(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년04월17일
(11) 등록번호 10-1255395
(24) 등록일자 2013년04월10일

(51) 국제특허분류(Int. Cl.)
G06F 17/30 (2006.01) *G06F 17/00* (2006.01)
H04K 1/00 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2008-7000503
(22) 출원일자(국제) 2006년07월11일
심사청구일자 2011년06월13일
(85) 번역문제출일자 2008년01월08일
(65) 공개번호 10-2008-0024192
(43) 공개일자 2008년03월17일
(86) 국제출원번호 PCT/US2006/026915
(87) 국제공개번호 WO 2007/008914
국제공개일자 2007년01월18일
(30) 우선권주장
11/276,496 2006년03월02일 미국(US)
60/698,525 2005년07월11일 미국(US)
(56) 선행기술조사문헌
KR1020040000323 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
피어스타인, 스코트 제이.
미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이
에반스, 브라이언 피.
미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이
(뒷면에 계속)
(74) 대리인
제일특허법인

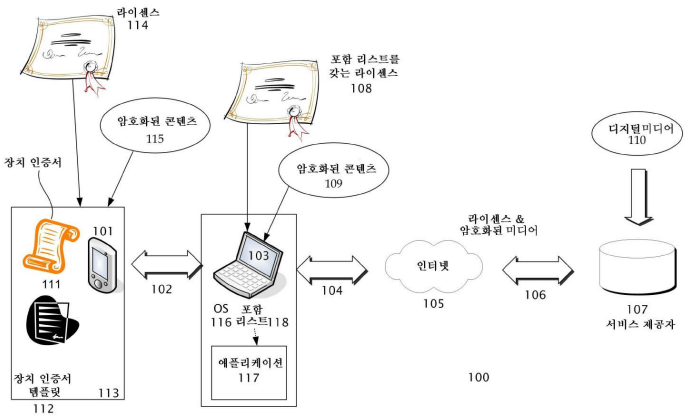
전체 청구항 수 : 총 16 항 심사관 : 이명진

(54) 발명의 명칭 **콘텐츠 보호 시스템들 간의 디지털 콘텐츠 전사**

(57) 요 약

디지털 콘텐츠 - 이 디지털 콘텐츠는 포함 리스트를 포함함 - 를 해독할 수 있는 제1 콘텐츠 보호 시스템과, 애플리케이션이 제1 콘텐츠 보호 시스템의 기능성에 액세스하게 하는 링크가능 라이브러리 - 이 애플리케이션은 제2 콘텐츠 보호 시스템을 포함함 - 와, 제2 콘텐츠 보호 시스템을 평가하여 제2 콘텐츠 보호 시스템이 포함 리스트 상에 있는 것인지 여부를 결정하는 수단을 포함하는, 디지털 콘텐츠를 보호하기 위한 기술을 제공한다.

대 표 도



(72) 발명자

던바, 제프리 티.

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

알코브, 제임스 엠.

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

로젠스테인, 다니엘

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

하워드, 매튜 엘.

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

마, 밍

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

그리고로비치, 알렉산드레 브이.

미국 98052-6399 워싱톤주 레드몬드 원 마이크로소프트 웨이

특허청구의 범위

청구항 1

디지털 콘텐츠를 전사하기 위한 컴퓨팅 시스템으로서,

상기 디지털 콘텐츠를 해독할 수 있는 제1 콘텐츠 보호 시스템 - 상기 디지털 콘텐츠는, 상기 디지털 콘텐츠가 이용될 수 있는 복수의 콘텐츠 보호 시스템들을 열거하는 포함 리스트를 포함함 -;

제2 콘텐츠 보호 시스템으로부터 상기 제2 콘텐츠 보호 시스템을 식별하는 증명서를 수신하고, 상기 증명서를 사용하고 상기 포함 리스트를 체크하여 상기 디지털 콘텐츠를 상기 제2 콘텐츠 보호 시스템에 전사할 수 있는지 아닌지를 판단하는 수단;

상기 디지털 콘텐츠를 해독하여 해독된 디지털 콘텐츠를 생성하는 해독 수단;

