(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월29일
(11) 등록번호 10-1127194
(24) 등록일자 2012년03월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 15/16* (2006.01)
G06F 21/00 (2006.01) *G06F 3/00* (2006.01)
(21) 출원번호 10-2009-0090132
(22) 출원일자 2009년09월23일
심사청구일자 2009년09월23일
(65) 공개번호 10-2010-0034716
(43) 공개일자 2010년04월01일
(30) 우선권주장
12/284,803 2008년09월24일 미국(US)
(56) 선행기술조사문헌
KR1020030041501 A*
KR1020030081878 A*
JP2002082917 A
KR1020030012556 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
디즈니엔터프라이지즈,인크.
미합중국캘리포니아주버어뱅크시사우스뷰나비스타스트리트500(우편번호91521)
(72) 발명자
리켈톤 앱디, 싸이릴
미국 91505 캘리포니아 버뱅크 카탈리나 스트리트 404 엔
(74) 대리인
김수진, 윤의섭

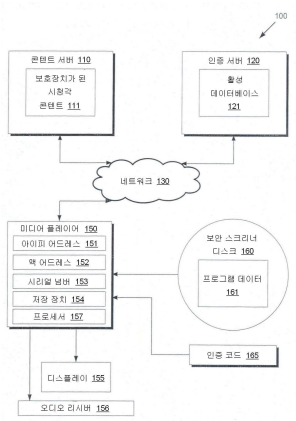
전체 청구항 수 : 총 22 항 심사관 : 양종필

(54) 발명의 명칭 **무효화 가능 접근을 이용한 보안 콘텐트 제공 시스템 및 방법**

(57) 요 약

미디어 콘텐트 접근을 제공하기 위한 미디어 플레이어에 의한 사용 방법이 제공된다. 그 방법은 미디어 콘텐트 재생을 위한 사용자의 요청을 수신, 사용자의 인증코드 입력을 요청, 사용자의 조작에 따른 상기 인증코드를 수신, 네트워크를 통하여 상기 인증코드를 인증서버로 전송, 인증코드가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신, 상기 네트워크를 통하여 유효 인증메세지를 콘텐트 서버로 전송, 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 미디어 콘텐트를 읽음을 포함하되, 상기 미디어 콘텐트는 미디어 콘텐트와 연관된 식별정보와 사용자를 병합하는 것을 특징으로 한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

시청각 콘텐트 재생을 위한 사용자의 요청을 수신하는 단계;

상기 시청각 콘텐츠 재생에 대한 요청의 수신에 응하여, 개인의 인증코드 입력을 요청하는 단계;

상기 인증코드 입력에 대한 요청에 응하여, 상기 개인으로부터 상기 인증코드를 수신하는 단계;

상기 인증코드의 수신에 응하여, 네트워크를 통하여 상기 인증코드 및 미디어 플레이어 식별자(media player indetifier)를 인증서버로 전송하는 단계;

상기 인증코드 및 미디어 플레이어 식별자의 전송에 응하여, 인증코드 및 상기 미디어 플레이어 식별자가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하는 단계;

상기 네트워크를 통하여, 상기 인증서버로부터 전송된 유효 인증메세지를 콘텐트 서버로 전송하는 단계; 및

상기 유효 인증메시지가 전송된 후에, 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 시청각 콘텐트 및 분리된(separate) 식별정보를 읽어들이는 단계를 포함하되,

상기 분리된 식별 정보는, 상기 개인 및 상기 미디어플레이어와, 상기 시청각 콘텐츠를 연결(associate)하는 것임을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 2

제1항에 있어서,

상기 식별정보는, 인증코드에 대응하여, 상기 미디어 플레이어에 의해서 상기 시청각 콘텐트에 포함되고, 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크인 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 3

제2항에 있어서,

상기 워터마크는 이미지 프로세싱을 통하여 검출될 수 있는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 4

제2항에 있어서,

상기 워터마크는 시청각 콘텐트 내에서 특정시간에 미리 결정된 위치들에 부호화된 디지털 데이터를 포함하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 5

제1항에 있어서,

상기 식별정보는 인증코드에 대응하여, 상기 미디어 플레이어에 의해서 상기 시청각 콘텐트에 포함된 사람이 인지할 수 있는 워터마크인 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 6

제5항에 있어서,

상기 워터마크는 인증코드에 대응되어 개인의 이름과 시청각 콘텐트의 저작권자를 식별하는 사람이 인지할 수 있는 비디오 오버레이를 포함하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 7

제1항에 있어서,

상기 개인의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 8

제1항에 있어서,

상기 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법은,

미디어 플레이어에 의해 상기 시청각 콘텐트가 플레이되는 동안 식별정보를 상기 시청각 콘텐트 위에 오버레이시키는 단계를 더 포함하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 9

시청각 콘텐트 접근 제공을 위한 미디어 플레이어에 있어서,

프로그램 코드; 및

상기 프로그램 코드를 실행하기 위해 설정된 프로세서;

를 포함하고,

상기 프로세서는,

시청각 콘텐트 재생을 위한 개인의 요청을 수신하는 과정;

상기 시청각 콘텐츠 재생에 대한 요청의 수신에 응하여, 개인의 인증코드 입력을 요청하는 과정;

상기 인증코드 입력에 대한 요청에 응하여, 상기 개인으로부터 상기 인증코드를 수신하는 과정;

상기 인증코드의 수신에 응하여, 네트워크를 통하여 상기 인증코드 및 미디어 플레이어 식별자를 인증서버로 전송하는 과정;

상기 인증코드 및 미디어 플레이어 식별자의 전송에 응하여, 상기 인증코드 및 상기 미디어 플레이어 식별자가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하는 과정;

상기 네트워크를 통하여 상기 인증서버로부터 전송된 유효 인증메세지를 콘텐트 서버로 전송하는 과정; 및

상기 유효 인증메시지가 전송된 후에, 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 시청각 콘텐트 및 분리된 식별 정보를 읽어들이는 과정;

을 수행하되,

상기 분리된 식별 정보는, 상기 개인 및 상기 미디어플레이어와, 상기 시청각 콘텐츠를 연결하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 10

제9항에 있어서,

상기 식별정보는 인증코드에 대응하여 상기 미디어플레이어에 의해서 상기 시청각 콘텐트에 포함되고, 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크인 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 11

제10항에 있어서,

상기 워터마크는 이미지 프로세싱을 통하여 검출될 수 있는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 12

제10항에 있어서,

상기 워터마크는 상기 시청각 콘텐트 내에서 특정시간에 미리 결정된 위치들에 부호화된 디지털 데이터를 포함하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 13

제9항에 있어서,

상기 식별정보는 인증코드에 대응하여 상기 미디어플레이어에 의해서 시청각 콘텐트에 포함되고, 사람이 인지할 수 있는 워터마크인 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 14

제13항에 있어서,

상기 워터마크는 인증코드에 대응되어 개인의 이름과 시청각 콘텐트의 저작권자를 식별하는 사람이 인지할 수 있는 비디오 오버레이를 포함하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 15

제9항에 있어서,

상기 개인의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 16

제9항에 있어서,

상기 프로세서는,

상기 미디어 플레이어에 의해 상기 시청각 콘텐트가 재생되는 동안 식별정보를 상기 시청각 콘텐트 위에 오버레이시키는 과정을 더 수행하는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

청구항 17

시청각 콘텐트 재생을 위한 개인의 요청을 수신하기 위한 코드;

상기 시청각 콘텐츠 재생에 대한 요청의 수신에 응하여, 개인의 인증코드 입력을 요청하기 위한 코드;

상기 인증코드 입력에 대한 요청에 응하여, 상기 개인으로부터 상기 인증코드를 수신하기 위한 코드;

상기 인증코드의 수신에 응하여, 네트워크를 통하여 상기 인증코드 및 미디어 플레이어 식별자를 인증서버로 전송하기 위한 코드;

상기 인증코드 및 미디어 플레이어 식별자의 전송에 응하여, 인증코드 및 상기 미디어 플레이어 식별자가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하기 위한 코드;

상기 네트워크를 통하여 상기 인증서버로부터 전송된 유효 인증메세지를 콘텐트 서버로 전송하기 위한 코드; 및

상기 유효 인증메시지가 전송된 후에, 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 시청각 콘텐트 및 분리된 식별 정보를 읽어들이기 위한 코드를 제공하되,

상기 분리된 식별 정보는, 상기 개인 및 상기 미디어플레이어와, 상기 시청각 콘텐츠를 연결하는 것을 특징으로 하는 미디어 플레이어의 프로세서에 의해 실행되는 프로그램 코드가 기록된 컴퓨터로 판독가능한 기록매체.

청구항 18

제17항에 있어서,

상기 식별정보는 인증코드에 대응하여, 상기 미디어 플레이어에 의해서 상기 시청각 콘텐트에 포함되고, 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크인 것을 특징으로 하는 미디어 플레이어의 프로세서에 의해 실

행되는 프로그램 코드가 기록된 컴퓨터로 판독가능한 기록매체.

청구항 19

제17항에 있어서,

상기 식별정보는 인증코드에 대응하여, 상기 미디어 플레이어에 의해서 상기 시청각 콘텐트에 포함되고, 사람이 인지할 수 있는 워터마크인 것을 특징으로 하는 미디어 플레이어의 프로세서에 의해 실행되는 프로그램 코드가 기록된 컴퓨터로 판독가능한 기록매체.

청구항 20

제17항에 있어서,

상기 개인의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되는 것을 특징으로 하는 미디어 플레이어의 프로세서에 의해 실행되는 프로그램 코드가 기록된 컴퓨터로 판독가능한 기록매체.

청구항 21

제1항에 있어서,

상기 개인으로부터의 요청은, 상기 미디어 플레이어 내로 보호된 컴퓨터로 읽을 수 있는 매체가 삽입됨으로써 개시되고,

상기 보호된 컴퓨터로 읽을 수 있는 매체가 삽입됨으로써, 상기 인증서버로의 접속 가능해지는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법.

청구항 22

제9항에 있어서,

상기 개인으로부터의 요청은, 상기 미디어 플레이어 내로 보호된 컴퓨터로 읽을 수 있는 매체가 삽입됨으로써 개시되고,

상기 보호된 컴퓨터로 읽을 수 있는 매체가 삽입됨으로써, 상기 인증서버로의 접속 가능해지는 것을 특징으로 하는 시청각 콘텐트 접근 제공을 위한 미디어 플레이어.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 일반적인 컴퓨터 시스템과 미디어 콘텐트에 관련된 발명이다. 보다 상세하게, 본 발명은 미디어 콘텐트 보안과 접속에 대한 시스템에 관련되어 있다.

