보이는 도면.

도 3과 도 4는 타원곡선암호화방식과 리베스트셰미르아델만방식(RSA: Rivest Shamir Adleman)의 성능을 비교하는 도면.

도 5는 다수의 비디오 스트림을 블럭체인화 된 경우와 블럭체인화 되지 않은 경우의 러닝타임을 비교하는 그래

프.

도 6은 위변조된 블럭이 있는 경우와 위변조된 블럭이 없는 경우에 블럭체인의 크기를 변경하며 엔코딩시간을 보이는 그래프.

발명을 실시하기 위한 구체적인 내용

[0033] 이하에서는 도면을 참조하여 본 발명의 구체적인 실시예를 상세하게 설명한다. 다만, 본 발명의 사상은 이하에 제시되는 실시예에 제한되지 아니하고, 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위 내에 포함되는 다른 실시예를 구성요소의 부가, 변경, 삭제, 또는 추가에 의해서 용이하게 제안할 수 있을 것이나 이 또한 본 발명의 사상에 포함된다고 할 것이다.

[0034] 본 문서에 개시되는 증거자료에는, 오디오, 비디오, 및 이미지의 디지털 증거자료가 바람직하게 포함될 수 있다. 상기 디지털 증거자료는 일정한 시간, 예를 들어, 한 두 시간 분량으로 저장되는 디지털 데이터일 수 있다. 이들 디지털 증거자료는, 데이터의 용량이 큰 특성, 연속적인 특성, 디지털 처리로 위조 또는 변조(이하, 위변조라고 한다)가 가능한 특성, 및 상기 디지털 증거자료가 발생한 시기부터 사용되는 시기까지 장시간 위변조없이 보존되고 검증되어야 하는 특성이 있다. 본 문서는 이들 특성에 적합한 블럭체인장치, 블럭체인제공장치, 블럭체인화방법, 및 블럭체인의 데이터구조를 개시한다.

[0035] 본 문서는 상기 디지털 증거자료에 더 바람직하게 적용될 수 있으나, 디지털 정보에 확장되어 그 검증 및 위변조의 불가능성을 이용할 수도 있다.

[0036] 본 문서에서 블럭체인은, 트랜잭션으로 생성된 데이터에 국한되지 않고, 독립된 노드에서 제공되는 데이터가, 블럭들이 체인 형태로 연결되어 모인 것을 포함할 수 있다.

[0037] 본 문서에서 현재, 이전, 및 다음의 의미는, 절대적인 시간의 흐름을 의미하는 것이 아니라, 블럭체인에 포함되는 현재의 어느 시점인 현재블럭을 중심으로 하여, 이전블럭 및 다음블럭의 시점을 지칭하는 것으로 이해할 수 있다.

[0038] 본 문서는, 비디오를 예로 들어 설명하지만, 오디오, 및 이미지 등과 같은 다른 디지털 정보도 포함될 수 있다. 이하의 설명에서 비디오라고 지칭된 부분은, 비디오, 오디오, 및 이미지 등과 같은 디지털 정보로 바꾸어 읽을 수 있다.

[0039] 도 1은 실시예에 따른 블럭체인장치를 개시한다.

[0040] 도 1을 참조하여 상기 블럭체인장치를 개략적으로 설명한다. 상기 블럭체인장치에는, 적어도 어느 하나의 디지털 정보의 블럭체인이 저장되는 메모리(40), 상기 메모리에 저장되는 상기 블럭체인을 생성하는 블럭체인제공장치가 포함된다.

[0041] 상기 블럭체인제공장치에는, 저장정보(1)를 해쉬하는 정보암호화부(20), 정보 암호화에 사용되는 키를 암호화하는 키암호화부(10), 블럭체인의 생성에 사용되는 블럭키를 생성하는 블럭키 생성부(30), 상기 블럭키 생성부에서 생성되는 블럭키를 키값으로 이전블럭의 정보를 해쉬하는 블럭작용부(150)가 포함될 수 있다.

[0042] 상기 블럭작용부(150)에서는, 이전블럭의 정보가 해쉬되어 현재블럭에 수록되는 블럭체인화방법이 수행될 수 있다. 상기 블럭체인화방법이 수행될 때, 해쉬를 위한 키값으로는 현재블럭에 포함되는 정보로부터 추출되는 블럭키(Block HMAC key)가 사용될 수 있다. 상기 블럭키는 각 블럭마다 다를 수 있다. 상기 이전블럭의 해쉬값(Blockhmac)은 상기 현재블럭에 저장될 수 있다.

[0043] 상기 블럭체인화방법에 따르면, 상기 이전블럭의 정보가 위변조되더라도, 상기 현재블럭에 저장되는 상기 이전블럭의 해쉬값(Blockhmac)을 위변조할 수는 없다. 따라서, 이전블럭의 정보가 위변조된 사실을 검증할 수 있다.

[0044] 상기 블럭체인제공장치에 의해서 제공되는 블럭체인은 도면번호 100으로 표시하였다. 상기 블럭체인(100)은 세 개의 블럭이 연결되는 것으로 도시되었으나, 디지털 정보의 용량에 따라서 더 많은 블럭이 연결될 수 있다.

[0045] 상기 블럭체인에 연결되는 각 블럭은 상기되는 블럭체인화방법에 의해서, 본 문서에서 개시되는 위변조가 불가능한 데이터 구조를 가질 수 있다.