일시적 암호화 키를 생성하고, 상기 일시적 암호화 키를 사용하여 상기 해독된 디지털 콘텐츠를 암호화하여 일시적 암호화 콘텐츠를 생성하는 일시적 암호화 수단;

상기 일시적 암호화 콘텐츠를 상기 제1 콘텐츠 보호 시스템으로부터 상기 제2 콘텐츠 보호 시스템에 제공하는 수단

을 포함하는 컴퓨팅 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

초기화 벡터를 계산하는 수단을 더 포함하며,

상기 초기화 벡터는, 공유 수단을 통해 상기 제1 콘텐츠 보호 시스템과 상기 제2 콘텐츠 보호 시스템 간에 공유되는 컴퓨팅 시스템.

청구항 4

제3항에 있어서,

상기 디지털 콘텐츠의 청크에 기초하여 솔트(salt) 값을 계산하는 수단을 더 포함하며,

상기 솔트 값은 암호화 해싱 수단을 통해 상기 초기화 벡터와 결합되어, 일시적 암호화 키를 발생시키는 컴퓨팅 시스템.

청구항 5

제4항에 있어서,

상기 일시적 암호화 키를 이용하여 상기 청크의 일시적 암호화를 생성하는 수단을 더 포함하는 컴퓨팅 시스템.

청구항 6

제5항에 있어서,

상기 청크의 일시적 암호화, 상기 초기화 벡터 및 상기 솔트 값을 상기 제2 콘텐츠 보호 시스템에 제공하는 수단을 더 포함하는 컴퓨팅 시스템.

청구항 7

디지털 콘텐츠를 전사하는 방법으로서 - 상기 디지털 콘텐츠는, 상기 디지털 콘텐츠가 이용될 수 있는 복수의 콘텐츠 보호 시스템들을 열거하는 포함 리스트를 포함함 -,

제1 콘텐츠 보호 시스템이, 제2 콘텐츠 보호 시스템으로부터 상기 제2 콘텐츠 보호 시스템을 식별하는 증명서를 수신하는 단계;

상기 제1 콘텐츠 보호 시스템이, 상기 증명서를 사용하고 상기 포함 리스트를 체크하여 상기 디지털 콘텐츠를 상기 제2 콘텐츠 보호 시스템에 전사할 수 있는지 아닌지를 판단하는 단계;

상기 제1 콘텐츠 보호 시스템이, 상기 디지털 콘텐츠를 해독하여 해독된 디지털 콘텐츠를 생성하는 단계;

상기 제1 콘텐츠 보호 시스템이, 일시적 암호화 키를 생성하고, 상기 일시적 암호화 키를 이용하여 상기 해독된 디지털 콘텐츠를 암호화하여 일시적 암호화 콘텐츠를 생성하는 단계; 및

상기 제1 콘텐츠 보호 시스템이, 상기 일시적 암호화 키 및 상기 일시적 암호화 콘텐츠를 제2 콘텐츠 보호 시스템에 제공하는 단계

를 포함하는, 디지털 콘텐츠 전사 방법.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 일시적 암호화 키는 초기화 벡터 및 솔트 값을 암호화 방식으로 해싱함으로써 생성되며,

상기 솔트 값은 상기 디지털 콘텐츠의 청크에 기초하여 계산되는, 디지털 콘텐츠 전사 방법.

청구항 10

디지털 콘텐츠를 전사하는 방법으로서 - 상기 디지털 콘텐츠는, 상기 디지털 콘텐츠가 이용될 수 있는 복수의 콘텐츠 보호 시스템들을 열거하는 포함 리스트를 포함함 -,

제1 콘텐츠 보호 시스템이, 제2 콘텐츠 보호 시스템으로부터 상기 제2 콘텐츠 보호 시스템을 식별하는 증명서를 수신하는 단계;

상기 제1 콘텐츠 보호 시스템이, 상기 증명서를 사용하고 상기 포함 리스트를 체크하여 상기 디지털 콘텐츠를 상기 제2 콘텐츠 보호 시스템에 전사할 수 있는지 아닌지를 판단하는 단계;