배 경 기 술

[0002] 연예 미디어 산업에 있어서, 자주 저작물의 견본 복제물 또는 판촉을 위한 복제물을 제공해야할 필요가 있다. 평판을 생성하고 수요자의 인식을 구축하는 것은 미디어 생산물의 성공적인 진출을 위한 중요한 요소가 된다. 예를 들어, 레코드 회사들은 소문이 퍼지는 채널들로 앨범이 도착한 그 시점에 신문 가판대에서 리뷰들이 활용될 수 있도록, 배포일 이전에 선택된 새로운 앨범들의 판촉용 복제물들을 전송할 수 있다. 유사하게, 필름과 비디오 제작에 있어서, 스크리너 디스크들은 자주 리뷰, 평점 또는 심사의 목적을 위하여 리뷰어들, 심사위원들 및 비평가들에게 극장 개봉일 또는 판매 예정일 전에 제공된다. 또한, 배급업자들은 가능한 분배 계약의 상업적 이익을 평가하기 위하여 이러한 스크리너 디스크들을 수신할 수도 있다.

[0003] 그러나, 동시에 저작권 침해에 따라 지금까지의 판촉 노력을 무의미하게 할 수 있으며, 강력한 구매 또는 티켓 판매를 흡수할 수 있는 이러한 스크리너 디스크들의 일반 대중에게로의 누설을 방지하는 것이 중요하다. 자주, 리뷰어들, 비평가들 및 심사위원들은 스크리너 디스크가 인터넷을 통하여 광범위하게 이용 가능해 지거나 또는

전문적인 저작권 침해자들에 의하여 대량으로 복제될 때까지 연쇄 반응을 일으키는 그들의 동료 네트워크에 스크리너 디스크를 차례로 분배하는 호기심 많은 친구들과 가족들로부터 그들의 견본 복제물을 지키는 것이 어렵다는 것을 발견한다. 한번 콘텐트가 광범위하게 이용이 가능해지면, 접근을 제한할 수 있는 용이한 방법이 없기 때문에 피해를 완화시키는 것은 어렵다.

[0004] 억제수단이 없는 사전배포 매체의 광범위한 누설은 매체 콘텐트 생산자가 피하고 싶은 명백한 재난이다. 따라서, 권한없는 접근과 분배에 대하여 스크리너 디스크를 보호하기 위한 다양하고 광범위한 방법들이 현재 사용되고 있으나, 각각의 방법은 최적의 해결책으로서의 채택을 방해하는 단점을 수반한다. 비싸거나, 불편하거나, 또는 시청각 품질의 희생이 요구되는 등, 현재 사용되고 있는 해결책들은 많은 면에 있어서 자주 불만족스럽다.

[0005] 스크리너 디스크들을 보호하기 위한 하나의 옵션은 누설이 발생되는 경우 분석자들이 최소한 어떠한 스크리너 디스크 또는 파티로부터 누설이 기원되었는지를 밝혀낼 수 있도록 각각의 스크리너 디스크의 시청각 콘텐트에 워터마크를 삽입하는 것이다. 그러나, 각각의 다른 수신자에 대하여 스크리너 디스크는 고유의 방법에 따라 워터마크되어야만 하며, 통상적으로 저렴한 디스크 복제 과정이 대단히 비싼 과정으로 바뀐다. 각각의 수신 파티에 대하여 고유한 워터마크들과 디스크들이 생성되어야 하므로, 하나의 마스터 디시크는 더 이상 간단하고 비용효율이 높은 복제 마스터로서 기능하지 못할 수 있다.

[0006] 다른 옵션은 누설의 방지 또는 완화를 위하여 DRM(Digital Right Management)을 강화한 소유권의 시청각 재생 해결책을 이용하는 것이다. 이 방법에 따른 문제점은 해결책의 소유권의 성질이며, 여기서 각각의 수신 파티는 적절하게 설치된 소유권의 재생장치를 구비해야하고, 만약 스크리너 디스크들이 짧은 마감시간 내에서 다수의 청중들에게 분배되어야할 필요가 있는 경우 소유권의 재생장치를 구비하는 것은 힘들 수 있다. 또한, 이러한 방법은 전형적으로 모든 필요 장치에 대하여 하나의 특정 공급자에 의존하며, 단지 하나의 공급자가 필요한 수리와 지원을 지원할 수 있으므로 하드웨어적으로 실패가 발생하는 경우 곤란한 상황이 될 수 있다. 부가적으로, 이러한 소유권 시스템은 표준적이고, 쉽게 획득될 수 있으며, 당장 손에 넣을 수 있는 재생 시스템에 비하여 보다 비용이 비싼 경향이 있다.

[0007] 또 다른 옵션은 안전한 온라인 배달 시스템을 통하여 콘텐트를 배달하는 것이다. 그러나, 이 방법은 통상적으로 작동을 위한 개인용 컴퓨터를 요구하며, 다수의 사람들은 그들의 개인용 컴퓨터를 그들의 홈 씨어터(Home Theatres)에 통합하지 않는다. 영화 감독들과 다른 개인 창작자들은 그들 작업의 완전한 임팩트를 수신할 수 있는 적절한 시청각 장치를 이용해 관객들이 그들의 창작물을 경험하는 것을 더 선호한다. 그러나, 통상적으로 단지 작은 LCD 스크린과 작은 2채널 컴퓨터 스피커로 특징되는 전형적인 개인용 컴퓨터는 일반적으로 그러한 임무에 적합하지 않다. 통상적으로 큰 디스플레이와 다채널 오디오 시스템으로 특징되는 전형적인 홈 씨어터에 쉽게 결합될 수 있는 배달 시스템이 없다면, 콘텐트의 생산자의 창작적 영감은 저품질의 비디오와 오디오 재생으로 인하여 희생될 수도 있다.

[0008] 최후의 수단으로서, 스크리너 디스크는 복사본의 제작에 따라 품질에 있어 아날로그 성질이 떨어지게 되는 VHS 테이프와 같은 아날로그 형식으로 공급될 수도 있다. 이러한 방식은 몇몇의 복사활동을 막을 수도 있음에도 불구하고, 복사본이 여전히 힘있는 구매자들의 정품 구매를 막을수 있을 정도의 적당한 품질을 가질수 있으며, 콘텐트의 시청각적인 완전성을 보존하고자 하는 콘텐트 제작자의 생각들이 무시될 것이다. 따라서, 아날로그 경로는 저작권 침해를 막거나 또는 평론하는 관객들에 대한 적합한 품질의 영상을 제공하는 본연의 기능을 수행하는데 도움이 되지 않을 수 있다.

[0009] 따라서, 종래기술의 단점들과 부족한 점들을 극복할 수 있는 비용효율성이 우수하고 편리하며 동시에 높은 품질의 시청각 경험을 제공할 수 있는 스크리너 디스크들의 안전한 분배 시스템이 필요하다.

발명의 내용

해결 하고자하는 과제

[0010] 본 발명은 상술한 바와 같은 종래기술의 문제점을 해결하기 위하여, 비용효율성이 우수하고 편리하며 동시에 높은 품질의 시청각 경험을 제공할 수 있는 보안 분배 시스템과 방법을 제공함을 목적으로 한다.

과제 해결수단

[0011] 상기한 바와 같은 목적을 달성하기 위해, 본 발명의 바람직한 일 실시예에 따르면, 미디어 콘텐트 재생을 위한 사용자의 요청을 수신하는 단계; 사용자의 인증코드 입력을 요청하는 단계; 사용자의 조작에 따른 상기 인증코드를 수신하는 단계; 네트워크를 통하여 상기 인증코드를 인증서버로 전송하는 단계; 인증코드가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하는 단계; 상기 네트워크를 통하여 유효 인증메세지를 콘텐트 서버로 전송하는 단계; 및 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 미디어 콘텐트를 읽어들이는 단계를 포함하되, 상기 미디어 콘텐트는 미디어 콘텐트와 연관된 식별정보와 사용자를 병합하는 것을 특징으로 하는 미디어 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법이 제공된다.

[0012] 이때, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크로 구성될 수 있다.

[0013] 또한, 전술한 워터마크는 이미지 프로세싱을 통하여 검출될 수 있도록 구성될 수 있다.

[0014] 여기서, 전술한 워터마크는 미디어 콘텐트 내에서 특정시간에 미리 결정된 위치들에 부호화된 디지털 데이터를 포함하도록 구성될 수 있다.

[0015] 한편, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 사람이 인지할 수 있는 워터마크로 구성될 수 있다.

[0016] 이때, 전술한 워터마크는 인증코드에 대응되어 사용자의 이름과 미디어 콘텐트의 저작권자를 식별하는 사람이 인지할 수 있는 비디오 오버레이를 포함하도록 구성될 수 있다.

[0017] 한편, 전술한 사용자의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되도록 구성될 수 있다.

[0018] 또 다른 한편으로, 전술한 미디어 콘텐트 접근 제공을 위한 미디어 플레이어 사용방법은, 미디어 플레이어에 의해 미디어 콘텐트가 플레이되는 동안 식별정보를 미디어 콘텐트 위에 오버레이시키는 단계를 더 포함하도록 구성될 수 있다.

[0019] 상기한 바와 같은 목적을 달성하기 위해, 본 발명의 다른 바람직한 일 실시예에 따르면, 미디어 콘텐트 재생을 위한 사용자의 요청을 수신하는 과정; 사용자의 인증코드 입력을 요청하는 과정; 사용자의 조작에 따른 상기 인증코드를 수신하는 과정; 네트워크를 통하여 상기 인증코드를 인증서버로 전송하는 과정; 인증코드가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하는 과정; 상기 네트워크를 통하여 유효 인증메세지를 콘텐트 서버로 전송하는 과정; 및 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 미디어 콘텐트를 읽어들이는 과정을 수행하되, 상기 미디어 콘텐트는 미디어 콘텐트와 연관된 식별정보와 사용자를 병합하는 것을 특징으로 하는 미디어 콘텐트 접근 제공을 위한 미디어 플레이어가 제공된다.

[0020] 이때, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크로 구성될 수 있다.