[0046] 실시예에 따른 블럭체인의 데이터 구조는, 블럭체인 상에 연결되는 각각의 블럭들은, 저장정보가 처리되는 순서에 따라서 서로 관계를 가질 수 있다. 이때, 저장정보가 처리되는 순서는 바람직하게 시계열 순서를 예시할 수 있다. 예를 들어, 비디어 정보가 처리되는 시간에 따라서, 현재시간의 비디오 정보는 현재블럭에 저장되고, 이

전시간의 비디오 정보는 이전블럭에 저장될 수 있다. 이때 상기 이전블럭은 상기 현재블럭의 직전에 놓이는 블럭일 수 있다.

[0047] 상기 현재블럭에는, 상기 이전블럭의 해쉬값(Blockhmac), 현재시점의 일시적 공개키(Ephemral public key), 상기 현재블럭의 색인(Index), 상기 현재블럭의 암호화 키값(VIC: Video Integrity Code), 상기 현재블럭의 비디오 세그먼트(V_seg), 및 상기 현재블럭의 비디오 세그먼트를 위한 타임 스탬프(Timestamp)가 포함될 수 있다.

[0048] 상기 이전블럭의 그 이전에 다른 블럭이 있었던 경우에는, 상기 이전블럭에도 마찬가지의 데이터가 포함될 수 있다. 상기 현재블럭의 다음 시점에도 상기 현재블럭의 데이터가 포함될 수 있는 것은 당연하다.

[0049] 상기 저장정보(1)로는 상기 디지털 정보가 예시된다. 상기 디지털 정보는, 대용량으로 디지털 증거자료로서의 사용될 수 있는 비디오, 오디오, 및 이미지를 바람직하게 예시할 수 있다. 즉, 증거자료로 사용될 수 있는 디지털 정보가 실시예의 블럭체인으로 저장됨으로써, 어느 한 블럭이라도 위변조가 불가능하고 위변조가 일어나는 경우에는 위변조의 사실을 검증할 수 있다. 나아가서 위변조가 발생한 블럭을 정확하게 알아낼 수 있다.

[0050] 상기 증거자료로 사용되는 상기 디지털 정보는, 대용량이고 연속적이고 위변조에 취약한 특성이 있다. 따라서 실시예의 블럭체인장치에 바람직하게 적용될 수 있다. 상기 디지털 정보는 압축된 형태로 제공되어 용량이 줄어들도록 할 수 있다.

[0051] 상기 블럭체인제공장치를 더 상세하게 설명한다.

[0052] 상기 정보암호화부(20)는 상기 디지털 정보를 암호화하여 암호값을 제공할 수 있다. 상기 정보암호화부(20)에는, 상기 디지털 정보를 암호화하여 디지털 정보의 해쉬데이터을 제공하는 제 1 정보암호화부(22), 소정의 공통키(24)를 이용하여 상기 디지털 정보의 해쉬데이터에 대한 메시지인증코드(message authentification code)를 제공하는 제 2 정보암호화부(23)를 포함할 수 있다. 상기 디지털 정보는 각 세그먼트별로 각 블럭에 메칭될 수 있다.

[0053] 상기 제 1 정보암호화부(22)는 SHA(Secure Hash Algorithm)-512 알고리즘을 이용할 수 있다. 상기 SHA-512 알고리즘을 이용하여 상기 디지털 정보의 해쉬데이터를 제공할 수 있다. 상기 제 1 정보암호화부(22)는 SHA-256 알고리즘을 이용하여, 상기 디지털 정보의 해쉬데이터를 제공할 수도 있다.

[0054] 상기 제 2 정보암호화부(23)는 해쉬기반메시지인증코드(HMAC: Hash-based Message Authentification Code)에 의해서 상기 디지털 정보의 해쉬데이터에 대한 암호화가 수행될 수 있다. 상기 제 2 정보암호화부(23)의 암호화에 사용되는 상기 공통키(24)는 공통 해쉬기반메시지인증코드(HMAC: Hash-based Message Authentification Code) 키가 사용될 수 있다.

[0055] 상기 공통 해쉬기반메시지인증코드는 유일하지는 않지만, 어느 한 블럭에 저장되는 비디오 세그먼트 별로는 서로 다르다. 상기 제 2 정보암호화부(23)는 어느 하나의 비디오 세그먼트에 대한 유일한 메시지인증코드(MAC: Message Authentification Code)를 출력할 수 있다.

[0056] 상기 제 2 정보암호화부(23)는 상기 디지털 정보에 대한 메시지인증코드(MAC:Message Authentification Code)를 키암호화부(10)로 출력할 수 있다. 상기 공통키(24)는 상기 키암호화부(10) 및 상기 블럭키생성부(30)로 출력될 수 있다.

[0057] 상기 키암호화부(10)는 상기 공통키(24)를 타원곡선암호화방식(ECC:Ellipti cCurve Cryptography)을 이용하여 암호화할 수 있다. 실시예에서는 상기 타원곡선암호화의 확장형태인 타원곡선집약암호화방식(ECIES: Elliptic Curve integrated Cryptography Scheme)을 이용할 수 있다.

[0058] 상기 키암호화부(10)에는 메인개인키(main private key)/메인공개키(main public key) 페어(11)가 포함될 수 있다. 상기 메인개인키/메인공개키의 조합(11)에서 공급되는 메인공개키와 일시 개인키(Ephemeral private key)(12)로부터 비밀키(secret kwy)(14)가 생성될 수 있다. 상기 일시 개인키(12)로부터 일시 공개키(Ephemeral public key)(13)가 생성될 수 있다.

