



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0084954
(43) 공개일자 2021년07월08일

(51) 국제특허분류(Int. Cl.)
H04N 21/442 (2011.01) G06F 21/10 (2013.01)
G06F 21/30 (2013.01) H04L 9/32 (2006.01)
H04N 21/254 (2011.01)
(52) CPC특허분류
H04N 21/44236 (2013.01)
G06F 21/10 (2013.01)
(21) 출원번호 10-2019-0177502
(22) 출원일자 2019년12월30일
심사청구일자 2019년12월30일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
박승욱
인천광역시 남동구 아암대로1503번길 21, 1004동 3401호(논현동, 에코메트로10단지한화꿈에그린아파트)
(74) 대리인
양성보

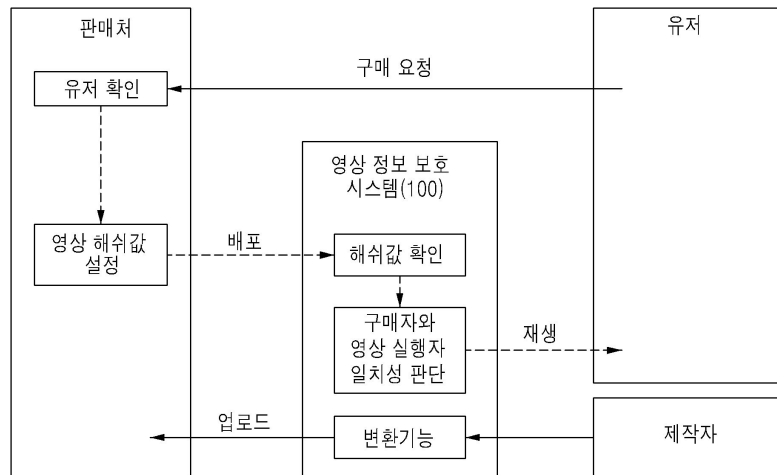
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 블록체인을 이용한 영상저작권 보호 방식

(57) 요약

블록체인을 이용한 영상저작권 보호 방식이 개시된다. 일 실시예에 따른 영상 정보 보호 시스템에 의해 수행되는 영상 정보 보호 방법은, 제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성하는 단계; 상기 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행하는 단계; 및 상기 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 상기 블록 체인화된 영상 정보를 재생하는 단계를 포함할 수 있다.

대표도



(52) CPC특허분류

G06F 21/30 (2013.01)

H04L 9/3236 (2013.01)

H04N 21/2541 (2013.01)

H04L 2209/38 (2013.01)

명세서

청구범위

청구항 1

영상 정보 보호 시스템에 의해 수행되는 영상 정보 보호 방법에 있어서,

제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성하는 단계;

상기 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행하는 단계; 및

상기 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 상기 블록 체인화된 영상 정보를 재생하는 단계를 포함하는 영상 정보 보호 방법.

청구항 2

제1항에 있어서,

상기 수행하는 단계는,

상기 생성된 블록 체인화된 영상 정보가 온라인 판매처 또는 오프라인 판매처에 등록됨에 따라 사용자에게 의하여 영상 정보에 대한 다운로드가 요청됨을 수신하는 단계

를 포함하고,

상기 생성된 블록 체인화된 영상 정보는, bluray Disk나 파일 형태, DVD, USB를 포함하는 저장 매체를 통해 등록되는

를 포함하는 영상 정보 보호 방법.

청구항 3

제2항에 있어서,

상기 블록 체인화된 영상 정보는, 사용자 정보에 대한 해쉬값 및 판매처 정보에 대한 해시값을 포함하고,

상기 수행하는 단계는,

상기 사용자로부터 상기 블록 체인화된 영상 정보에 대한 다운로드가 요청됨에 따라 상기 판매처로부터 생성된 제1 블록에 영상 정보의 해시값과 연결된 사용자의 해쉬값과 판매처의 해쉬값을 등록하는 단계

를 포함하는 영상 정보 보호 방법.

청구항 4

제2항에 있어서,

상기 수행하는 단계는,

상기 수신된 다운로드 요청에 따라 상기 블록 체인화된 영상 정보에 상기 사용자에게 대한 해쉬값을 설정하여 사용자에게 영상 정보를 배포하고, 상기 블록 체인화된 영상 정보에 대한 체인 정보, 영상 정보의 해쉬값을 판단하는 영상 정보의 인증을 수행하고, 상기 영상 정보의 인증을 완료함에 따라 상기 블록 체인화된 영상 정보에 설정된 해시값에 대응하는 사용자와 상기 프로그램을 실행하는 사용자에게 대한 사용자 인증을 수행하는 단계

를 포함하는 영상 정보 보호 방법.