[0021] 또한, 전술한 워터마크는 이미지 프로세싱을 통하여 검출될 수 있도록 구성될 수 있다.

[0022] 여기서, 전술한 워터마크는 미디어 콘텐트 내에서 특정시간에 미리 결정된 위치들에 부호화된 디지털 데이터를 포함하도록 구성될 수 있다.

[0023] 한편, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 사람이 인지할 수 있는 워터마크로 구성될 수 있다.

[0024] 이때, 전술한 워터마크는 인증코드에 대응되어 사용자의 이름과 미디어 콘텐트의 저작권자를 식별하는 사람이 인지할 수 있는 비디오 오버레이를 포함하도록 구성될 수 있다.

[0025] 한편, 전술한 사용자의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되도록 구성될 수 있다.

[0026] 또 다른 한편으로, 전술한 미디어 콘텐트 접근 제공을 위한 미디어 플레이어는, 미디어 플레이어에 의해 미디어 콘텐트가 플레이되는 동안 식별정보를 미디어 콘텐트 위에 오버레이시키는 과정을 더 수행하도록 구성될 수 있다.

[0027] 상기한 바와 같은 목적을 달성하기 위해, 본 발명의 또 다른 바람직한 일 실시예에 따르면, 미디어 콘텐트 재생을 위한 사용자의 요청을 수신하기 위한 코드; 사용자의 인증코드 입력을 요청하기 위한 코드; 사용자의 조작에 따른 상기 인증코드를 수신하기 위한 코드; 네트워크를 통하여 상기 인증코드를 인증서버로 전송하기 위한 코드; 인증코드가 유효한 것으로 확인되는 경우, 상기 네트워크를 통하여 인증서버로부터 전송되는 유효 인증메세지를 수신하기 위한 코드; 상기 네트워크를 통하여 유효 인증메세지를 콘텐트 서버로 전송하기 위한 코드; 및 상기 네트워크를 통하여 상기 콘텐트 서버로부터 상기 미디어 콘텐트를 읽어들이기 위한 코드를 포함하되, 상기 미디어 콘텐트는 미디어 콘텐트와 연관된 식별정보와 사용자를 병합하는 것을 특징으로 하는 미디어 플레이어의 프로세서에 의해 실행되는 프로그램 코드가 기록된 컴퓨터로 판독가능한 기록매체가 제공된다.

[0028] 이때, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 기계가 인지할 수 있고 사람이 인지할 수 없는 워터마크로 구성될 수 있다.

[0029] 다른 한편으로, 전술한 식별정보는 인증코드에 대응되어 미디어 콘텐트에 병합된 사람이 인지할 수 있는 워터마크로 구성될 수 있다.

[0030] 또 다른 한편으로, 전술한 사용자의 요청은 미디어 플레이어에 디스크를 삽입함으로써 시작되도록 구성될 수 있다.

효 과

[0031] 이상에서 살펴본 바와 같이, 본 발명에 따르면 콘텐트 제작자들이 비용대비 효율이 우수하고, 보호장치가 되어 있으며, 무효화가 가능한 방식으로 청중들에게 판촉할 수 있고 결과적으로 재정상의 자원을 보존하며, 보호장치가 된 자료들의 우연한 복제를 방지하고, 만일 콘텐트 누설이 발생한 경우 뜻밖의 사고에 대한 계획을 제공하는 보안 스크리너 디스크들 또는 다른 수단들을 통한 보안 콘텐츠의 분배가 가능하다는 장점이 있다.

[0032] 또한, 본 발명에 따르면 각각의 수령인에 대하여 커스터마이즈된 데이터를 구비하는 물리적인 매체는 더 이상 창조될 필요성이 없으므로, 일반적인 스크리너 디스크들의 분배는 상업적인 미디어에 대한 비용 효율이 우수한 대량 생산 기술들에 영향을 줄 수 있다는 장점이 있다.

[0033] 또한, 본 발명에 따르면 산업과 소비자들에 의하여 광범위하게 채택된 표준 콘텐트 포맷들과 미디어들이 이용될 수 있으므로, 재생과 분배는 소매 채널들에서 광범위하게 이용이 가능한 필수적인 하드웨어를 이용함으로써 용이하게 달성될 수 있다는 장점이 있다.

[0034] 또한, 본 발명에 따르면 네트워크 연결의 도움으로 인하여, 그러한 표준 규격 하드웨어가 각각의 수령인에 대하여 우발적인 불법 분배에 대한 효과적인 장애물을 제공하는 고유의 워터마크들을 삽입할 수 있고, 고립된 사건들이 눈사태처럼 큰 재앙이되는 것을 방지하는 즉각적인 관련 인증코드들의 무효화로 인하여 콘텐트 누설 피해는 쉽고 단순하게 제어할 수 있다는 장점이 있다.

[0035] 또한, 본 발명에 따르면 누설된 자료들에 포함된 인식불가능한 워터마크들의 존재는 누설 출처를 결정함에 있어 가치있는 법적 증거를 제공할 수 있다는 장점이 있다..

발명의 실시를 위한 구체적인 내용

[0036] 본 발명은 무효화 가능 접속을 이용한 보안 콘텐트를 위한 시스템과 방법을 지향한다. 후술되는 설명은 본 발명을 실행하기에 적합한 명확한 정보를 포함한다. 본 발명에 대해 통상의 지식을 가진 당업자라면 본 발명이 본 출원에서 명확하게 설명되고 있는 것으로부터 다양한 방법으로 실행될 수 있음을 인식할 수 있을 것이다. 나아가, 이하에서 논의되지 않는 본 발명의 몇몇 사소한 것들이 본 발명을 모호하게 하지 않는다. 본 출원 내에서 설명되지 않는 그 사소한 것들은 당업자에게 자명한 지식 속에 포함된다. 본 출원의 도면들과 이에 수반되는 상세한 설명은 단지 본 발명의 예시적인 실시예에 불과하다. 간결함을 유지하기 위하여, 본 발명의 원칙들을 이용하는 본 발명의 다른 실시예들은 본 출원 내에서 특별하게 설명되지 아니하며, 본 발명의 도면들에 의하여 특별하게 도시되지 아니한다.

[0037] 도 1은 본 발명의 바람직한 일 실시예에 따른 무효화 가능 접속과 보안 콘텐트를 이용하기 위한 보안 배달 시스템의 구성 블록도이다. 보안 배달 시스템(Secure delivery system)(100)은 콘텐트 서버(content server)(110), 인증서버(authentication server)(120), 네트워크(130), 미디어 플레이어(150), 보안 콘텐트가 포함된 보안 스크리너 디스크(secure screener disc)(160), 및 인증코드(165)를 포함한다. 콘텐트 서버(110)는 보호장치가 된 시청각 콘텐트(111)를 포함한다. 인증서버(120)는 활성 데이터베이스(121)를 포함한다. 미디어 플레이어(150)는 아이피 어드레스(151), 맥 어드레스(152), 암호해독 키(decryption key)(153), 저장장치(154) 및 프로세서(157)를 포함한다. 보안 스크리너 디스크(160)는 프로그램 데이터(161)를 포함한다. 네트워크(130)는 콘텐트 서버(110), 인증서버(120), 및 미디어 플레이어(150)에 대하여 데이터 통신을 제공한다.

[0038] 콘텐트 서버(110)는 일반 대중이 아닌 제한된 청중에 의하여 판촉용 시청이 의도된 영화 또는 다른 프로그래밍을 포함하고 있는 보호장치가 된 시청각 콘텐트(111)를 포함한다. 예를 들어, 보호장치가 된 시청각 콘텐트(111)는 단지 콘테스트의 심사위원들에게 제공되도록 의도된 영화 콘테스트에 출품된 영화일 수 있다. 그 콘텐트는 일반 대중에게 제공될 의도가 아니므로, 콘텐트를 보호해야할 필요성이 있다. 다른 실시예에서, 콘텐트는 구매자와 같은 인증된 사람에게 제공되는 오디오 콘텐트 또는 영상 콘텐트일 수 있다. 따라서, 만일 인증서버(120)로부터 전송된 유효한 인증 메세지를 포함하는 적합한 자격이 표현되지 않는 경우, 콘텐트 서버(110)는 보호장치가 된 시청각 콘텐트(111)를 배포하지 않을 수 있다. 일반적으로, 암호화는 무분별한 분배로부터 콘텐트를 보호하기 위하여 이용되는 방법이고, 어드밴스드 인크립션 스탠다드(Advanced Encryption Standard, AES)를 이용하는 암호화는 블루-레이 디스크(Blu-ray Disc)에 대한 어드밴스드 액세스 콘텐트 시스템(Advanced Access Content System, AACS)과 같은 콘텐트 보호 시스템에 대한 합의를 찾아냈다. AES 또는 AACS가 보호장치가 된 시청각 콘텐트(111)를 보호하기에 충분할 수 있음에도 불구하고, 컴퓨팅 기술과 암호해독 기술에서의 진보들은 장래에 기존방식과 다른 암호화 시스템이 더 선호되도록 만들 수 있다.

[0039] 인증서버(120)는 활성 데이터베이스(121)를 포함하며, 활성 데이터베이스(121)는 인증코드의 유효성 상태, 각각의 인증코드에 대응되는 워터마크 데이터, 미디어 플레이어 식별자들의 유효성 상태, 및 요청되는 인증과정을 수행하기 위하여 필요한 다른데이터를 포함한다. 비록, 도 1에서 인증서버(120)와 콘텐트 서버(110)는 분리되어 도시되어 있으나, 다른 선택적인 실시예에서 이 두개의 서버는 범용-목적 서버로 결합될 수 있다.

[0040] 네트워크(130)는 도 1에 포함된 콘텐트 서버(110), 인증서버(120) 및 미디어 플레이어와 같은 연결된 장치들 간의 데이터 통신을 제공한다. 네트워크(130)는 사유의 닫힌 네트워크일 수도 있으며, 또한 다양한 장소에 위치된 미디어 플레이어들에 대하여 광범위한 도달범위를 제공하는 인터넷과 같은 공중 접속이 가능한 네트워크가 될 수도 있다.