제1 콘텐츠 보호 시스템에서, 초기화 벡터를 발생시키는 단계;

제1 콘텐츠 보호 시스템에서, 상기 디지털 콘텐츠의 청크를 해독하는 단계;

제1 콘텐츠 보호 시스템에서, 상기 청크에 기초하여 솔트 값을 발생시키는 단계;

제1 콘텐츠 보호 시스템에서, 상기 초기화 벡터 및 상기 솔트 값을 암호화 방식으로 해싱하여, 일시적 키를 발생시키는 단계;

제1 콘텐츠 보호 시스템에서, 상기 일시적 키를 이용하여 상기 청크를 암호화함으로써 상기 청크의 일시적 암호화를 생성하는 단계; 및

제1 콘텐츠 보호 시스템에서, 상기 일시적 암호화를 상기 제2 콘텐츠 보호 시스템으로 제공하는 단계;

를 포함하는, 디지털 콘텐츠 전사 방법.

청구항 11

삭제

청구항 12

제10항에 있어서,

상기 초기화 벡터는 난수인, 디지털 콘텐츠 전사 방법.

청구항 13

제10항에 있어서,

상기 솔트 값은 상기 청크를 이용하여 계산된 수인, 디지털 콘텐츠 전사 방법.

청구항 14

제10항에 있어서,

상기 일시적 암호화는 스트림 사이퍼(stream cipher)를 이용하여 생성되는, 디지털 콘텐츠 전사 방법.

청구항 15

제10항에 있어서,

제2 콘텐츠 보호 시스템에서,

상기 제1 콘텐츠 보호 시스템으로부터 암호화된 초기화 벡터를 수신하는 단계;

상기 초기화 벡터를 해독하며 저장하는 단계;

상기 제1 콘텐츠 보호 시스템으로부터 상기 일시적 암호화를 수신하는 단계;

상기 제1 콘텐츠 보호 시스템으로부터 상기 솔트 값을 수신하는 단계;

상기 초기화 벡터 및 상기 솔트 값을 암호화 방식으로 해싱하여, 상기 일시적 키의 복제를 발생시키는 단계; 및

상기 일시적 키의 복제를 이용하여 상기 일시적 암호화를 해독하는 단계

를 더 포함하는, 디지털 콘텐츠 전사 방법.

청구항 16

삭제

청구항 17

제15항에 있어서,

상기 초기화 벡터는, 상기 제2 콘텐츠 보호 시스템에 의해 제공되는 공개 키를 이용하여 상기 제1 콘텐츠 보호 시스템에 의해 암호화되는, 디지털 콘텐츠 전사 방법.

청구항 18

제15항에 있어서,

상기 암호화된 초기화 벡터는, 상기 제2 콘텐츠 보호 시스템에 의해 제공되는 비밀 키를 이용하여 상기 제2 콘텐츠 보호 시스템에 의해 해독되는, 디지털 콘텐츠 전사 방법.

청구항 19

제15항에 있어서,

상기 초기화 벡터는 보안 방식으로 저장되는, 디지털 콘텐츠 전사 방법.

청구항 20

제15항에 있어서,

상기 방법은 컴퓨터 판독가능 매체에서 구현되는, 디지털 콘텐츠 전사 방법.

명 세 서

기 술 분 야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은 2005년 7월 11일자로 제출한 미국 가출원 번호 제60/698,525호의 우선권(대리인 정리 번호: 313859.01)을 주장한다.

[0003] 본 발명은 일반적으로 디지털 콘텐츠의 보호에 관한 것으로서, 보다 상세하게는, 서로 다른 콘텐츠 보호 시스템들에 의해 사용되는 암호화 포맷들 간의 디지털 콘텐츠의 전사, 및 디지털 콘텐츠가 시스템들 및/또는 소프트웨어 컴포넌트들 간에 전달되는 동안 디지털 콘텐츠를 위한 일시적 암호화의 제공에 관한 것이다.