청구항 5

제4항에 있어서,

상기 수행하는 단계는,

상기 블록 체인화된 영상 정보에 대한 체인 정보를 확인함에 따라 상기 블록 체인화된 영상 정보에 구성된 블록 정보의 연결 여부를 판단하고, 상기 블록 체인화된 영상 정보에 구성된 블록 정보가 정상적으로 연결되어 있을 경우, 상기 블록 체인화된 영상 정보 내의 블록과 프로그램을 실행하는 사용자의 일치 여부를 판단하는 단계

를 포함하는 영상 정보 보호 방법.

청구항 6

제5항에 있어서,

상기 수행하는 단계는,

상기 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자의 일치 여부를 판단하고, 판단 결과 일치하지 않을 경우, 상기 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자를 블랙 리스트에 등록하고, 판단 결과 일치할 경우, 영상 정보의 화면 녹화 프로그램을 감지하여 블록 체인화된 영상 정보의 재생을 결정하는 단계

를 포함하는 영상 정보 보호 방법.

청구항 7

영상 정보를 보호하기 위한 영상 정보 보호 시스템에 있어서,

컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성하고,

상기 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행하고,

상기 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 상기 블록 체인화된 영상 정보를 재생하는

영상 정보 보호 시스템.

발명의 설명

기술 분야

[0001] 아래의 설명은 영상저작권을 보호하는 기술에 관한 것이다.

배경 기술

[0003]블록체인은 중앙 시스템이 운영하는 것이 아닌 분산된 컴퓨팅 자원을 이용하므로 탈중앙화의 특징을 갖는다. 또한 블록체인은 네트워크 상에서 발생하는 모든 거래에 대하여 투명하게 관리할 수 있다. 모든 거래는 거래 발생 시점부터 추적이 가능하고, 누구나 공개된 거래 기록에 접근할 수 있으며 거래의 양성화와 규제 비용을 절감하는 효과를 얻을 수 있다. 또한 블록체인은 위변조가 불가능하다는 특징이 있다. 블록체인은 이전 블록의 정보를 이용하여 블록을 생성한다. 블록은 사슬처럼 모두 연결되어 있는 구조이기 때문에 블록의 특정 거래를 조작 하려면 이후에 생성된 모든 블록의 정보도 변경해야 한다. 블록체인 네트워크를 해킹하는 일은 사실상 불가능하기 때문에 위변조에 대한 가장 신뢰있는 기술이라고 평가받고 있다. 또한 블록체인은 확장성의 특징을 갖는다. 대부분의 블록체인 기술은 오픈소스 소프트웨어로 높은 확장성을 가지고 있다.

[0004]최근 다양한 콘텐츠 플랫폼이 성장하면서 기존 영화에서부터 최근에는 개인 창작물까지 영상 창작물이 많이 생겨나고 있다. 하지만, 이러한 창작물에 대한 저작권의 개념은 아직 부족한 현실이다. 이에 대한 가장 큰 피해자는 창작자이다. 과거 DRM(디지털 저작권 관리)이라는 기술이 적용된 수많은 창작물이 나왔지만 메모리 해킹

등 수많은 우회 방법이 제시가 되어 무용지물이 되었다. DRM기술은 디지털 콘텐츠를 사용하기 위해선 반드시 저작권자가 배포하는 라이선스를 발급 받아야 하는데, 이 라이선스만 해킹한다면 쉽게 이용이 가능하기 때문이다. 이에, 저작권 문제를 블록체인에 기반하여 해결하고자 하는 노력이 요구된다.

발명의 내용

해결하려는 과제

[0006] 블록체인 기술을 이용하여 영상 창작물의 불법 복제 및 불법 유통을 방지하는 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

[0008] 영상 정보 보호 시스템에 의해 수행되는 영상 정보 보호 방법은, 제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성하는 단계; 상기 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행하는 단계; 및 상기 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 상기 블록 체인화된 영상 정보를 재생하는 단계를 포함할 수 있다.

[0009] 상기 수행하는 단계는, 상기 생성된 블록 체인화된 영상 정보가 온라인 판매처 또는 오프라인 판매처에 등록됨에 따라 사용자에게 의하여 영상 정보에 대한 다운로드가 요청됨을 수신하는 단계를 포함하고, 상기 생성된 블록 체인화된 영상 정보는, bluray Disk나 파일 형태, DVD, USB를 포함하는 저장 매체를 통해 등록될 수 있다.