[0041] 미디어 플레이어(150)는 콘텐트 서버(110)와 인증서버(120)와 통신하기 위하여 도 1의 네트워크(130)에 대한 연결과 같은 네트워크 연결을 가진다. 따라서, 미디어 플레이어(150)는 인터넷 접속을 지원하는 BD-Video 프로파일 2.0(또는 더 상위 버전) 규격에 따른 플레이어가 될 수 있다. 콘텐트 서버(110)에 저장된 콘텐트의 분배를 제어하기 위하여, 예를 들어 특정 인증코드를 이용할 수 있는 미디어 플레이어의 최대 허용 숫자를 제한함으로써 연결된 각각의 미디어 플레이어를 고유하게 식별할 수 있도록 구성되는 것이 보다 바람직하다. 단순화된 시스템은 하나의 인증코드에 대하여 하나의 미디어 플레이어만을 허용하도록 구성될 수 있으나, 보다 유연하게 구성된 시스템은 보는 사람들이 다른 장소에 위치된 다른 플레이어를 이용하여 보안 스크리너 디스크를 볼 수 있도록 동일한 인증코드를 사용하는 부가적인 미디어 플레이어를 허용할 수도 있다. 예를 들어, 영화제의 심사위원은 집에서 또는 사무실에서 또는 휴대용 미디어 플레이어 통하여 영화를 관련할 수 있는 유연성을 희망한다. 이러한 희망을 달성하기 위하여, 미디어 플레이어(150)는 다른 미디어 플레이어들과 고유하게 구별되어야 할 필요성이 있다.

[0042] 미디어 플레이어(150)가 인증서버(120)에 의하여 다른 미디어 플레이어들과 구별될 수 있도록, 미디어 플레이어(150)는 다른 플레이어들과 구별될 수 있는 식별자를 생성할 수 있어야 한다. 인터넷 프로토콜(IP) 어드레스(151)와 미디어 맥세스 콘트롤(MAC) 어드레스(152)와 같은 표준의 그리고 활용이 보장된 네트워크 식별자들은 미디어 플레이어(150)를 식별하기에 적합할 수 있으나, 이러한 식별자들은 몇몇의 제한으로 인하여 항상 정확하게 동일 접속된 장치를 식별할 수 있는 것은 아니다. 예를 들어, 많은 네트워크 라우터들에서 일반적으로 사용되는 테크닉인 네트워크 변환(network translation)으로 인하여 하나의 아이피 어드레스는 복수의 장치들을 지칭할 수도 있다. 또한, 인터넷 서비스 사업자들은 지속적인 아이피 어드레스의 변화를 가져오는 프락시들과 동적 어드레스 할당과 같은 기술들을 채택할 수도 있다. 결정된 각각의 플레이어들은 그들의 인터넷 패킷들을 분

명한 아이피 어드레스로 변환한다. 부가적으로, 맥 어드레스도 개개의 장치에 대한 고유값으로 의도될수 있음에도 불구하고, 맥 어드레스레는 쉽게 변경된다. 따라서, 아이피 어드레스 뿐만 아니라 맥 어드레스도 특정 미디어 플레이어와의 관계에서 변경되지 않는 관계를 형성하는 것은 아니다.

[0043] 따라서, 부가적인 또는 선택적인 데이터의 조각들은 미디어 플레이어(150)를 식별함에 있어 보다 유용할 수 있다. 만일 미디어 플레이어(150)가 블루레이 디스크 플레이어와 같은 AACS 규격의 플레어이인 경우, ACCS 라이센싱 관리자(Licensing Administrator, LA)에 의하여 인증된 후 플레이어는 모델-특유 암호해독 키를 전달한다. 이러한 암호해독 키는 최소한의 서로 다른 플레이어 모델들 사이에서의 차별화를 가지지만, 만일 특정 플레이어 모델이 대중적인 경우 통상적으로 발생할 수 있듯이 동일한 모델의 다른 플레이어들 사이에서의 차별화에는 부적합하다. 따라서, 만일 미디어 플레이어(150)가 시리얼 넘버(153)와 같은 부가적인 플레이어 특유정보에 대한 질의를 지원하는 경우, 식별된 미디어 플레이어(150)의 고유성에 대하여 보다 높은 보증이 될 수 있다.

[0044] 미디어 플레이어(150)의 설계에 따르면, 저장장치(154)는 유저 콘텐트와 다운로드 콘텐트를 저장하기 위하여 제공된다. 이것은 관람자에게 영화의 다운로딩과 뒤에 영화를 관람할 편리한 시간을 선택함에 있어 유연성을 제공한다. 그러나 만일, 저장장치(154)의 용량이 제한되어 있거나 또는 완전히 생략되어 있다면, 어떠한 사소한 크기의 시청각 콘텐트의 다운로딩은 불가능하다. 이런 제한된 하드웨어의 경우에 있어, 실시간 주문형(on-demand) 스트림드 콘텐트는 다운로드 콘텐트 또는 보안 스크리너 디스크(160)의 대안으로서 기능할 수 있다.

[0045] 미디어 플레이어(150)는 각각 디스플레이(155)와 오디오 리시버(156)에 의하여 제공되는 영상 출력장치와 음성 출력장치를 포함한다. 디스플레이(155)는 HD티브이(high-definition television, HDTV) 또는 다른 LCD 모니터와 같은 고화질 고대역 디지털 콘텐트 보호(High-bandwidth Digital Content Protection, HDCP) 규격 디스플레이를 포함할 수 있다. 또한, 디스플레이(155)는 도 2에서 후술되는 것과 같은, 사용자와의 상호작용을 위한 사용자 인터페이스를 제공할 수 있다. 오디오 리시버(156)는 다채널 오디오 신호의 수신과 디코딩이 가능하고, 다채널 오디오 신호를 증폭하여 입체 환경 내에 위치된 복수의 스피커들로 출력할 수 있는 입체 사운드 리시버를 포함할 수 있다. 도 1에서는 디스플레이(155)와 오디오 리시버(156)가 직접적으로 미디어 플레이어(150)에 연결되는 것으로 도시되어 있으나, 또한 디스플레이와 오디오 리시버는 비디오 신호와 오디오 신호 모두의 전송이 가능한 일련의 하이-데피니션 멀티디미어 인터페이스(High-Definition Multimedia Interface, HDMI) 케이블 등을 이용하여 직렬연결 관통방식(daisy-chain pass-through fashion)으로 연결될 수도 있다. 이 경우에 있어, 미디어 플레이어(150)는 먼저 오디오 신호를 디코드하고 비디오 신호를 디스플레이(155)에 전송하는 오디오 리시버(156)에 연결된다. 비록 HDMI 케이블이 통상적으로 상호연결에 이용되지만, 디스플레이포트 또는 다른 앞으로의 표준들과 같은 오디오와 비디오에 대한 선택적 상호연결들 또한 이용될 수 있다. 선택적으로, 미디어 플레이어(150)는 내부 미디어 드라이버를 구비한 휴대용 컴퓨어 또는 플레이어와 HDTV가 결합된 경우와 같이 디스플레이(155)와 하나의 유닛으로 통합될 수도 있다.

[0046] 프로그램 데이터(161)를 포함하는 보안 스크리너 디스크(160)는 관람자에게 보호장치가 된 시청각 콘텐트(111)의 관람과정을 시작하도록 허락하는 요소들 중 하나이다. 인증과 콘텐트의 다운로드에 대해서는 네트워크(130)에 의존하도록 구성된 바, 보안 스크리너 디스크(160)는 그 자체에 어떠한 비디오 데이터도 포함하지 않는다. 따라서, 보안 스크리너 디스크(160)는 보호장치가 된 시청각 콘텐트(111)를 다운로드하기 위한 접속을 가능하게 하는 특유한 활성화 디스크와 같이 취급될 수도 있다.

[0047] 동일한 보안 스크리너 디스크(160)가 복수의 파티들에게 제공될 수 있으므로, 인증코드(165)는 특정 파티를 식별하는 부가적인 데이터 조각들을 제공한다. 인증코드(165)는 리모크 콘트롤과 같은 제한된 키를 가진 입력 수단을 이용한 용이한 입력이 가능하도록 알파벳과 숫자를 조합한 문자들 또는 단지 숫자로 구성되는 문자열을 포함할 수 있다. 인증코드(165)는 활성 데이터베이스(121) 내에서 생성, 저장되어야 하며, 제3자의 복제를 방해할 수 있는 방식으로 연관된 파티에게 제공되어야 한다. 예를 들어, 통상적으로 선지급 포인트 카드에 이용되는 바와 같은 불투명하고 제거가능한 레이어 아래에 인증코드가 존재하는 스크래치 카드가 이용될 수 있다. 이러한 스크래치 카드는 개인에게 직접 지급되거나 또는 항공우편으로 배달되거나 또는 기타 다른 배달 수단들을 이용하여 제공될 수 있다. 선택적으로, 네트워크(130)는 암호화된 이메일 또는 보안 소켓 레이어를 이용한 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol over Secure Socket Layer, HTTPS)과 같은 인증코드(165)에 대한 보안 분배 채널을 제공할 수 있다. 보안코드의 전송들은 나아가 관람파티(viewing party)의 동일성을 증명하기 위한 디지털 서명을 포함할 수 있다.

[0048] 도 2는 본 발명의 바람직한 일 실시예에 따른 보안 배달 시스템의 사용자 인터페이스 순서도이다. 사용자 인터

페이스(200)는 디스플레이(255a), 디스플레이(255b), 디스플레이(255c), 및 디스플레이(255d)를 포함하고, 각 디스플레이는 도 1로부터 디스플레이(155)의 가능한 환경설정을 나타낸다. 디스플레이(255a)로부터, 디스플레이(255b), 디스플레이(255c), 디스플레이(255d), 또는 도 2에 도시되지 않은 다른 사용자 인터페이스 상태로 변환되는 것이 가능하다. 유사하게, "Back" 버튼을 선택하거나 또는 리모트 콘트롤 또는 키보드의 백 버튼과 같은 뒤쪽 방향을 탐색하는 어떤 다른 수단을 이용함으로써, 디스플레이(255b), 디스플레이(255c) 및 디스플레이(255d)로부터 디스플레이(255a)로 복귀하는 것도 가능하다.