[0059] 상기 비밀키(14)는 타원곡선암호화부(15)에 의해서 암호화를 위한 키값으로 사용될 수 있다. 상기 타원곡선암호화부(15)는 상기 비밀키(14)를 이용하여, 상기 공통키(24)와 상기 메시지인증코드를 함께 암호화할 수 있다. 상기 타원곡선곡선암호화부(15)의 출력값은 비디오인증코드(VIC: Video Authentificaion Code)로서 대응하는 블럭에 저장될 수 있다.

[0060] 상기 블럭키 생성부(30)는 상기 공통키(24)를 이용하여 블럭체인에서 이전블럭의 HMAC에 대한 블럭 키값을 생성

할 수 있다. 상기 블럭키 생성부(30)에는, 제 1 블럭키 암호화부(31), 및 제 2 블럭키 암호화부(32)가 포함될 수 있다.

[0061] 상기 제 1 블럭키 암호화부(31)는, 상기 일시 공개키(13)를 시드값으로 이용하여, 상기 공통키(24)를 랜덤해쉬(randomly hashing)한, 상기 공통키에 대한 해쉬데이터를 상기 제 2 블럭키 암호화부(32)로 출력한다. 상기 제 2 블럭키 암호화부(32)는 SHA-526알고리즘이 사용될 수 있다.

[0062] 상기 제 2 블럭키 암호화부(32)는 블럭키(Block HMAC key)을 출력한다. 상기 블럭키는 블럭작용부(150)로 전달된다. 상기 블럭키 생성부에서 생성되는 블럭키를 키값으로 하여, 이전블럭의 정보를 해쉬하는 블럭작용부(150)가 포함될 수 있다.

[0063] 상기 블럭작용부(150)를 이용하여 블럭체인화방법을 설명한다.

[0064] 실시예에 따른 블럭체인화방법은, 상기 이전블럭의 정보를 해쉬하여 현재블럭에 저장할 수 있다. 이때 블럭작용을 위한 블럭키는, 현재블럭을 생성할 때 제공되는 정보를 이용하여 생성될 수 있다. 예를 들어, 상기 저장정보(1) 중에서 현재의 비디오 세그먼트, 현재의 공개키(24), 현재의 일시 공개키(13), 및 현재의 일시 개인키(12) 중의 적어도 하나를 이용하여 생성되는 값이다. 따라서 상기 블럭키는 블럭작용부(150)가 현재블럭을 생성할 때마다 달라질 수 있다.

[0065] 상기 블럭키를 키값으로 이용하여 이전블럭이 해쉬된 해쉬값(Blockhmac)은, 상기 현재블럭에 저장될 수 있다. 상기 이전블럭의 해쉬값은 메시지인증코드의 형식으로 주어질 수 있다. 상기 블럭체인(100)에는 제 1, 2, 및 3 블럭(110)(120)(130)이 도시된다. 상기 이전블럭이 해쉬된 해쉬값(Blockhmac)은, 이전블럭을 가지지 않는 제 1 블럭(110)에는 없고, 다른 블럭은 모두 가질 수 있다.

[0066] 상기 블럭체인화방법에 따르면, 현재블럭은 이전블럭을 검증할 수 있는 해쉬값을 포함할 수 있다. 이에 따라, 어느 하나의 현재블럭이 위변조되는 경우에는 다음 블럭을 이용하여 위변조사실을 알아낼 수 있다.

[0067] 상기 블럭체인의 데이터 구조를 설명한다.

[0068] 상기 블럭체인(100)의 각 블럭(110)(120)(130)에는, 현재블럭의 일시 공개키(Pubkey)(1112)(122)(132), 현재블럭의 비디오인증코드(VIC)(114)(124)(134), 현재블럭의 색인(Index)(113)(123)(133), 현재블럭의 비디오 세그먼트(V_seg)(116)(126)(136), 및 상기 현재블럭의 비디오 세그먼트에 부착되는 타임스탬프(Timestamp)(115)(125)(135)가 포함될 수 있다. 뿐만 아니라, 상기 이전블럭이 해쉬된 해쉬값(Blockhmac)(121)(131)을 가질 수 있다.

[0069] 상기 현재블럭과 시계열 상으로 대응되는 비디오 세그먼트는, 상기 현재블럭에 저장될 수도 있고, 상기 다음 블럭에 저장될 수도 있다.

[0070] 상기 비디오인증코드 및 상기 일시공개키(13)는 상기 키암호화부(10)에서 생성된 값이다. 상기 블럭키는 상기 블럭키 생성부(30)에서 생성된 값이다. 상기 일시공개키와 상기 비디오인증코드를 이용하여 정보를 해독할 수 있다.

[0071] 상기 블럭작용의 키값, 즉 블럭키는, 상기 블럭작용부(150)에서 블럭체인화방법의 수행 시에, 이전블럭의 정보가 해쉬될 때 해쉬를 위한 키값으로 사용될 수 있다. 상기 블럭작용의 키값을 이용하여 이전블럭의 정보가 해쉬되어, 블럭메시지인증코드(Blockhmac)로서 각 블럭에 저장될 수 있다.

[0072] 상기 이전블럭의 정보가 해쉬될 때, 현재블럭으로부터 추출한 블럭작용의 키값이 사용된다. 마찬가지로 현재블럭의 정보가 해쉬될 때, 다음 블럭으로부터 추출한 블럭작용의 키값이 사용된다. 이에 따르면, 가장 앞선 제 1 번 블럭을 제외하는 모든 현재블럭은, 그 현재블럭의 이전블럭의 정보를 검증할 수 있는 정보를 포함하는 것과 마찬가지이다.