[0010] 상기 블록 체인화된 영상 정보는, 사용자 정보에 대한 해쉬값 및 판매처 정보에 대한 해쉬값을 포함하고, 상기 수행하는 단계는, 상기 사용자로부터 상기 블록 체인화된 영상 정보에 대한 다운로드가 요청됨에 따라 상기 판매처로부터 생성된 제1 블록에 영상 정보의 해쉬값과 연결된 사용자의 해쉬값과 판매처의 해쉬값을 등록하는 단계를 포함할 수 있다.

[0011] 상기 수행하는 단계는, 상기 수신된 다운로드 요청에 따라 상기 블록 체인화된 영상 정보에 상기 사용자에게 대한 해쉬값을 설정하여 사용자에게 영상 정보를 배포하고, 상기 블록 체인화된 영상 정보에 대한 체인 정보, 영상 정보의 해쉬값을 판단하는 영상 정보의 인증을 수행하고, 상기 영상 정보의 인증을 완료함에 따라 상기 블록 체인화된 영상 정보에 설정된 해쉬값에 대응하는 사용자와 상기 프로그램을 실행하는 사용자에게 대한 사용자 인증을 수행하는 단계를 포함할 수 있다.

[0012] 상기 수행하는 단계는, 상기 블록 체인화된 영상 정보에 대한 체인 정보를 확인함에 따라 상기 블록 체인화된 영상 정보에 구성된 블록 정보의 연결 여부를 판단하고, 상기 블록 체인화된 영상 정보에 구성된 블록 정보가 정상적으로 연결되어 있을 경우, 상기 블록 체인화된 영상 정보 내의 블록과 프로그램을 실행하는 사용자의 일치 여부를 판단하는 단계를 포함할 수 있다.

[0013] 상기 수행하는 단계는, 상기 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자의 일치 여부를 판단하고, 판단 결과 일치하지 않을 경우, 상기 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자를 블랙 리스트에 등록하고, 판단 결과 일치할 경우, 영상 정보의 화면 녹화 프로그램을 감지하여 블록 체인화된 영상 정보의 재생을 결정하는 단계를 포함할 수 있다.

[0014] 영상 정보를 보호하기 위한 영상 정보 보호 시스템은, 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성하고, 상기 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행하고, 상기 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 상기 블록 체인화된 영상 정보를 재생할 수 있다.

발명의 효과

[0016] 일 실시예에 따르면, 블록 체인의 개념 중 하나인 연쇄 사슬(체인화)에서 착안하여 클립 영상, 움짤과 같은 부

본 불법 복제나 영상 전체의 불법복제를 사전에 방지할 수 있다.

[0017] 또한, 불법 복제자의 IP를 기록하므로 범인검거에도 도움을 줄 수 있다. 이를 통해 콘텐츠 저작권에 대한 의식을 함양할 수 있고 불법 복제에 따른 금전적 손실 또한 줄일 것으로 기대된다.

도면의 간단한 설명

[0019] 도 1은 일 실시예에 따른 영상 정보 보호 시스템의 동작을 설명하기 위한 도면이다.

도 2는 일 실시예에 따른 영상 정보 보호 시스템에서 블록 정보 변경의 권한을 부여하는 것을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 영상 정보 보호 시스템에서 영상 변환 동작을 설명하기 위한 도면이다.

도 4는 일 실시예에 따른 영상 정보 보호 시스템에서 영상 정보에 해쉬값을 설정하는 동작을 설명하기 위한 도면이다.

도 5는 일 실시예에 따른 영상 정보 보호 시스템에서 영상 정보를 보호하는 방법을 설명하기 위한 흐름도이다.

도 6은 일 실시예에 따른 영상 정보 보호 시스템에서 블록 체인화된 영상 정보를 확인하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0022] 실시예에서는 영상 정보(예를 들면, 영상 창작물)의 불법 복제 및 불법 유통을 원하는 않는 창작자를 위한 것으로, 블록 체인을 이용하여 영상 정보의 불법 복제 및 유통을 방지하는 기술에 대하여 설명하기로 한다. 예를 들면, 클립 영상, 움짤과 같은 부분 불법 복제나 영상 전체의 불법 복제를 사전에 방지할 수 있으며, 불법 복제자의 IP를 기록하기 때문에 범인 검거에도 도움을 줄 수 있다.

[0023] 도 1은 일 실시예에 따른 영상 정보 보호 시스템의 동작을 설명하기 위한 도면이다.