[0049] 디스플레이(255a)는 사용자가 인증코드를 입력하기 위한 환영화면을 묘사하고 있다. 이러한 환영화면은 도 1에서의 보안 스크리너 디스크(160)가 미디어 플레이어(150)에 삽입된 직후 즉시 표시될 수 있다. 현재 이러한 인터페이스에 대한 프로그램은 도 1의 프로그램 데이터(161) 내에 화체되어 있거나, 또는 보안 스크리너 디스크(160)가 단지 원격서버에 접속하기 위한 인터페이스를 제공하도록 인증서버(120)와 같은 원격서버에 저장될 수 있다. 예를 들어, 보안 스크리너 디스크(160)는 원격적으로 제공되는 웹기반의 사용자 인터페이스를 지칭하는 특정한 유알엘(Uniform Resource Locator, URL)에 접속할 수 있다. 사용자가 인증코드(도 2에서의 "123456790")를 입력하고 "확인" 버튼을 선택하면, 사용자 인터페이스는 인증서버(120)의 결과에 따라 다수의 상이한 상태들을 이행할 수 있다.

[0050] 디스플레이(255b)는 유효하지 않은 인증코드에 의하여 자동적으로 문제가 발생하거나 또는 관리자의 초기화에 의하여 문제가 발생한 경우를 도시한다. 예를 들어, 인증코드는 특정 기간이 경과하면 인증코드를 자동적으로 소멸시키는 유효 기간을 가질 수 있다. 예를 들어 영화제에 사용하는 경우, 유효기간은 관련된 수상식의 개최일에 종료될 수 있다. 선택적으로, 관리자는 수동으로 강력한 손실 또는 도난된 인증코드 및/또는 보안 스크리너 디스크와 같은 특별한 사고들의 어드레스에 대하여 실효를 명령할 수도 있다. 예를 들어, 만일 인증코드가 운송수단을 이용하여 발송되고 운송 중 분실된 경우, 인증되지 않은 제3의 파티에 의하여 인증코드가 이용되는 것을 방지하기 위하여 그 특정한 인증코드는 실효될 수 있다. 그 관련된 인증코드를 실효시킴으로써, 보안 스크리너 디스크들의 각각 또는 집합은 즉시 무효화 된다.

[0051] 디스플레이(255c)는 유효한 특정 인증코드에 대한 미디어 플레이어의 최대 허용 수량이 존재하는 경우를 도시한 것이다. 예를 들어, 동일한 시간, 어떤 장소에서 3대의 동시 활성화된 미디어 플레이어에 대한 제한이 존재할 때, 디스플레이(255c)는 사용자가 4번째 미디어 플레이어를 활성화시키고자 하는 경우를 나타낸다. 따라서, 활성화된 미디어 플레이어가 비활성화될 때까지, 부가적인 미디어 플레이어는 동일한 인증코드를 사용할 수 없다. 수량 제한은 비인증 관람에 대항하는 향상된 보안에 대한 다수의 장소에서의 재생 유연성의 경쟁적 이득의 균형을 맞추도록 조정될 수 있다. 부가적으로, 만일 개별적인 미디어 플레이어가 평균적인 사용자에 비하여 보다 높은 최대수량을 필요로하는 특별한 요구가 있는 경우, 수량 제한은 사례별로 조정될 수 있다. 나아가, 몇몇의 실시예에 있어, 부가적인 수량 제한은 콘텐트가 관람되는 횟수에 대한 제한을 포함할 수 있다.

[0052] 디스플레이(255d)는 도 1의 인증서버(120)가 제공된 인증코드로부터 문제점을 발견하지 못한 경우, 연결된 미디어 플레이어를 활성화하고 보호장치가 된 콘텐트에 접근을 허용하는 것을 도시한 것이다. 디스플레이(255d)에 도시된 바와 같이, 보호장치가 된 콘텐트는 복수의 분리된 선택들을 포함할 수 있으며, 실시간 스트리밍 또는 추후 관람을 위한 다운로드와 같은 서로 상이한 배달 옵션을 제공한다. 부가적으로, 사용자가 최대 미디어 플레이어 수량제한에 도달한 경우, 연결된 미디어 플레이어에 대한 비활성화 옵션이 선택되면, 오래된 미디어 플레이어는 비활성화되고 사용자가 희망하는 새로운 미디어 플레이어가 활성화된다.

[0053] 사용자가 관람 콘텐트를 선택하고 재생을 시작하면, 도 3a에서의 확장된 뷰(view)와 유사하게 구성되는 비디오 프레임들이 도 1의 디스플레이(155) 상에 보여진다. 도 3a는 본 발명의 일 실시예에 따라, 보안 배달 시스템의 미디어 플레이어에 의하여 플레이되는 비디오 프레임의 확장된 묘사를 나타낸다. 비디오 프레임(300)은 비디오 레이어(video layer)(370), 인지할 수 없는 워터마크(371), 및 인지할 수 있는 워터마크(372)를 포함한다. 비디오 레이어(370)은 도 1의 보호장치가 된 시청각 콘텐트(11)로부터의 실질적인 비디오 콘텐트의 프레임을 포함한다. 그러나, 이러한 비디오 레이어 위에 겹쳐 놓여지는 부가적인 워터마크 레이어들은 비인증 분배를 방해하고 누설이 일어난 경우에 과학적인 수사의 출처 증거를 제공하도록 기능한다. 누설 출처를 목적으로한 필요성이 있는 경우, 워터마크들이 정확한 인증코드들과 연관될 수 있도록, 인증서버(120)는 이러한 워터마크 레이어들을 활성 데이터베이스(121) 내에서 생성하고 저장한다. 인증서버(120)는 미디어 플레이어(150)로 워터마크 레이들을 공급할 수 있으며, 여기서 비디오 스트림은 실시간 비디오 오버레이를 이용하여 워터마크 레이어들과 합성될 수 있다. 비디오 오버레이들이 같이 합성될 때, 비디오 프레임은 시각적으로 덜 두드러질 수 있는 인지할 수 없는 워터마크(371)를 제외하면 도 3b의 비디오 프레임(300)과 유사하게 보일 수 있다.

[0054] 도 3a에 도시된 바와 같은 인지할 수 없는 워터마크(371)는 점들의 패턴(pattern of dots)을 제외하면 대부분 투명할 수 있다. 이러한 점들의 패턴은 도 1의 보호장치가 된 시청각 콘텐트(111) 내에서 특별히 정의된 시간들에 특별히 정의된 XY 좌표들로 정확한 방식으로 배열될 수 있으며, 일반적인 관람환경에서 육안으로 이러한 패턴들을 검출하기 어려운 방식으로 형성될 수 있다. 그러나, 기계적 지원을 받는 이미지 프로세싱의 도움으로 인하여, 이러한 패턴들이 검출될 수 있다. 이러한 인지할 수 없는 워터마크의 삽입으로 인하여, 인증코드와 같은 콘텐트 분배에 관련된 데이터는 실질적인 비디오 프레임들 내에 은밀하게 삽입될 수 있다. 이러한 정보는 가능한 누설 출처들을 추적하고 고립시키는데 유용할 수 있다. 예시적으로 점들이 주어졌으나, 특정 시간의 특정 위치의 일정한 컬러 음영들의 미세한 변화 또는 미리 결정된 방식에 따른 광도의 변화와 같은 비디오 프레임 내에 삽입되는 인지할 수 없는 데이터에 대한 다른 방법들 또한 이용될 수 있다.

[0055] 도 3a에 도시된 바와 같은 인지할 수 있는 워터마크(372)는 우발적인 복제에 대한 억제물로서 기능하는 가시적인 식별정보를 포함한다. 도 3a에 도시된 바와 같이, 이 경우 "James Jaeger(ID 1234)"라는 인증코드와 연관된 파티를 식별하는 가시적인 텍스트가 오버레이된다. 부가적으로, "Property of Northen Entertainment"는 저작권자를 식별하고, 만일 비인증 분배가 발생하는 경우 저작권자가 자신의 저작권을 행사할 수 있음을 관람자에게 전달한다. 이러한 텍스트 오버레이들은 크기 또는 폰트를 변화시키거나, 스크리 주변으로 움직일 수 있으며, 그렇지 않으면 다른 방법으로 오버레이들의 간단한 방해 또는 상실을 방지하기 위하여 고정되어 있지 않을 수 있다. 부가적으로, 이러한 텍스트의 움직임은 플라즈마 텔레비젼과 같은 특별한 디스플레이 기술에서 민감한 이미지 잔류를 방지하는데 도움이 될 수 있다.

[0056] 워터마크 데이터 표현에 대하여, 스크립팅 메타데이터, 비디오 트랙 분할, 또는 변환정보를 구비한 일련의 이미지들와 같은 다양한 기술들이 이용될 수 있다. 워터마크 데이터 기술에 대한 가능한 반대 기술을 방지하기 위하여, 워터마크 데이터는 단지 미디어 플레이어(150)의 임시 메모리에 저장되거나, 또는 저장장치(154)에 암호화되고 보호된 상태로 저장되거나 또는 다른 방식으로 분석하기 어렵고 난해하게 저장될 수 있다. 특정한 데이터 표현이 선택되면, 대응되는 실행방법이 부호화될 수 있다. BD-J(또는 블루레이 디스크 자바(Blu-ray Disc Java))는 블루레이 디스크 포맷으로 저장된 보안 스크리너 디스크에 대하여 오버레이 지원을 프로그램적으로 실행하는데 이용될 수 있다. 따라서, 특정하게 선택된 데이터 표현을 처리할 수 있도록 작성된 자바코드는 도 1의 프로그램 데이터(161)에 삽입될 수 있다. BD-J에 기반한 하이레벨 프레임워크 또한 이용될 수 있다. 선택적으로, 만일 미디어 플레이어(150)가 작동 중 프레임들을 합성하는 능력이 결여되는 경우, 인증서버(120) 또는 콘텐트 서버(110)는 합성 프레임들의 사전조합이 가능할 수도 있다. 또한, 오버레이들의 사전조합은 워터마크 데이터를 미디어 플레이어(150)로 전송하는 것을 회피할 수 있으며, 나아가 워터마크들에 대한 반대 기술을 보다 어렵게 할 수 있다.

[0057] 도 4는 본 발명의 바람직한 일 실시예에 따른 무효화 가능 접속을 이용한 보안 콘텐트 활용에 따른 네트워크를 통한 보호장치가 된 시청각 콘텐트의 접근 및 재생이 가능한 미디어 플레이어의 동작 단계를 도시한 순서도이다. 본 발명이 속하는 기술분야에서 통상의 지식을 가지는 자에게 자명한 세부항목들과 특징들은 순서도(400)로부터 배제되었다. 예를 들어, 하나의 단계는 당업계에서 자명한 하나 또는 복수의 하위단계들을 포함하거나 또는 특화된 장치 또는 물질들을 수반할 수 있다. 순서도(400)에서 지칭되고 있는 410 단계에서 470 단계는 본 발명에 따른 하나의 실시예를 설명하기에 충분하며, 본 발명의 다른 실시예들은 순서도(400)에서 도시되고 있는 것과 다른 방식으로 단계들을 이용할 수 있다. 미디어 플레이어(150)의 프로세서(157)는 410 단계에서 470 단계를 수행하도록 구성된다.