[0073] 예를 들어, 이전블럭의 정보가 위변조되는 경우에는, 현재블럭의 블럭메시지인증코드와, 블럭작용의 키값을 이용하여 위변조된 이전블럭의 정보를 해쉬하여 재구성한 블럭메시지인증코드가, 서로 일치하지 않는다. 이때 블럭작용의 키값은 이전블럭으로 부터 추출한 값인 것에 유의하여야 한다.

[0074] 결국, 비록 어느 하나의 블럭의 암호를 알아내서 어느 하나의 블럭의 정보를 위변조하더라도, 다음 블럭의 블럭메시지인증코드를 이용하여 위변조사실을 알아낼 수 있다. 위변조를 하고자 하는 자는 모든 블럭의 암호를 알아내야만이 위변조가 가능하다. 모든 블럭의 위변조를 알아내는 것을 실질적으로 불가능하다.

[0075] 상기 블럭체인(100)의 정보는 단일의 중앙저장소인 메모리(40)에 저장될 수 있다. 실시예에 따른 블럭체인장치는, 블럭체인제공장치와 단일의 메모리(40)로 이루어질 수 있다. 이에 따르면, 폐쇄회로카메라로 촬영되는 증거영상을 실시간으로 계속해서 메모리에 저장하여, 촬영시부터 비디오의 위변조가 불가능한 상태로 제공될 수 있다. 촬영된 비디오의 디지털 정보는 엄정한 증거능력을 가지고 향후 사법재판에 증거로서 사용될 수 있다.

[0076] 본 문서에 따르면, 사법재판에서 큰 증거능력을 가지는 디지털 정보를 얻을 수 있다.

[0077] 도 2는 실시예의 블럭체인장치에서 위변조가 불가능한 이유를 설명하는 도면이다.

[0078] 도 2를 참조하면, 도 2(a)는 각 비디오 세그먼트(116)(126)(136)와 그 비디오 세그먼트를 이용하여 제 2 정보암호화부(23)로부터 추출되는 메시지인증코드(301)(302)(303)를 도시한다. 이때 많은 키(201)(202)(203)이 사용될 수 있다. 여기서 키는 공통키(24), 일시개인키(12), 및 일시공개키(13) 등이 포함될 수 있다.

[0079] 도 2(b)는, 상기 이전블럭의 정보를 상기 현재블럭을 이용하여 생성된 블럭키를 이용하여 이전블럭이 해쉬된 해쉬값(Blockhmac)(121)(131)을 더 도시한다.

[0080] 도 2(c)를 참조하면, 현재블럭에, 상기 키(402)가 유출되어 위변조가 되는 상태를 도시한다. 이때 상기 키(402)가 유출되어, 상기 메시지인증코드(502)가 올바르게 재생성되고(410), 저장된 메시지인증코드(302)와 동일할 수 있다. 이때에는 위변조가 검증되지 않을 수 있다(510).

[0081] 그러나, 다음 블럭에 있는 상기 이전블럭이 해쉬된 해쉬값(131)은 상기 다음 블럭의 정보가 참조되는 것이므로 검증이 불가능하다. 즉, 현재블럭만으로는 이전블럭의 해쉬된 해쉬값(131)을 생성하는 것이 불가능하므로(411), 검증단계를 통과할 수 없다(511). 비록 다음 블럭의 정보를 알아낼 수 있더라도, 비디오 정보를 위변조하기 위하여 블럭체인의 상당한 블럭의 키를 알아내는 것을 현실적으로 불가능하다.

[0082] 도 3과 도 4는 타원곡선암호화방식과 리베스트셰미르아델만방식(RSA: Rivest Shamir Adleman)의 성능을 비교하는 도면이다. 각 실험은 키의 크기를 변경하면서 암호/복호를 위한 실행시간과 보안비트레벨(security bit level)에 대하여 수행되었다.

[0083] 도 3을 참조하면, 종래 리베스트셰미르아델만방식에 비하여 상기 타원곡선암호화방식에 비하여 시간소모가 약간 더 높은 것을 확인할 수 있다.

[0084] 도 4를 참조하면, 종래 리베스트셰미르아델만방식과 상기 타원곡선암호화방식의 키의 크기차이는 보안비트레벨에 큰 차이를 초래한다. 따라서, 주어진 보안비트레벨에서 상기 타원곡선암호화방식에서는 더 작은 키의 크기가 요구되므로, 연산이 빨라지고, 전력소모가 낮고, 메모리 소모가 작은 장점이 있다.

[0085] 상기 도 3, 및 도 4의 결과에 비추어 볼 때, 상기 키암호화부(10)에서 타원곡선암호화방식을 사용한다는 사실은, 보안성과 효율성의 면에서 뛰어난 것을 의미하는 것을 알 수 있다.

[0086] 도 5는 다수의 비디오 스트림을 블럭체인화 된 경우와 블럭체인화 되지 않은 경우의 러닝타임을 비교하는 그래프이다. 본 실험은 H.264/AVC 비디오 코덱으로 실험대상인 길이가 다른 비디오를 압축하고, 그 압축스트림은 해쉬되어 블럭체인화 되었다. 검증과정은 동일한 과정이 반대로 수행되어 비트스트림으로 수행되었다.

[0087] 도 5를 참조하면, 블럭체인화 한 경우에는 블럭체인화 하지 않은 경우에 비하여, 약간의 엔코딩시간의 증가가 있는 것을 확인하였다. 증가한 시간은 블럭 및 키의 해쉬를 위하여 증가한 것으로 사료되지만, 예상가능한 수준으로서, 사용에 제한을 주지는 않는다. 검증의 경우에도 비슷한 정도의 시간증가가 있는 것을 확인할 수 있다.