[0024] 도 1에서는 판매처, 프로그램, 제1 사용자(유저), 제2 사용자(제작자) 사이의 동작을 설명하기로 한다. 영상 정보 보호 시스템(100)은 프로그램 형태로 구현될 수 있다. 도 1에 도시된 바와 같이, 유저로부터 판매처까지 송수신되는 데이터와 유저가 영상 정보(영상 창작물)를 보기까지의 송수신되는 데이터를 확인할 수 있다.

[0025] 영상 정보 보호 시스템(100)은 블록 체인화된 영상 처리 모드와 블록 체인화된 영상 재생 모드를 제공할 수 있다. 영상 창작자 또는 제작자를 포함하는 제공자는 기존의 방식대로 영상을 제작할 수 있다. 영상 창작자 또는 제작자로부터 영상이 제작됨에 따라 프로그램 변환 기능을 이용하여 블록 체인화된 영상 창작물이 완성될 수 있다. 이후, bluray Disk나 파일 형태로 오프라인 판매처나 온라인 판매처에 등록될 수 있다. 상기 제시된 bluray Disk나 파일 형태 이외에도 DVD, USB 등 기타 다른 매체도 포함된다.

[0026] 유저는 오프라인 판매처에서 Disk를 구매하거나 온라인 판매처(사이트)에서 파일을 다운로드 받을 수 있다. 판매처는 유저를 확인하고, 유저마다 각기 다른 해쉬값을 설정하여 영상 정보를 등록하고 유저에게 배포할 수 있다. 유저는 프로그램을 이용하여 영상 정보를 재생할 수 있다. 영상 정보 보호 시스템은 해당 영상이 제대로 체인화된 영상인지, 해쉬값이 올바른지, 영상 해쉬값의 구매자와 프로그램의 실행자가 동일한 지 여부를 판단하는 과정을 수행하여 영상을 재생할 수 있다.

[0027] 참여자들이 수행하는 역할, 획득할 수 있는 잠재적 이익을 정리하여 표1과 같이 표시될 수 있다.

[0028] 표 1:

참여자 ^㉔	역할 ^㉔	잠재적 이익 ^㉔
유저 ^㉔	- 서비스 이용 ^㉔	- 저작권에 대한 의식을 키울 수 있다. ^㉔
제작자 ^㉔	- 서비스 이용 ^㉔	- 본인의 영상 창작물이 불법적으로 복제되거나 유통되는 일을 당하지 않는다. ^㉔ - 불법 복제 및 유통업자들을 빠르게 잡을 수 있다. ^㉔
판매처 ^㉔	- 서비스 제공 ^㉔	^㉔

[0029]

[0030] 도 2는 일 실시예에 따른 영상 정보 보호 시스템에서 블록 정보 변경의 권한을 부여하는 것을 설명하기 위한 도면이다.

[0031] 블록 체인 기술은 제작자가 프로그램의 변환 기능을 사용하여 영상을 블록화 처리하고, 판매처에서 해쉬값을 할당하고, 재생 시 프로그램 내에서 블록 체인을 확인하고, 블록 정보를 변경하기 위한 권한을 부여할 때 적용될 수 있다.

[0032] 해쉬값을 변경하거나 블록을 새로 생성할 경우, 불법 복제가 가능하며 불법으로 변경된 영상 정보의 재생이 가능하므로 특정된 사람만 해당 권한을 가질 수 있게 해야 한다. 블록 정보(블록 생성, 해쉬값 부여 및 변경)를 변경하는 경우, 제작자가 프로그램을 이용하여 영상 정보(영상 창작물)를 블록화 처리할 때, 판매처에서 사용자의 개인 해쉬값을 영상 정보 안에부여할 때가 있다. 이에 따라 제작자와 판매처만 권한을 가질 수 있습니다.

[0033] 영상 정보 보호 시스템은 블록 체인 생성 방식(합의 알고리즘)을 이용하여 권한자를 등록할 수 있다. 제작자는 제작자 네트워크 상에서 하나의 노드로, 판매처는 판매처 네트워크 상에서 하나의 노드로 등록될 수 있다. 제작자와 판매처를 참여자라고 하면, 도 2와 같이, 참여자는 노드(Node)로 도시될 수 있다. 노드는 권한을 얻어야 생성이 가능하다(프라이빗 블록체인). 만약, 악의적 노드가 생성이 되어도 큰 규모의 정상적 노드가 있으므로 증명 방식을 통해 악의적 노드의 접근을 차단할 수 있다. 이외에도 블록체인의 다른 증명 과정으로 적용할 수 있다.