[0058] 영화제에 대한 예시에 계속하여, 그들의 최신작 "The Tetrahedron"에 대한 촬영을 완료하고 그들의 작품을 영화제의 심사위원들에게 분배하기 원하는 "Northern Entertainment"라는 독립 영화 제작사를 가정한다. 나아가, 영화 심사위원들 중 한명은 아이디 넘버 "1234"를 가지는 "James Jaeger"이다. Northern Entertainment는 제임스가 "The Tetrahedron"를 관람할 수 있도록 제임스에게 보안 스크리너 디스크(160)와 인증코드(165)를 제공하기 원한다. 따라서 관리자는 인증코드(165)와 연결된 제임스와 노썬 엔터테인먼트의 정보를 활성 데이터베이스(121)에 입력할 것이다. 예시적인 목적으로, 인증코드(165)는 도 2에 도시된 바와 같은 "123456790"라는 아라비아 숫자의 문자열로 표현될 수 있다.

[0059] 제임스에게 "The Tetrahedron" 관람에 필요한 아이템을 제공하기 위한 준비에 있어서, 약간의 단계들이 먼저 완료되어야 한다. 먼저, "The Tetrahedron"의 원본 영화 데이터가 비디오와 돌비 디지털 오디오를 부호화하는 H.264와 같은 적합한 포맷으로 부호화될 필요가 있다. 부호화들의 서로 다른 집합들은 예를 들어 대량의 고화질 다운로드와 저속 네트워크 연결에 적합한 저화질 실시간 스트림을 제공하는 것과 같은 서로 다른 다운로드 속도에 적합하도록 생성될 수 있다. 다음으로, 무차별적인 복제와 재생에 대하여 보호장치를 제공하기 위하여 부호

화된 비디오들은 암호화되어야 한다. 이러한 단계들이 완료된 후, 비디오들은 보호장치가 된 시청각 콘텐트(111)로서 콘텐트 서버(110)에 저장될 수 있다. 이러한 지점에서, 제임스에게 보안 스크리너 디스크(160)와 인증코드(165)를 자신 있게 제공할 수 있는 환경이 충분히 구성된다.

[0060] 도 4의 순서도(400)의 410 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 410 단계는 보안 스크리너 디스크(160) 또는 컴퓨터로 판독할 수 있는 기록매체로부터 프로그램 데이터(161)를 실행하는 미디어 플레이어(150)를 포함한다. 이러한 단계가 실행되기 전에, 제임스는 프로그램 데이터(161)가 판독될 수 있도록 보안 스크리너 디스크(160)를 미디어 플레이어(150)에 삽입해야 한다. 프로그램 데이터(161)가 판독되면, 미디어 플레이어(150)의 프로세서(157)는 제임스에게 노썬 엔터테인먼트로부터 제공된 "The Tetrahedron"에 접근하고 관람하는 과정의 시작을 허용하는 프로그램 데이터(161)에 포함된 코드의 실행을 시작할 수 있다.

[0061] 도 4의 순서도(400)의 420 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 420 단계는 제임스에게 인증코드(165)의 입력을 요청하는 미디어 플레이어(150)를 포함한다. 이러한 입력창은 디스플레이(155)에 표시되고, 도 2의 디스플레이(255a)와 유사하게 나타날 수 있다. 제임스로부터의 인증코드(165) 입력에 리모트 콘트롤 또는 키보드와 같은 입력장치가 이용될 수 있다.

[0062] 도 4의 순서도(400)의 430 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 430 단계는 420 단계로부터의 인증코드와 미디어 플레이어 식별자를 네트워크(130)를 통해 인증서버(120)로 전송하는 미디어 플레이어(150)를 포함한다. 전술한 바와 같이, 미디어 플레이어 식별자는 미디어 플레이어(150)의 고유한 식별을 위한 하나의 상이한 데이터 순열이 될 수 있다. 가능한 모든 식별자들의 이용에 의해, 아이피 어드레스(151), 맥 어드레스(152) 및 시리얼 넘버(153)는 단일 미디어 식별자로 결합될 수 있다. 또한, 인증서버(120)는 미디어 플레이어 식별자 해석에 있어 어느 정도의 유연성을 허용할 수 있다. 예를 들어, 대부분의 사용자들은 동적 변환 어드레스를 가지고 있으므로, 아이피 어드레스(151)에 대한 어느 정도의 변환은 허용될 수 있다. 부가적으로, 인터넷 서비스 사업자들(ISPs)은 어떠한 사용자의 동작이 없더라도 프락시들(proxies)을 통하여 아이피 어드레스와 경로를 재설정할 수 있다.

[0063] 도 4의 순서도(400)의 440 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 440 단계는 430 단계로부터의 인증코드와 미디어 플레이어 식별자가 유효한 것으로 확인되는 경우, 네트워크(130)를 통하여 인증서버(120)로부터의 유효 인증 메세지를 수신하는 미디어 플레이어(150)를 포함한다. 따라서 인증서버(120)는 인증코드(165)의 존재여부, 철폐여부 및 활성화된 플레이어의 수가 일정한 연관된 한계를 초과하는지 여부를 활성 데이터베이스(121)에 문의할 수 있다. 따라서 미디어 플레이어 식별자는 최대 활성화 플레이어들의 제한을 실행함에 도움이 되도록 고유 활성화 플레이어들 사이에서의 구별에 이용된다.

[0064] 만일 인증코드(165)가 여전히 유효한 경우, 도 2의 디스플레이(255d)가 나타난다. 그러나, 제3의 파티에 의한 인증코드(165)의 의심스러운 손상과 같은 장래의 사건들은 인증코드(165)의 무효화를 유발할 수 있다. 이러한 경우에, 관리자는 인증코드를 즉시 무효화하도록 인증서버(120)에 지시하고 도 2의 디스플레이(255b)를 나타내거나, 또는 만일 제임스가 그에게 할당된 활성화 미디어 플레이어의 최대 수량에 도달한 경우 제임스에게 그의 제한수량에 도달되었음을 알려주기 위하여 도 2의 디스플레이(255c)가 나타나도록 할 수 있다. 예를 들어, 만일 제임스가 이전에 그의 가정극장의 미디어 플레이어와 직장의 미디어 플레이어를 활성화 시켰다면, 노썬 엔터테인먼트가 동일한 두대의 플레이어 최대 제한수량을 부과하기로 결정했으므로 그의 형제의 집에서의 세번째 미디어 플레이어 활성화 시도는 실패할 수 있다. 이 경우, 제임스는 그의 형제 집에서 영화를 관람하기 전에 그의 사무실 또는 집의 미디어 플레이어를 비활성화시킬 필요가 있다. 인증서버(120)는 나아가 불법적인 남용으로부터 그러한 기능을 방지하기 위하여 지나친 활성화와 비활성화 행동을 검출하고 방지할 수 있도록 구성될 수 있다. 제임스가 성공적으로 유효한 인증코드(165)를 제출하면, 미디어 플레이어(150)는 인증서버(120)로부터 유효한 인증 메세지를 수신한다.

[0065] 도 4의 순서도(400)의 450 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 450 단계는 440 단계로부터의 유효한 인증 메세지를 네트워크(130)를 통하여 콘텐트 서버(110)로 전송하는 미디어 플레이어(150)를 포함한다. 이 단계는 제임스가 궁극적으로 보호장치가 된 시청각 콘텐트(111)인 "The Tetrahedron"에 접근할 수 있도록 하기 위하여 유효한 적격을 콘텐트 서버(110)에 제출하는 것으로 완료된다. 또한, 440 단계와 450 단계는 중계를 통하여 미디어 플레이어(150) 없이 수행될 수도 있다.; 즉, 450 단계의 필요를 해소하기 위한 440 단계로부터의 유효 인증 메세지가 직접적으로 콘텐트 서버(110)로 전송될 수 있다. 만일 이러한 선택적인 방법이 이용되는 경우, 보호장치가 된 시청각 콘텐트(111)에 대한 목적으로 제공되는 430 단계로부터의 미디어 플레이어 식별자 또한 콘텐트 서버(110)로 전송될 수 있다.

[0066] 도 4의 순서도(400)의 460 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 460 단계는 네트워크(130)를 통하여 콘텐트 서버(110)로부터, 인증서버(120)로부터 보호장치가 된 시청각 콘텐트(111)를 읽어들이는 미디어 플레이어(150)를 포함하고, 여기서 보호장치가 된 시청각 콘텐트(111) 또는 미디어 콘텐트는 워터마킹 미디어 콘텐트와 같이 미디어 콘텐트와 연관된 식별정보를 사용자와 통합한다. 전술한 바와 같이, 읽어들임은 실시간 스트리밍 어플리케이션들을 이용하여 재생과 동시에 발생하거나 또는 재생단계는 미디어 플레이어(150)의 저장장치의 용량과 사용자의 요구에 따라 460 단계가 완료될 때까지 연기될 수도 있다. 도 2의 디스플레이(255d)와 유사하게 단일 인증코드로부터 몇몇의 아이템들에 대한 접근을 허용할 수 있도록 상이한 콘텐트의 선택 또한 사용자에게 제공될 수 있다. 만일 제임스가 "The Tetrahedron"를 저장장치(154)에 다운로드하기로 결정한 경우, 보안 스크리너 디스크(160)는 장래의 재생을 허용하기 전에 인증코드(165)이 여전히 유효한지에 대한 확인을 위하여 미디어 플레이어(150)가 인증서버(120)에 접속하도록 지시할 수 있다. 만일 인증코드(165)가 무효화된 경우, 보안 스크리너 디스크(160)는 저장장치(154)로부터 "The Tetrahedron"를 삭제하도록 미디어 플레이어(150)에 지시할 수 있다.