[0088] 도 6은 위변조된 블럭이 있는 경우와 위변조된 블럭이 없는 경우에 블럭체인의 크기를 변경하며 엔코딩시간을 측정하는 그래프이다.

[0089] 도 6을 참조하면, 위변조된 블럭이 있는 경우에 약간(많아야 8ms)의 시간증가가 있는 것을 확인할 수 있었다. 이에 따르면, 실제 증거자료의 위변조를 검증할 수 있는 방법으로서 실시예에 따른 블럭체인장치, 블럭체인제공장치, 블럭체인화방법, 및 블럭체인의 데이터구조는 적용될 수 있는 수준인 것을 확인할 수 있다. 특히, 대용량의 연속적인 디지털 증거자료에 대하여 더 바람직하게 적용될 수 있다.

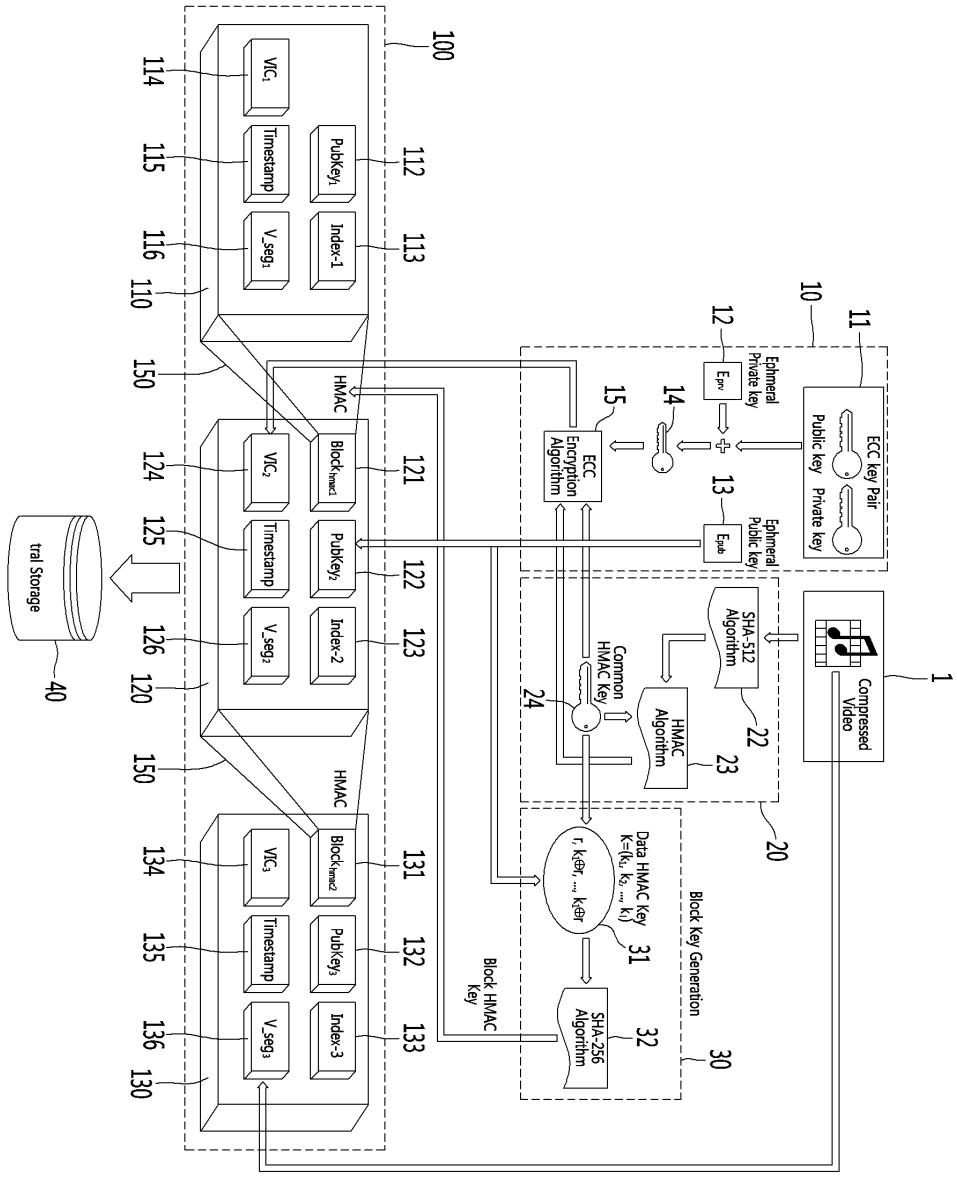
산업상 이용가능성

[0090] 본 발명은, 디지털 위변조기술의 발달에 따른 분쟁의 소지를 방지하고, 신뢰사회에 진입하는 일환으로서 작용할 수 있다. 특히, 비디오, 오디오, 및 이미지 등 디지털 정보의 발생시부터 위변조가 불가능하고, 대용량의 증거