[0034] 이와 같이 권한자를 등록하는 방식을 사용하면, 허가되지 않은 판매점은 악의적 노드로 판단되어 접근이 차단될 수 있다. 다시 말해서, 영상 판매 및 배포가 불가능하게 된다. 또한, 해쉬값을 임의로 변경하려는 경우 악의적 노드로 판단되어 접근이 차단될 수 있다. 이에, 불법 유저를 색출할 수 있다.

[0035] 도 3은 일 실시예에 따른 영상 정보 보호 시스템에서 영상 변환 동작을 설명하기 위한 도면이다.

[0036] 동영상은 보통 초당 프레임수(fps)로 표현하는데, 이는 1초당 이미지(사진)의 개수를 나타낸다. 고품질의 영상일 경우 60fps를 사용하는데 이는 1초당 60개의 이미지로 구성된다는 의미이다. 이에 따라 각 이미지들에 해쉬값을 부여하고 블록 체인화할 수 있다. 각 영상마다 설정된 프레임수가 다르므로 꼭 초당 60개의 블록을 생성할 필은 없다. 영상 제작시 설정된 프레임수로 블록을 나누는 것도 포함한다. 또한, 블록화되어 체인처럼 연결된 영상 정보는 하나의 해쉬 구성을 가지지 않는다. 예를 들면, 100명에게 영상 정보를 판매하고자 할 때, 영상 변환 기능을 100번 사용해야 한다. 영상 변환 기능을 100번 사용하면 해쉬 구성이 다른 100가지의 영상 정보가 출력되지만, 영상 실행 시 동일한 영상 정보가 출력될 수 있다.

[0037] 판매되는 영상마다 다른 해쉬 구성을 사용하는 것은, 구매하는 유저마다 다른 해쉬 구성을 가지도록 함으로써 불법 영상 제작 및 재생 시 불법 유저를 색출하기 위함이다.

[0038] 또한, 도 3에서와 같이 체인처럼 연결되면 불법적으로 클립 영상, 움짤과 같은 부분 불법 복제를 생성하는 행위를 근절할 수 있다. 재생 프로그램에서 체인 연결이 올바르게 안고 블록1부터 시작하지 않을 경우, 재생이 제

대로 되지 않기 때문이다.