[0067] 전술한 바와 같이, 460 단계에서 읽혀진 워터마크는 비디오 콘텐트 위에 오버레이드되는 인식가능한 워터마크와 인식불가능한 워터마크를 포함할 수 있다. 선택적으로, 분리된 워터마크를 읽어들일 필요가 없는 경우에 있어, 워터마크는 이미 보호장치가 된 시청각 콘텐트(111)에 미리 오버레이드될 수 있다. 보안성의 제고를 위하여, 워터마크들을 생성하는 알고리즘은 워터마크들이 반대되는 기술에 의하여 제거되는 경우에 있어 워터마크 제거의 영향력을 최소화하기 위하여 주기적으로 또는 요구에 따라 변경될 수 있다.

[0068] 미디어 플레이어(150)가 보호장치가 된 시청각 콘텐트(111)를 수신하면, 콘텐트의 암호해독을 위한 몇몇의 방법이 필요하다. 예를 들어, 만일 보호장치가 된 시청각 콘텐트(111)가 콘텐트 보호를 위하여 AACS를 이용한 경우, 그리고 미디어 플레이어(150) 또한 AACS를 이용한 경우, 보호장치가 된 시청각 콘텐트의 암호해독에 필요한 암호해독 키는 미디어 플레이어(150) 상에 이미 존재하고 있어야 하며, 키의 공유와 분배에 대한 문제는 미리 해결되어 있어야 한다. 그러나, 만일 콘텐트 보호를 위하여 다른 방법이 사용된 경우, 콘텐트 서버(110), 인증서버(120) 및 미디어 플레이어(150)는 보호장치가 된 시청각 콘텐트(111)의 암호해독에 대한 암호화 프로토콜들에 대한 협의를 해야할 필요가 있을 수 있다. 예를 들어 인터넷과 같은 네트워크는 공개적이고 불안할 수 있기 때문에 중계자로 믿어지는 부가적인 제3의 파티 또한 네트워크(130)에 연결된 장치들에 대한 보안 서비스들을 제공할 필요가 있을 수 있다. 이 경우, 공개키 기반구조(public key infrastructure, PKI)는 동일성들을 인증하기 위해 필요한 지원을 제공할 수 있으며, 네트워크(130)를 통해 연결된 장치들 간의 메세지들을 암호화할 수 있다.

[0069] 도 4의 순서도(400)의 470 단계와 도 1의 보안 배달 시스템(100)을 참조하면, 순서도(400)의 470 단계는 460 단계로부터 읽혀지는 콘텐트와 워터마크를 이용하여 워터마크를 포함하는 오버레이가 구비된 보호장치가 된 시청각 콘텐트(111)를 재생하는 미디어 플레이어(150)를 포함한다. 도 3a를 참조하면, 재생 프레임은 암호해독된 보호장치가 된 시청각 콘텐트(111)를 포함하는 비디오 레이어(370)와 읽혀진 워터마크를 포함하는 인지할 수 없는 워터마크(371) 및 인지할 수 있는 워터마크(372)를 구비한 비디오 프레임(300)과 유사하게 보일 수 있다. 전술한 바와 같이, 보안 스크리너 디스크 상의 프로그램 데이터(161)는 작동 중인 비디오 프레임(300)과 유사하게 비디오 프레임들을 합성하도록 미디어 플레이어(150)에 지시를 하기 위한 BD-J코드 또는 몇몇의 다른 메커니즘을 포함할 수 있다. 만일 460 단계에서 워터마크 합성이 미리 종료된 경우, 보호장치가 된 시청각 콘텐트(111)는 이미 비디오 레이어(370) 내에 통합된 인지할 수 없는 워터마크(371)와 인지할 수 있는 워터마크(372)를 가지고 있으며, 따라서 미디어 플레이어(150)는 비디오 스트림에 대한 후속 과정이 필요하지 않게 된다. 따라서, 470 단계가 완료된 후, 제임스는 영화제에서의 그의 심사를 위하여 제임스의 법적 의무들을 상기시키는 인식할 수 있는 워터마크와 제임스가 그것들의 의무들을 무시하기로 결정한 경우에 있어 노썬 엔터테인먼트를 위한 보험 수단을 제공하는 인식할 수 없는 워터마크를 구비한 "The Tetrahedron"를 관람할 수 있다.

[0070] 본 발명의 다양한 실시예의 장점들 중 일부로서, 콘텐트 제작자들이 비용대비 효율이 우수하고, 보호장치가 되어 있으며, 무효화가 가능한 방식으로 청중들에게 판촉할 수 있고 결과적으로 재정상의 자원을 보존하며, 보호장치가 된 자료들의 우연한 복제를 방지하고, 만일 콘텐트 누설이 발생한 경우 뜻밖의 사고에 대한 계획을 제공하는 보안 스크리너 디스크들 또는 다른 수단들을 통한 보안 콘텐츠의 분배가 가능하다는 것이다. 일 실시예에 있어, 각각의 수령인에 대하여 커스터마이즈된 데이터를 구비하는 물리적인 매체는 더 이상 창조될 필요성이 없으므로, 일반적인 스크리너 디스크들의 분배는 상업적인 미디어에 대한 비용 효율이 우수한 대량 생산 기술들에 영향을 줄 수 있다. 유사하게, 산업과 소비자들에 의하여 광범위하게 채택된 표준 콘텐트 포맷들과 미디어들이 이용될 수 있으므로, 재생과 분배는 소매 채널들에서 광범위하게 이용이 가능한 필수적인 하드웨어를 이용함으

로써 용이하게 달성될 수 있다. 네트워크 연결의 도움으로 인하여, 그러한 표준 규격 하드웨어가 각각의 수령인에 대하여 우발적인 불법 분배에 대한 효과적인 장애물을 제공하는 고유의 워터마크들을 삽입할 수 있다. 고립된 사건들이 눈사태처럼 큰 재앙이되는 것을 방지하는 즉각적인 관련 인증코드들의 무효화로 인하여 콘텐트 누설 피해는 쉽고 단순하게 제어될 수 있다. 부가적으로, 누설된 자료들에 포함된 인식불가능한 워터마크들의 존재는 누설 출처를 결정함에 있어 가치있는 법적 증거를 제공할 수 있다.

[0071] 본 발명에 대한 이상의 설명으로부터, 본 발명의 범위로부터 벗어나지 않고 본 발명의 개념들을 실행하기 위한 다양한 기술들이 사용될 수 있다는 것은 명백하다. 나아가, 특정 실시예에 대한 구체적인 참조와 함께 본 발명이 설명되었다고 할 지라도, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명의 범위와 기술적 사상 내에서 다양한 형태의 변형이 가능함을 인식할 수 있을 것이다. 이와 같이, 설명된 실시예들은 모든 점에 있어 예시적으로 간주되어야 하며, 제한적으로 간주되어서는 안될 것이다. 또한, 본 발명은 여기서 설명된 특정한 실시예들에 한정되는 것이 아니라, 본 발명의 범위로부터 벗어나지 않는 범위에서의 다양한 재배열들, 변형들, 그리고 치환이 가능함이 이해되어야 할 것이다.

도면의 간단한 설명

[0072] 도 1은 본 발명의 바람직한 일 실시예에 따른 무효화 가능 접속과 보안 콘텐트를 이용하기 위한 보안 배달 시스템의 구성 블록도.

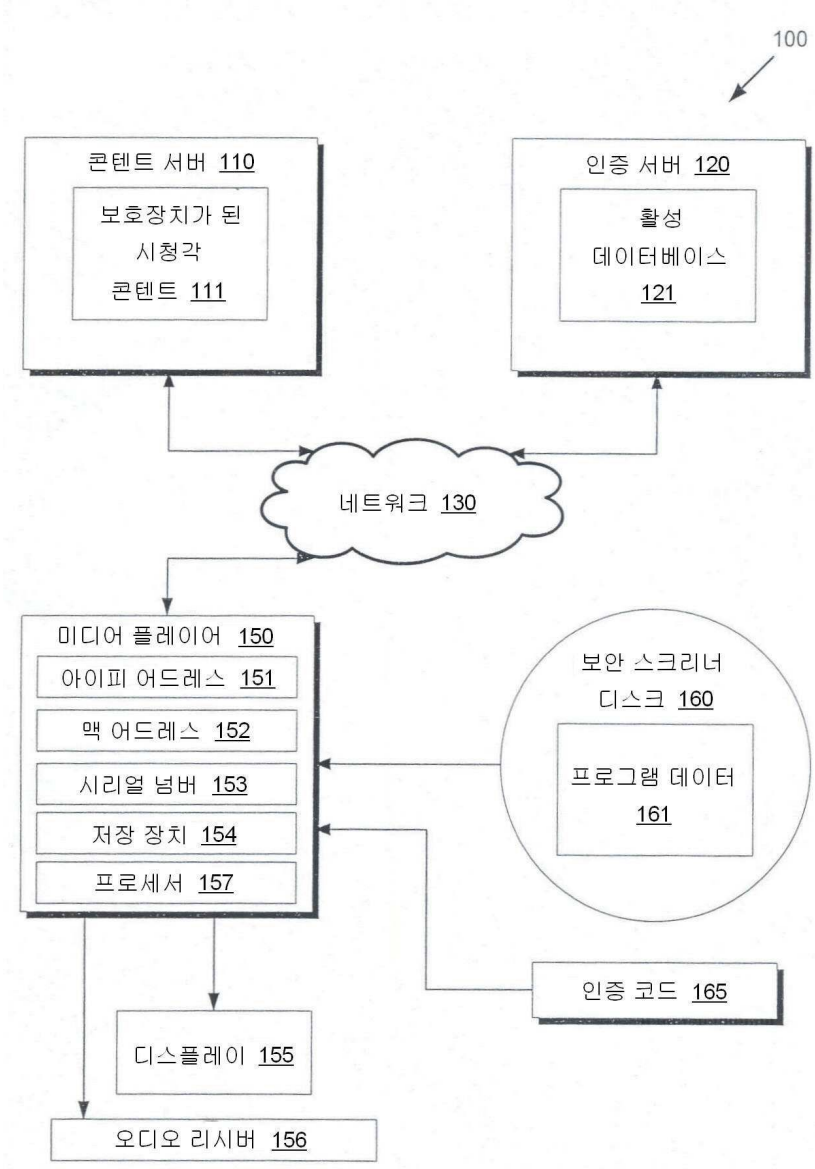
[0073] 도 2는 본 발명의 바람직한 일 실시예에 따른 보안 배달 시스템의 사용자 인터페이스 순서도.

[0074] 도 3a와 도 3b는 은 본 발명의 바람직한 일 실시예에 따른 미디어 플레이어를 통해 플레이되는 비디오 프레임의 묘사도.