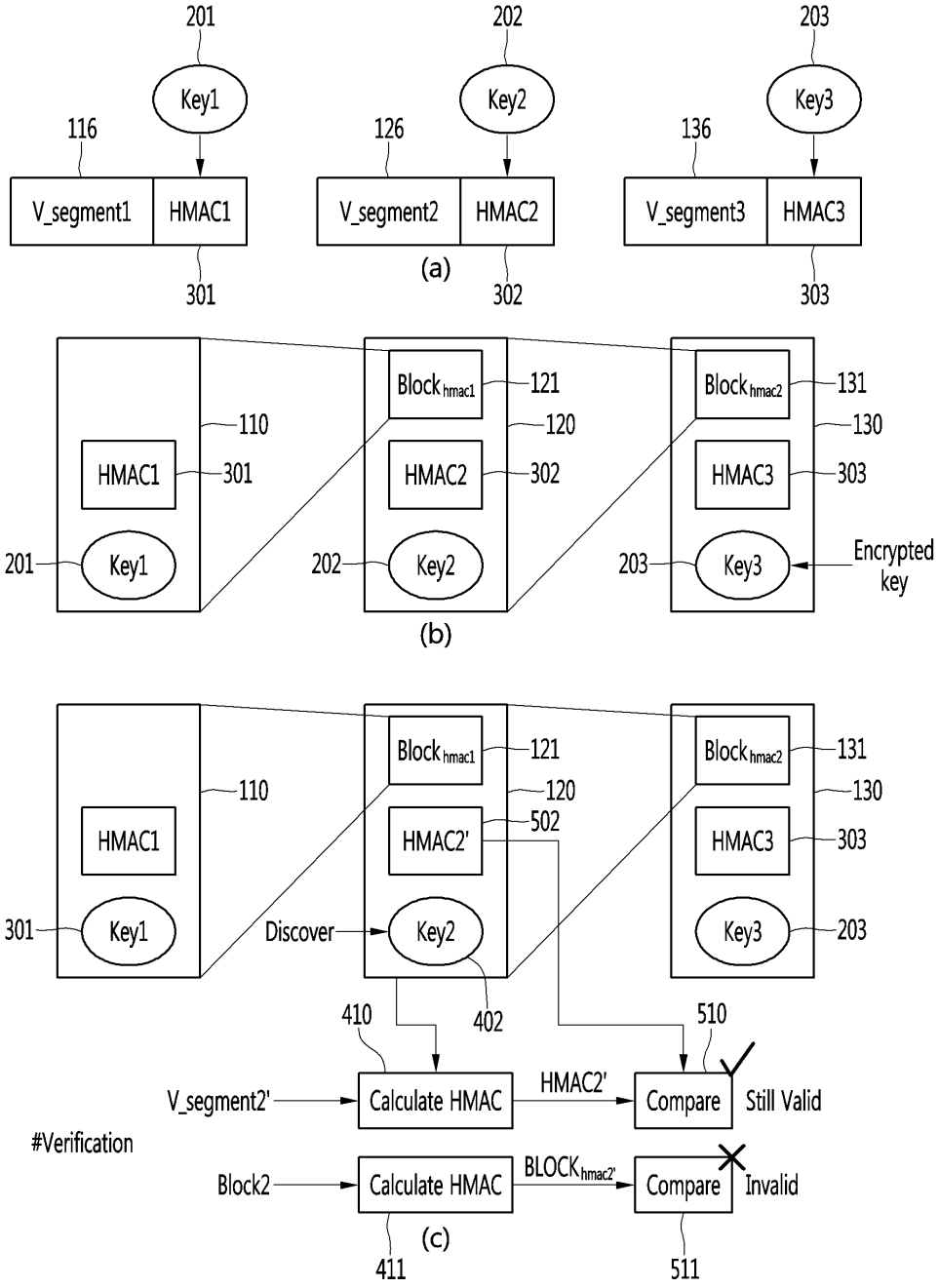
자료를 위변조가 불가능하게 보존할 수 있어서, 그 산업상의 적용이 크게 기대된다.