- [0039] 도 4는 일 실시예에 따른 영상 정보 보호 시스템에서 영상 정보에 해쉬값을 설정하는 동작을 설명하기 위한 도면이다.
- [0040] 판매점에서 영상 정보의 초기 블록 앞에 새로운 블록이 생성될 수 있다. 생성된 새로운 블록 내에는 구매자의 정보가 포함된 해쉬값과 판매점 정보가 포함된 해쉬값이 존재할 수 있다. 영상 불법 제작자를 쉽게 검거하고 차후에 재생 프로그램에서 영상을 재생시키기 위하여 이러한 정보가 기록될 수 있다.
- [0041] 유저가 영상 정보(창작물)를 구매할 때, 판매점은 제1 블록(도 4에서는 블록0)을 생성하고, 서버에 영상 정보의 해쉬값과 연결된 사용자의 해쉬값을 서버에 등록할 수 있다. 불법 영상이 유통되었을 때 유통된 영상 정보의 해쉬값을 파악하면, 서버상에서 유통된 영상 정보의 최초 구매자를 찾을 수 있다. 이에, 최초 구매자는 불법 영상 제작자일 확률이 높다.
- [0042] 도 5는 일 실시예에 따른 영상 정보 보호 시스템에서 영상 정보를 보호하는 방법을 설명하기 위한 흐름도이다.
- [0043] 단계(510)에서 영상 정보 보호 시스템은 제공자의 영상 정보를 프로그램 변환을 통하여 블록 체인화된 영상 정보를 생성할 수 있다.
- [0044] 단계(520)에서 영상 정보 보호 시스템은 생성된 블록 체인화된 영상 정보가 사용자에게 대하여 설정된 해쉬값에 기초하여 사용자에게 배포됨에 따라 영상 정보 및 사용자의 인증 과정을 수행할 수 있다. 영상 정보 보호 시스템은 생성된 블록 체인화된 영상 정보가 온라인 판매처 또는 오프라인 판매처에 등록됨에 따라 사용자에게 의하여 영상 정보에 대한 다운로드가 요청됨을 수신할 수 있다. 영상 정보 보호 시스템은 사용자로부터 블록 체인화된 영상 정보에 대한 다운로드가 요청됨에 따라 판매처로부터 생성된 제1 블록에 영상 정보의 해쉬값과 연결된 사용자의 해쉬값과 판매처의 해쉬값을 등록할 수 있다.
- [0045] 영상 정보 보호 시스템은 수신된 다운로드 요청에 따라 블록 체인화된 영상 정보에 사용자에게 대한 해쉬값을 설정하여 사용자에게 영상 정보를 배포하고, 블록 체인화된 영상 정보에 대한 체인 정보, 영상 정보의 해쉬값을 판단하는 영상 정보의 인증을 수행하고, 영상 정보의 인증을 완료함에 따라 블록 체인화된 영상 정보에 설정된 해쉬값에 대응하는 사용자와 프로그램을 실행하는 사용자에게 대한 사용자 인증을 수행할 수 있다.
- [0046] 영상 정보 보호 시스템은 블록 체인화된 영상 정보에 대한 체인 정보를 확인함에 따라 상기 블록 체인화된 영상 정보에 구성된 블록 정보의 연결 여부를 판단하고, 블록 체인화된 영상 정보에 구성된 블록 정보가 정상적으로 연결되어 있을 경우, 블록 체인화된 영상 정보 내의 블록과 프로그램을 실행하는 사용자의 일치 여부를 판단할 수 있다. 영상 정보 보호 시스템은 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자의 일치 여부를 판단하고, 판단 결과 일치하지 않을 경우, 블록 체인화된 영상 정보의 제1 블록에 등록된 사용자 정보와 프로그램을 실행하는 사용자를 블랙 리스트에 등록하고, 판단 결과 일치할 경우, 영상 정보의 화면 녹화 프로그램을 감지하여 블록 체인화된 영상 정보의 재생을 결정할 수 있다.
- [0047] 단계(530)에서 영상 정보 보호 시스템은 수행된 영상 정보 및 사용자의 인증 과정을 완료함에 따라 블록 체인화된 영상 정보를 재생할 수 있다.
- [0048] 도 6은 일 실시예에 따른 영상 정보 보호 시스템에서 블록 체인화된 영상 정보를 확인하는 방법을 설명하기 위한 흐름도이다.
- [0049] 영상 정보 보호 시스템은 블록 체인화된 영상 정보를 재생하는 재생 모드를 실행할 수 있다. 영상 정보 보호 시스템은 블록 체인화된 영상 정보의 체인 정보를 확인할 수 있다. 영상 정보 보호 시스템은 블록 체인화된 영상 정보를 구성하는 블록들이 정상적으로 연결되어 있는지 여부를 판단할 수 있다.
- [0050] 영상 정보 보호 시스템은 영상 정보의 체인 정보가 정상적으로 연결되어 있지 않은 것으로 판단됨에 따라 클립 영상, 움짤과 같은 부분 불법 복제로 인식하여 영상 정보를 재생하지 않는다. 이때, 인터넷 연결 상태에서 판단될 수 있다. 영상 정보 보호 시스템은 영상 정보의 체인 정보가 정상적으로 연결된 것으로 판단됨에 따라 영상 정보 내의 블록 0(제1 블록)과 프로그램을 실행시키는 사용자가 일치하는지 판단할 수 있다(610). 이때, 블록 0은 사용자의 해쉬값과 판매처의 해쉬값을 포함한 블록을 의미할 수 있다.
- [0051] 판매처에서 유저가 영상을 구매하면, 블록0에 정보를 기록함에 동시에 서버에 판매처 정보와 유저 정보를 등록하게 된다. 영상 정보 보호 시스템은 구매자가 영상 정보를 임의로 조작 하였는지 판단하기 위하여, 영상 정보의 재생 전에 한번 더 영상 정보를 서버상에서 다운로드하고 현재 재생하려는 영상 정보의 블록0과 비교할 수

있다. 또한, 프로그램을 처음 실행할 때 사용자의 정보를 등록하는데, 블록0상의 구매자 정보와 현재 실행하려는 프로그램의 사용자 정보도 동일한 지 비교할 수 있다. 만약 두 정보 사이에 불일치한 정보가 발생되면 영상 정보를 불법 영상으로 판단하여 블록0상의 유저와 프로그램 유저를 블랙리스트에 등록하고 재생을 하지 않는다(611). 조작한 사람은 블록0상의 사용자이고 실행한 사람은 프로그램 사용자로서 판단할 수 있다. 이와 같은 불법 영상의 실행은 조작한 사람도 잘못이지만 실행한 사람도 잘못이기 때문에 둘 다 블랙리스트에 등록할 수 있다.