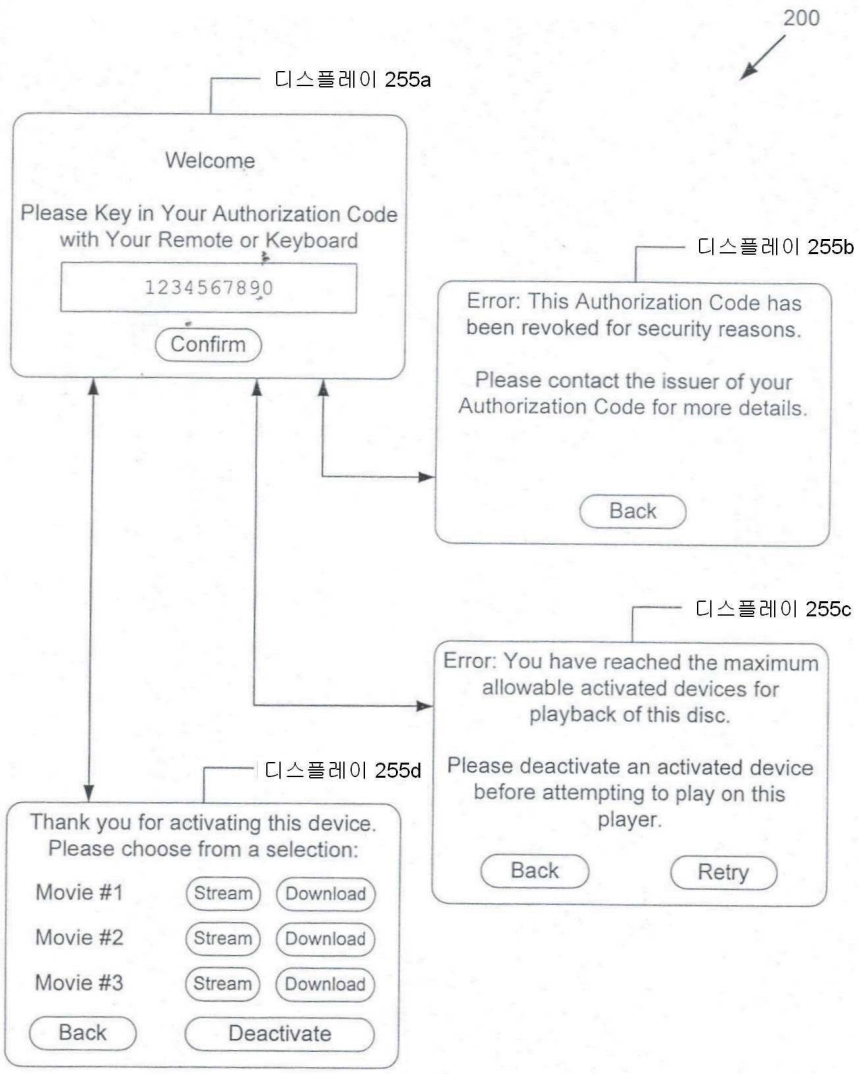
[0075] 도 4는 본 발명의 바람직한 일 실시예에 따른 무효화 가능 접속을 이용한 보안 콘텐트 활용에 따른 네트워크를 통한 보호장치가 된 시청각 콘텐트의 접근 및 재생이 가능한 미디어 플레이어의 동작 단계를 도시한 순서도.

도면

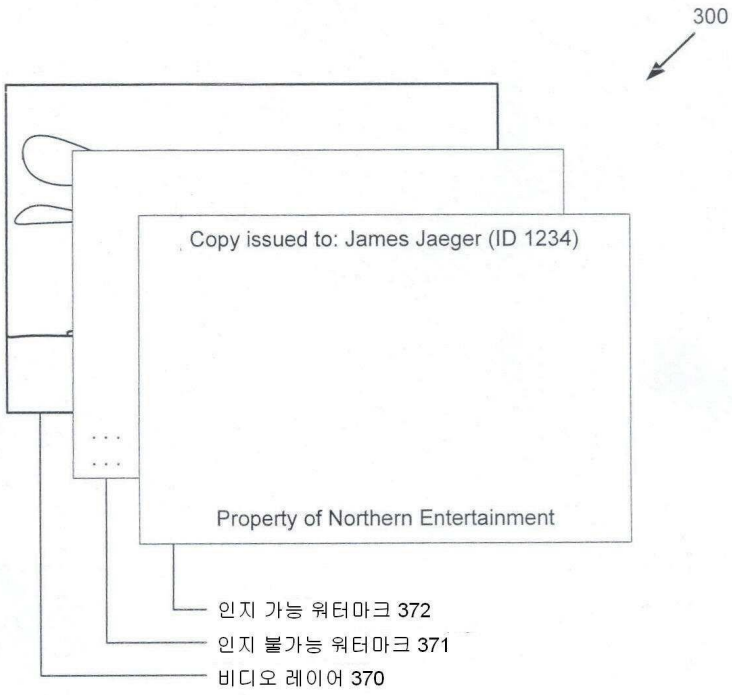
도면1


100
콘텐트 서버 110
보호장치가 된
시청각
콘텐트 111
인증 서버 120
활성
데이터베이스
121
네트워크 130
미디어 플레이어 150
아이피 어드레스 151
맥 어드레스 152
시리얼 넘버 153
저장 장치 154
프로세서 157
보안 스크리너
디스크 160
프로그램 데이터
161
인증 코드 165
디스플레이 155
오디오 리시버 156

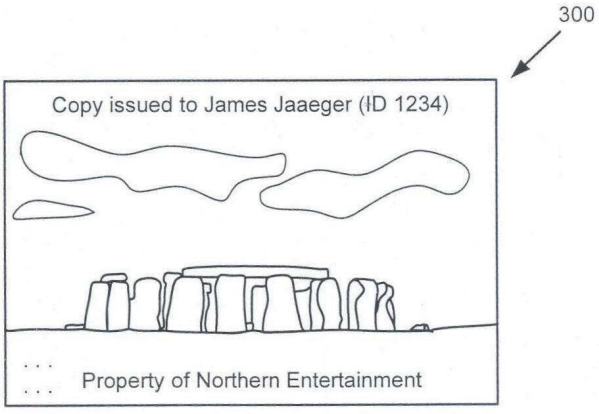
도면2


200
디스플레이 255a
Welcome
Please Key in Your Authorization Code with Your Remote or Keyboard
1234567890
Confirm
디스플레이 255b
Error: This Authorization Code has been revoked for security reasons.
Please contact the issuer of your Authorization Code for more details.
Back
디스플레이 255c
Error: You have reached the maximum allowable activated devices for playback of this disc.
Please deactivate an activated device before attempting to play on this player.
Back
Retry
디스플레이 255d
Thank you for activating this device. Please choose from a selection:
Movie #1
Stream
Download
Movie #2
Stream
Download
Movie #3
Stream
Download
Back
Deactivate

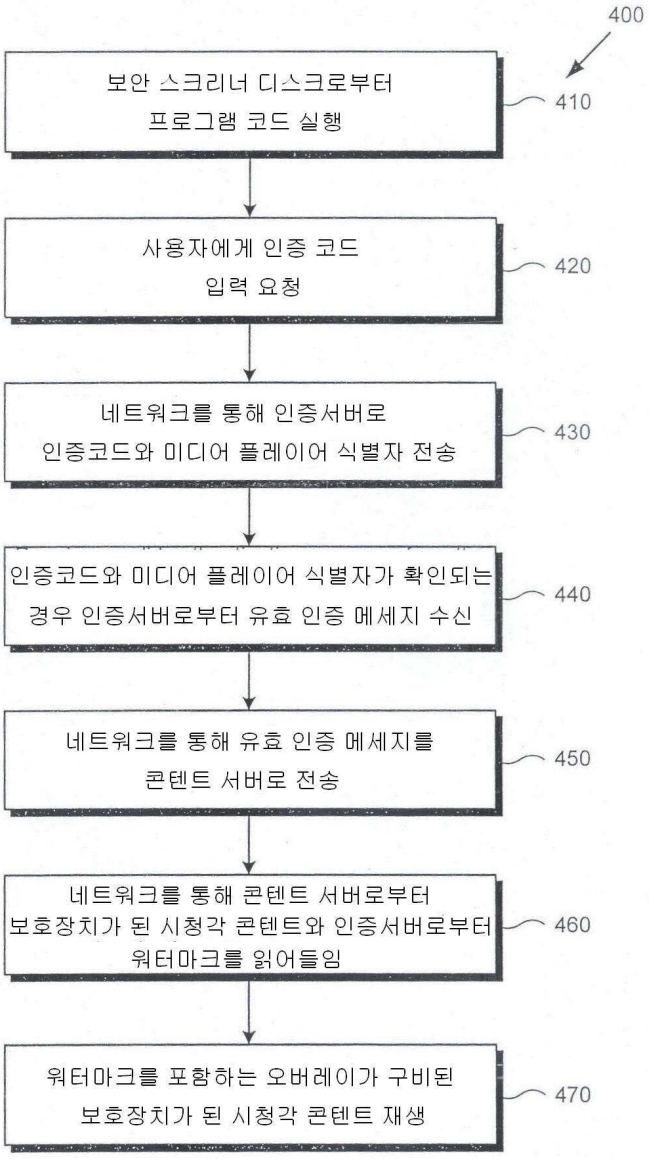
도면3a


300
Copy issued to: James Jaeger (ID 1234)
Property of Northern Entertainment
인지 가능 워터마크 372
인지 불가능 워터마크 371
비디오 레이어 370

도면3b


300
Copy issued to James Jaaeger (ID 1234)
Property of Northern Entertainment

도면4


400
보안 스크리너 디스크로부터
프로그램 코드 실행
410
사용자에게 인증 코드
입력 요청
420
네트워크를 통해 인증서버로
인증코드와 미디어 플레이어 식별자 전송
430
인증코드와 미디어 플레이어 식별자가 확인되는
경우 인증서버로부터 유효 인증 메세지 수신
440
네트워크를 통해 유효 인증 메세지를
콘텐트 서버로 전송
450
네트워크를 통해 콘텐트 서버로부터
보호장치가 된 시청각 콘텐트와 인증서버로부터
워터마크를 읽어들임
460
워터마크를 포함하는 오버레이가 구비된
보호장치가 된 시청각 콘텐트 재생
470