도면

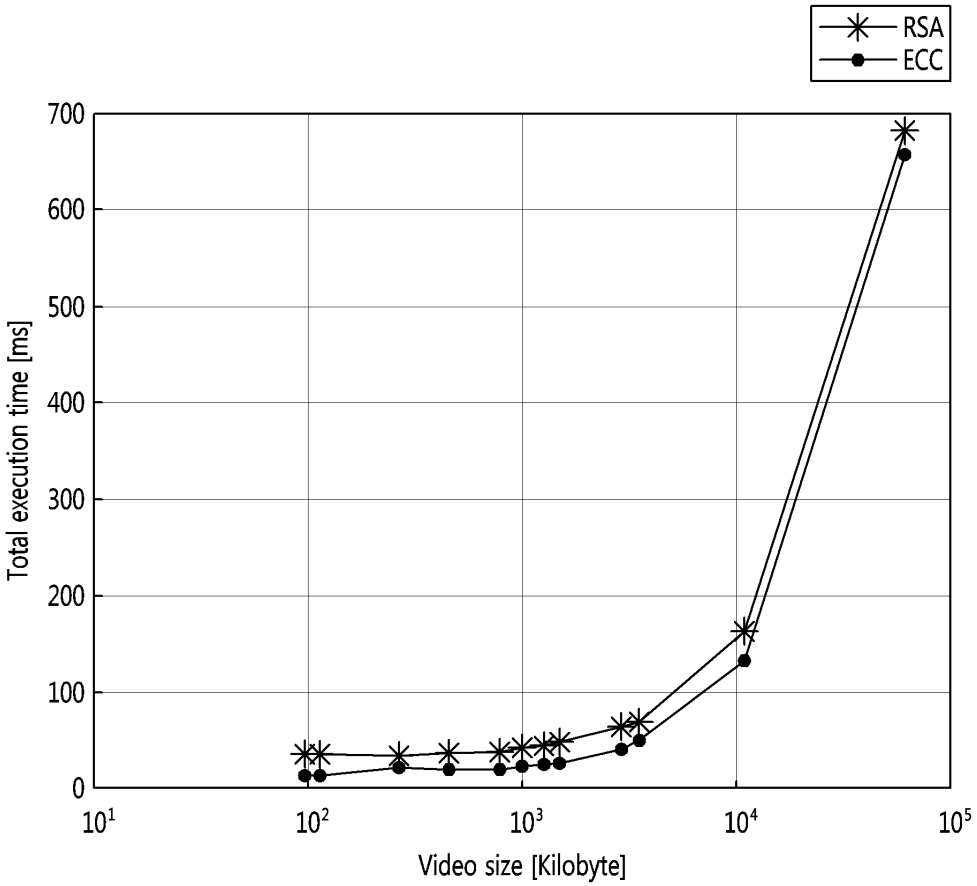
도면1



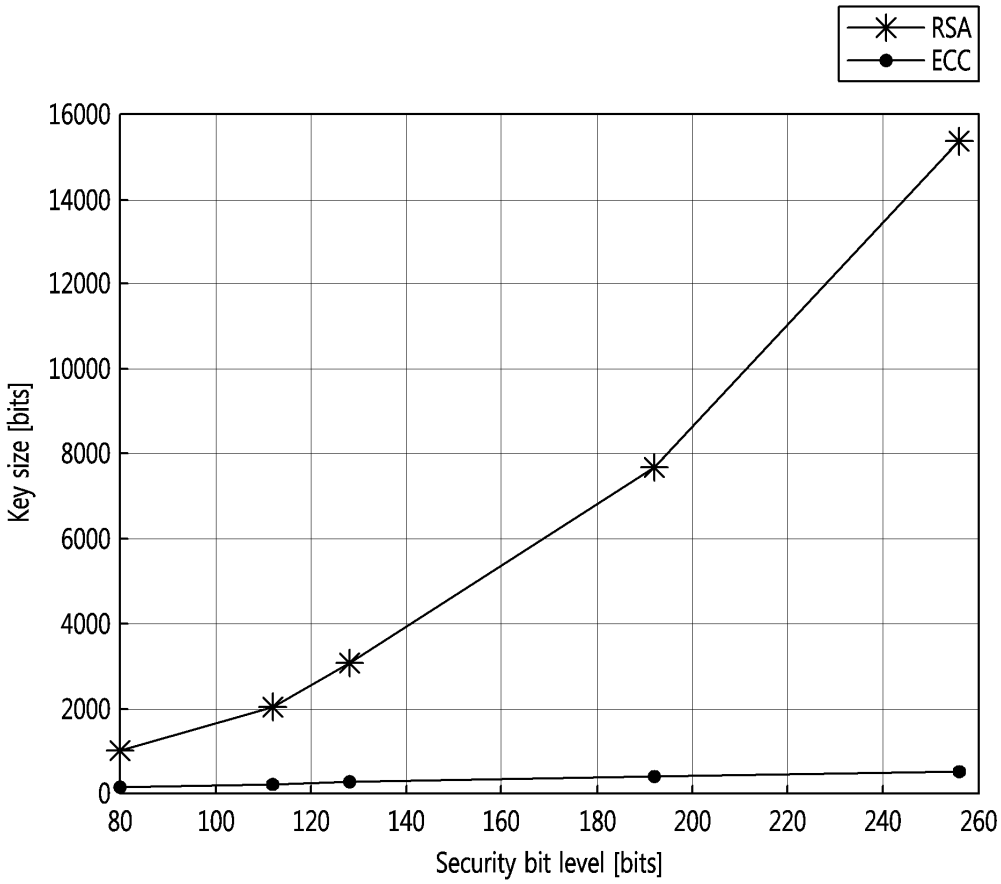
도면2


201
202
203
Key1
Key2
Key3
116
126
136
V_segment1
HMAC1
V_segment2
HMAC2
V_segment3
HMAC3
301
302
303
(a)
Block hmac1
Block hmac2
121
131
110
120
130
HMAC1
HMAC2
HMAC3
301
302
303
201
202
203
Key1
Key2
Key3
Encrypted key
(b)
HMAC2'
502
Discover
410
402
510
V_segment2'
Calculate HMAC
HMAC2'
Compare
Still Valid
#Verification
Block2
BLOCK hmac2'
Invalid
411
511
(c)