배 경 기 술

[0004] 본 출원은 일반적으로 가전 제품들에서의 디지털 콘텐츠의 사용에 관한 것으로서 보다 상세하게는 다양한 콘텐츠 보호 메카니즘들 간의 전사 및 호환성의 생성에 관한 것이다.

[0005] 전자 시스템 및 컴퓨팅 시스템은 규정된 디지털 콘텐츠를 재생하거나 처리하도록 설계될 수 있다. 이러한 디지털 콘텐츠는, 이용되고 있는 보호 메카니즘에 따라 제한적으로 이 콘텐츠에 대한 액세스를 허용하는 제삼자에 의해 제어되거나 소유될 수 있다. 액세스 제어의 예로는, 소정 횟수로, 또는 소정의 시간 주기 동안 정보에 액세스하는 것을 포함한다. 디지털 콘텐츠에 대한 액세스를 제어하는 일반적인 방식은, 암호 키를 이용해야만 하며 그리고 콘텐츠에 대한 액세스 권한을 특정하는 라이센스를 포함해야만 콘텐츠에 액세스할 수 있도록 그 콘텐츠를 암호화하는 것이다. 콘텐츠의 사용은, 시스템이 디지털 콘텐츠에 액세스할 수 있도록 라이센스와 일치해야 한다. 액세스 제어는, 통상적으로 암호화 및 액세스 권한과 같은 보안 특징들을 포함시킴으로써 콘텐츠 오서링(authoring) 또는 제작시 확립된다. 그러나, 통상적으로, 다양한 콘텐츠 보호 메카니즘들은 높은 상호운용성을 허용하지 못한다.

발명의 상세한 설명

[0006] 다음에 따르는 설명에서는, 당업자에게 기본적인 이해를 제공하고자 본 발명의 간략한 개요를 제공한다. 이 개요는 본 발명의 광범위한 개요가 아니며 본 발명의 핵심/주요 요소들을 식별하지 않고 또는 본 발명의 범위를 제한하지 않는다. 이 개요의 유일한 목적은, 본 명세서에서 제공되는 일부 개념들을, 추후에 제시되는 상세한 설명에 대한 도입부로서 간략한 형태로 제시하는 것이다.

[0007] 본 예에서는, 콘텐츠 보호 시스템들 간의 디지털 콘텐츠의 전사를 지원하고, 디지털 콘텐츠가 콘텐츠 보호 시스템들 및/또는 소프트웨어 컴포넌트들 간에 전달되고 있는 동안 디지털 콘텐츠를 위한 일시적 암호화를 제공하는 기술을 제공한다. 이러한 기술은, 디지털 콘텐츠에 관련된 포함 리스트를 제공하여, 콘텐츠가 전사될 수 있는 콘텐츠 보호 시스템의 유형을 특정한다.

[0008] 많은 부수 특징들은 첨부 도면과 함께 다음에 따르는 상세한 설명을 참조함으로써 더욱 쉽게 이해 및 인식될 것이다.

실 시 예

[0016] 첨부 도면과 함께 이하에서 제공되는 상세한 설명은 본 실시예들을 설명하고자 하는 것이며, 이러한 예시적인 실시예들을 구성하거나 활용할 수 있는 형태들만 제시하려는 것이 아니다. 이러한 설명은 본 실시예의 기능 및 본 실시예를 구성하고 동작하기 위한 단계들의 시퀀스를 설정한다. 그러나, 다른 예들에 의해 동일하거나 등가의 기능 및 시퀀스를 달성할 수 있다.