[0052] 블록 0과 프로그램을 실행하는 사용자 정보가 일치함에 따라 화면 녹화 프로그램을 감지할 수 있다(620). 화면 전체를 녹화하는 경우 블록체인으로 영상 창작물을 보호하는 효과가 없기 때문이다. 이 기능은 현재 인터넷 강의 등을 들을 때도 적용되는 기능이다. 화면 녹화 프로그램이 감지 된다면 현재 영상을 실행하고 있는 프로그램 사용자가 악의적인 목적을 가지고 있다고 판단하고 유저를 블랙리스트에 등록하며 영상 정보를 재생하지 않는다(621).

[0053] 영상 정보 보호 시스템은 영상 정보를 보호하기 위한 서비스를 이용하는 요금을 부가할 수 있다. 예를 들면, 영상 창작자가 자신의 영상 정보를 보호하고 싶을 경우, 프로그램 변환 기능을 사용할 때 서비스 이용료를 지불해야 한다. 이때, 100명에게 영상을 팔기 위해서 영상 변환 기능을 100번 사용해야 해쉬 구성이 다른 100가지의 영상이 출력되지만, 100번의 서비스 이용료를 지불하는 것이 아니라, 영상 하나에 대한 한 번의 서비스 이용료가 부가될 수 있다. 또한, 프로그램을 재생 용도로 사용하는 유저의 경우, 따로 서비스 이용료가 부가되지 않는다.

[0054] 일 실시예에 따른 영상 정보 보호 시스템은 영상 창작물의 불법 복제를 방지할 수 있다.

[0055] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0056] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0057] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0058] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가

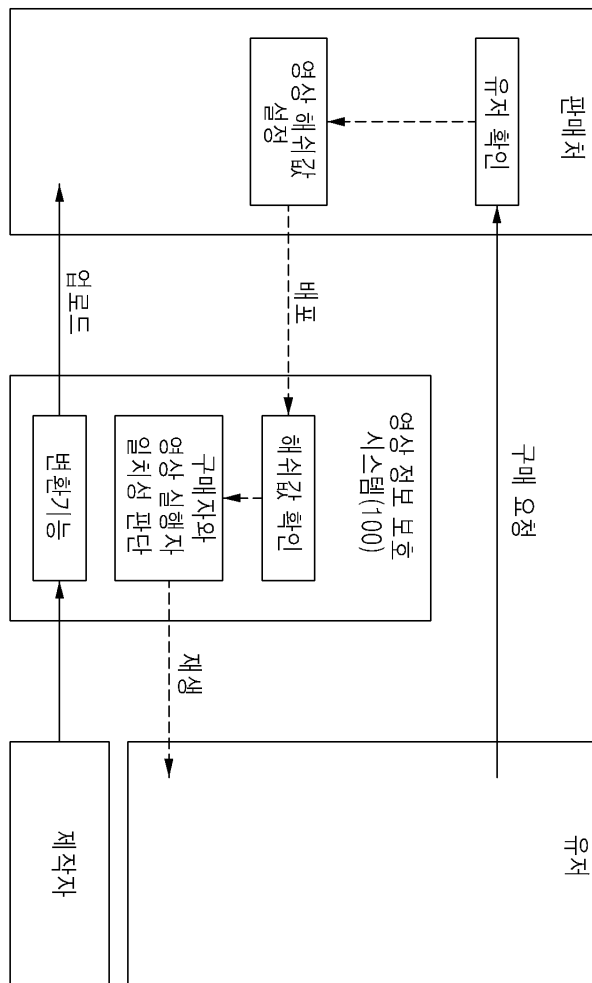
진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0059]

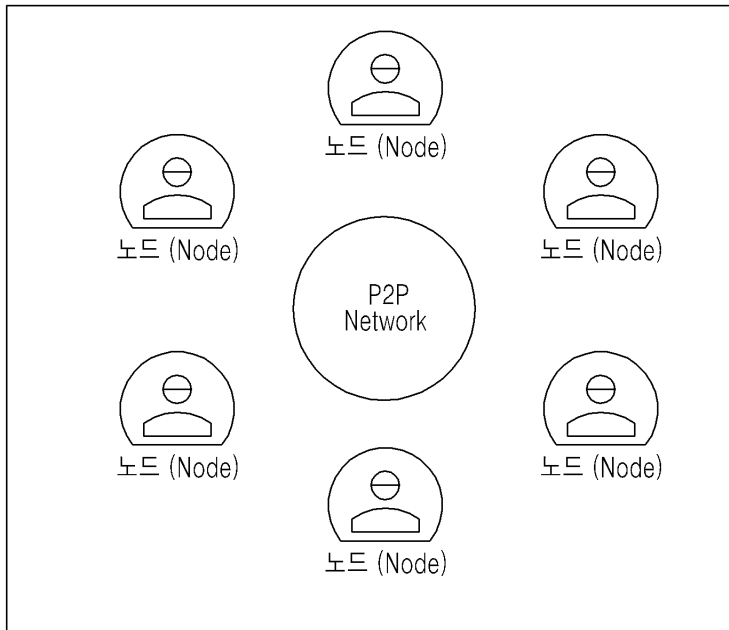
그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