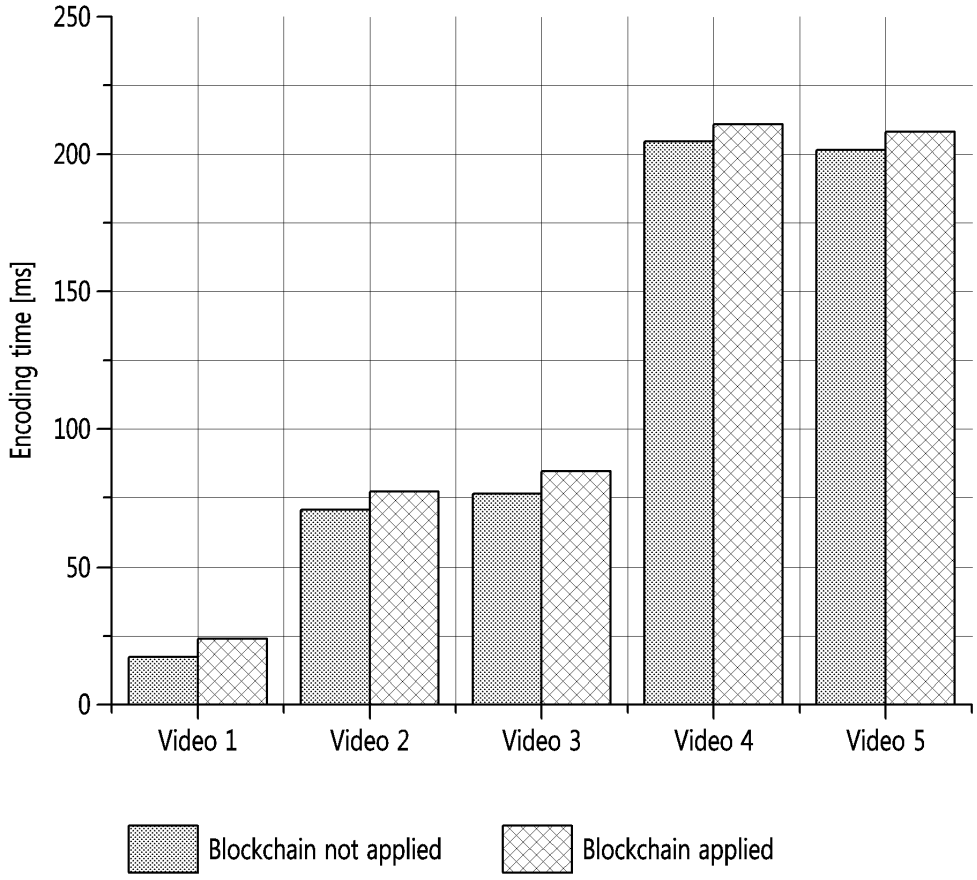
도면3


RSA
ECC
700
600
500
400
300
200
100
0
Total execution time [ms]
10^1
10^2
10^3
10^4
10^5
Video size [Kilobyte]

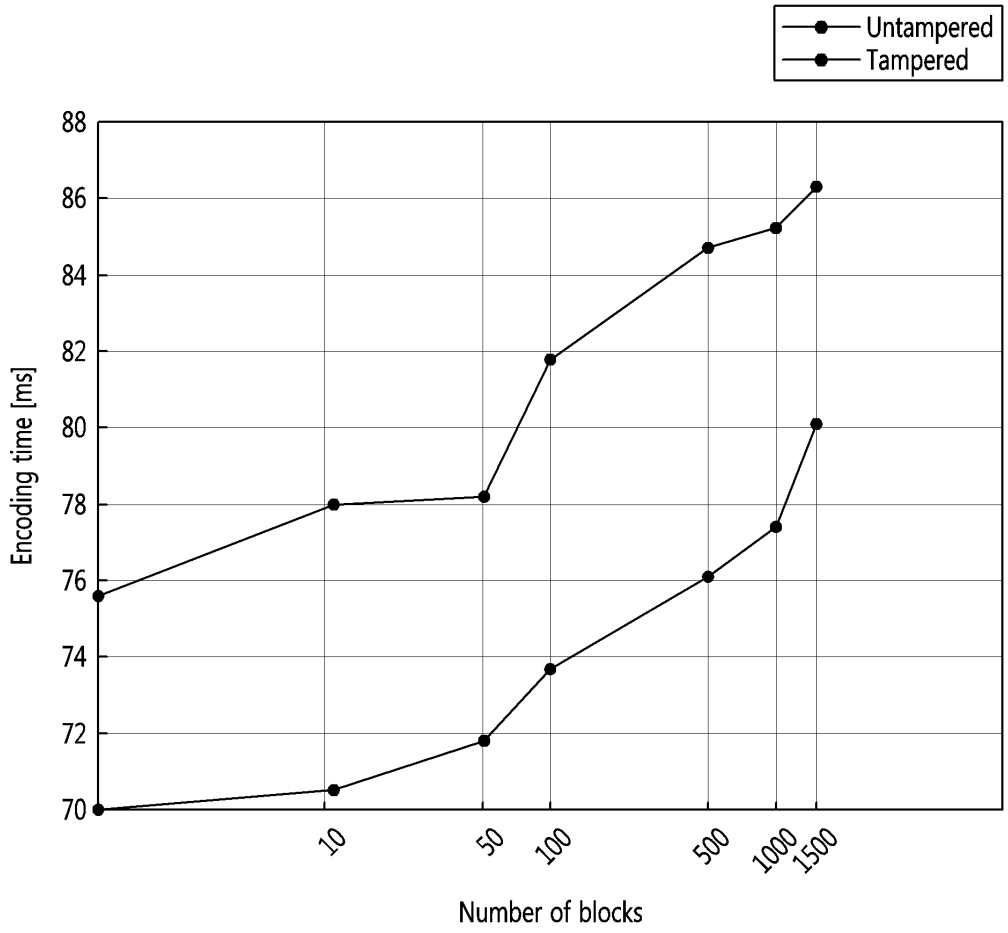
도면4


RSA
ECC
16000
14000
12000
10000
8000
6000
4000
2000
0
Key size [bits]
80
100
120
140
160
180
200
220
240
260
Security bit level [bits]

도면5


250
200
150
100
50
0
Encoding time [ms]
Video 1
Video 2
Video 3
Video 4
Video 5
Blockchain not applied
Blockchain applied

도면6


Untampered
Tampered
88
86
84
82
80
78
76
74
72
70
Encoding time [ms]
10
50
100
500
1000
1500
Number of blocks