[0017] 본 발명은 본 명세서에서 가전 제품(CE) 시스템에서 구현될 수 있는 것으로 설명되고 예시되고 있지만, 설명되는 이 시스템은 일 예로서 제공되며 이러한 예로 한정되지 않는다. 본 발명은 디지털 콘텐츠를 지원할 수 있는 임의의 장치나 시스템으로 실시할 수 있다. CE 장치는, 포켓 PC, 셋톱 박스, 휴대용 미디어 센터, 셀 폰, 뮤직 플레이어, PC, 소프트웨어 구성된 미디어 플레이어 등을 포함할 수 있다. 당업자가 인식할 수 있듯이, 본 발명은 디지털 콘텐츠 액세스 및 콘텐츠 보호를 제공하는 서로 다른 다양한 유형의 시스템들의 애플리케이션에 적합하다. 콘텐츠 보호 시스템의 일 예는, 디지털 권한 관리(DRM) 시스템이며, 이하의 설명에서 이용된다. 다른 콘텐츠 보호 시스템들을 이용하여 본 발명을 실시할 수도 있다.

[0018] 그 예로는, 콘텐츠 보호 스킴(scheme)들 간에 전사될 보호받는 콘텐츠를 인가하는 명시적이고 강건한(robust) 수단을 제공할 수 있다. 이 예에서, 디지털 콘텐츠의 제공자 및 콘텐츠 보호 시스템은, 다운스트림 애플리케이션이, 예를 들어, 윈도우즈 미디어 DRM (WMDRM)과 같은 콘텐츠 보호 포맷으로부터 디지털 전송 콘텐츠 보호

(DTCP) 등과 같은 기타 포맷으로 전사를 수행할 때, 콘텐츠의 개별적인 부분들을 리베스트 사이퍼 4(RC4)와 같은 중간 콘텐츠 보호 포맷으로 전사하는 것을 인가할 수 있다.

[0019] 도 1은 포함 리스트를 구비하고 디지털 콘텐츠의 전사를 허용하는 콘텐츠 보호 시스템(100)의 일 예를 도시하는 도면이다. 전사는, DRM 시스템과 같은 제1 콘텐츠 보호 시스템과 호환성있는 디지털 콘텐츠를, 다른 DRM 시스템과 같은 제2 콘텐츠 보호 시스템과 호환성있는 포맷으로 변환될 수 있게 한다. 포함 리스트는, 콘텐츠 소유자가 허용가능한 변환을 특정하는 방식을 제공한다. 이러한 변환은 통상적으로 PC(103) 상에서 수행된다. DRM은, 멀티미디어 콘텐츠 또는 기타 디지털 콘텐츠 등과 같은 디지털 콘텐츠(110)에 대한 권한을 정의하고, 통합하며, 강화하는 시스템을 제공한다. DRM 시스템(100)은, 인터넷(105)과 같은 불안전한 채널 또는 CD, DVD, 컴퓨터 파일 등을 통해 서비스 제공자(107)로부터 콘텐츠(110)를 안전하게 배포한다. 시스템(100)은, 사용 규칙을 강화할 수 있고 콘텐츠(110)가 불법적으로 사용되는 것을 방지할 수 있다. 사용 규칙은, 만료일, 사용자가 오디오 파일 또는 비디오 파일을 재생할 수 있는 횟수, 사용자가 오디오 파일 또는 비디오 파일을 카피할 수 있는 횟수 등을 포함할 수 있다. 디지털 권한 관리 시스템의 예는, 1999년 4월 12일자로 출원한 미국 특허출원번호 제09/290,363호, 및 2002년 6월 28일자로 출원한 미국 특허출원번호 제10/185,527호. 제10/185,278호 및 제10/185,511호에 개시되어 있으며, 이들의 내용 모두는 본 명세서에서 참고로 포함된다.

[0020] 퍼스널 컴퓨터(103)는, 인터넷(105)에 접속되고 콘텐츠를 서비스 제공자(107)로부터 가전 제품(101)으로 전달하는 데 이용될 수 있다. PC(103)는, 제1 DRM 시스템과 호환성있는 암호화된 콘텐츠(109)를, 예를 들어, CE 장치(101) 상에 존재하는 제2 DRM 시스템과 호환성있는 암호화된 콘텐츠(115)로 전사할 수 있다. 미디어 파일(109)을 전사하기 위해, 포함 리스트를 갖는 라이센스(108)가, 통상적으로 서비스 제공자(107)로부터 미디어 파일(109)과 함께 PC(103)로 전달된다.