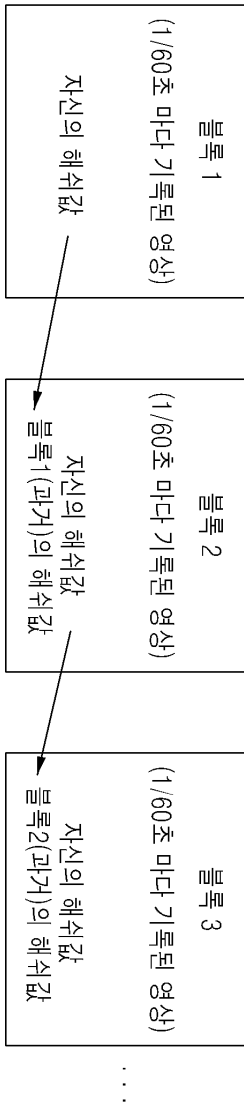
도면1



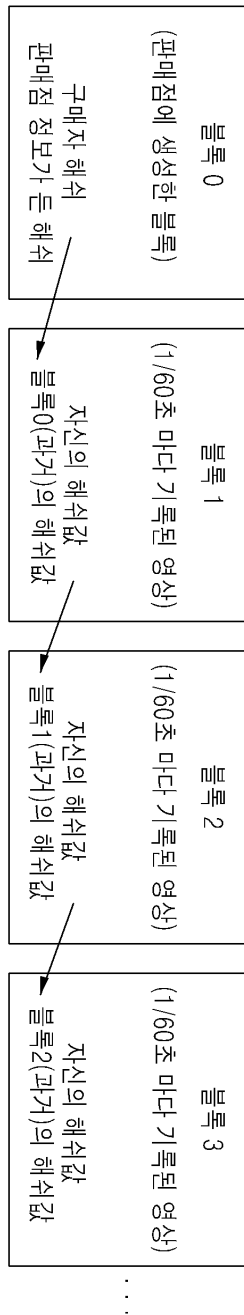
도면2



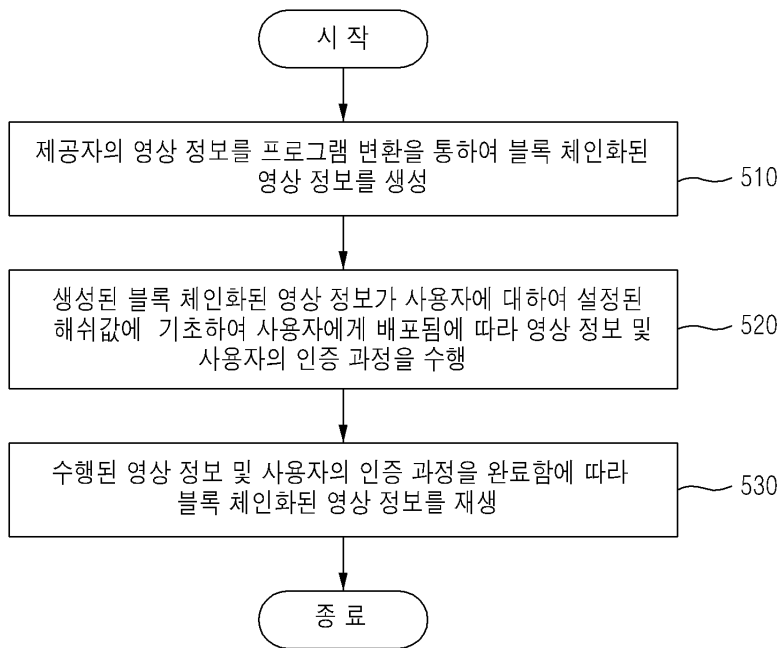
도면3



도면4



도면5



도면6