[0021] 포함 리스트에 포함되어 있는 콘텐츠 보호 포맷을 위한 액세스 권한 및 제한은, 첨부되는 미디어 파일(109)이 전사될 수 있는 장치 및/또는 콘텐츠 보호 시스템의 유형을 비롯하여, 통상적으로 콘텐츠 소유자에 의해 설정되는 호환성 규칙에 의해 관리된다. 일 예로, 포함 리스트는, 암호화된 콘텐츠(109)가 전사될 수 있는 허용가능한 기술들을 고유하게 식별하는 16바이트 수일 수 있는 글로벌 유니크 식별자(GUI)를 포함할 수 있다. 다른 예로, 포함 리스트는, 허용가능한 보호 기술들을 고유하게 식별하는 스트링 "Windows Media DRM"과 같은 문자 스트링을 포함할 수 있다. 따라서, 포함 리스트를 갖는 라이센스(108)를 제공함으로써, 시스템 및 장치 간의 동작가능성이 증가할 수 있다.

[0022] PC(103)는 통상적으로 애플리케이션 프로그램(117)과 함께 동작하는 운영 체제(116)를 이용하여 기능한다. 애플리케이션 프로그램(117)은, 통상적으로, 타겟 보호 시스템이 디지털 콘텐츠(109)에 대하여 인가되어 있는지 여부를 결정하도록 포함 리스트(118)를 검사한 후 디지털 콘텐츠(109)의 전사를 수행한다.

[0023] 경로(102, 104)를 통해 PC(103) 및 CE 장치(101)로 정보를 전달하기 위한 프로토콜 및 메카니즘은, 이더넷 네트워크, 유니버설 시리얼 버스(USB), 적외선 데이터 관련(IrDA), 블루투스 등과 같은 종래의 프로토콜 및 메카니즘일 수 있다. 다른 실시예들에서, 가전 제품은 퍼스널 컴퓨터(103)를 이용하지 않고서 서비스 제공자에 결합될 수 있다. 퍼스널 컴퓨터 및 CE 장치는 당업자에게 알려져 있는 임의의 개수의 적합한 운영 체제들을 활용하며 동작할 수 있다. 이 예에서 설명하는 기능들을 구현하기 위한 명령어들은, 컴퓨터 실행가능 소프트웨어, 하드웨어(예를 들어, ASIC 내로 버닝된 명령어들), 또는 이들의 조합으로서 존재할 수 있다.

[0024] 사용시, DRM(100)은 암호화된 콘텐츠(109)를 제공함으로써 콘텐츠를 보호한다. 콘텐츠(109)가 암호화되어 있기 때문에, 데이터 자체가 보호된다. 따라서, 콘텐츠(109)는 제한 없이 이동(move), 아카이브(archive), 카피, 또는 배포될 수 있다. 이러한 디지털 콘텐츠가 시스템 간에 전송될 때에는, 암호화된 콘텐츠를 숨기거나 액세스 불가능하게 만들거나, 특별한 보호를 걸 필요가 없다. 예를 들어, 이러한 콘텐츠를 카피하여 친구에게 주더라도 그 친구가 인가받지 않는 이상 그 콘텐츠를 이용할 수 없다. 암호화된 콘텐츠를 이용할 수 있게 하려면, 사용자가 라이센스를 획득해야 하고, 이 예에서는, 포함 리스트를 갖는 라이센스(108)를 획득해야 한다. 이 포함 리스트를 갖는 라이센스(108)는 암호화된 콘텐츠(110)를 보호하는 수단이다. 일 예로, 라이센스는, 단일 머신(101)에 대하여 허가될 수 있으며, 카피되더라도, 다른 머신들 상에선 기능하지 않을 것이다. 그러나, 이러한 포함 리스트를 이용하게 되면, 콘텐츠 소유자 또는 서비스 제공자(107)에 의해 라이센스 포함 리스트에 특정되어 있는 바와 같이, 디지털 콘텐츠는 서로 다른 보호 스킴들로 동작하는 서로 다른 머신들에게 제공될 수 있다. 다른 예에서, 라이센스는, 사용자가 인가된 사용자 계정을 통해 로그인 할 때 네트워크 상의 임의의 장치로부터의 콘텐츠에 액세스할 수 있도록, 네트워크 상의 특별한 사용자 계정에 허가될 수 있다.

[0025] 포함 리스트를 갖는 각 라이센스(108)는, 콘텐츠를 사용할 수 있는 방식 및 콘텐츠를 어떠한 조건에서 사용할

수 있는지를 정의하는 액세스 권한 및 제한을 포함한다. 예를 들어, 음악 파일 라이센스는, "재생할 권한"을 포함하지만 "CD로 버닝할 권한"은 포함하지 않을 수 있으며, 2005년 10월 1일부터 2005년 11월 1일까지의 기간 동안 이러한 권한을 유효하게 할 수 있다. 또한, 디지털 콘텐츠 선택을 위한 다수의 라이센스가 존재할 수 있다. 이러한 라이센스들 중 하나의 라이센스가 필요한 권한을 허가하는 한, 사용자는 콘텐츠 데이터에 액세스하여 사용할 수 있다. 액세스는 콘텐츠에 암호화 방식으로 해독하는 것, 패스워드를 통해 콘텐츠에 액세스를 얻는 것 등을 가리킬 수 있으며, 이에 따라 사용자는 디지털 콘텐츠를 사용하고, 뷰잉하며, 재생하고, 또는 다른 방법으로 디지털 콘텐츠를 사용할 수 있다. 일 실시예에서는, 포함 리스트를 갖는 라이센스를 XML 포맷 등으로 제공할 수 있다.

[0026] 전술한 바와 같이, 포함 리스트는 디지털 콘텐츠가 서로 다른 다양한 콘텐츠 보호 시스템들에게 제공될 수 있게 한다. 일 예로, PC(103) 상에서 동작하는 DRM 시스템은, CE 장치(101)로부터 얻은 장치 인증서(111)와 함께, 포함 리스트를 갖는 라이센스(108)를 이용하여, 콘텐츠가 장치(101) 상에서 동작하는 DRM 시스템에서 이용되도록 전사될 수 있는지 여부를 결정한다. 뷰잉 또는 재생을 위한 디지털 콘텐츠는 통상적으로 음악 파일, 사진 파일, 비디오 파일, 다큐먼트 등을 포함한다. CE 장치(101) 상에서 동작하는 것과 같은 콘텐츠 보호 시스템은 장치 인증서를 이용하여 자신을 식별한다. 일 예로, 장치 인증서는 확장성 마크업 언어(XML) 데이터 구조 등일 수 있고, 이것은 시스템, 리스트 지원 특징들, 액세스 제어를 기술하며, 통상적으로 시스템의 공개 키를 포함한다. 장치 인증서(111)는 가전 제품 (101) 상에서 동작하는 콘텐츠 보호 시스템과 함께 패키징(113)된 장치 인증서 템플릿(112)으로부터 발생할 수 있다. 장치 인증서 템플릿은, 장치 인증서의 생성을 보조하는 특별한 패턴, 가이드 등으로서 고려될 수 있다.

[0027] 장치 인증서(111)는, 가전 제품(101)의 DRM 시스템이 보호 콘텐츠(115)에 액세스하는 데 적합한지의 유효성을 검사함으로써 보안을 제공하는 것을 돕도록 가전 제품(101)의 DRM 시스템에 의해 사용될 수 있는 유효성 검사(validation) 메카니즘이다. 장치 인증서는, 신뢰될 수 있으며 보호받는 디지털 콘텐츠의 소유자에 의존할 수 있으며 콘텐츠에 대한 액세스를 제공하는 프로세스의 개시를 돕는 자격 증명이다. 이러한 자동 콘텐츠 보호 유효성 검사는, 보호받는 디지털 콘텐츠의 보안 재생 또는 사용을 위해 설계되고 디지털 방식으로 서명된 인증서(111) 등이 디지털 콘텐츠에 액세스하는 권한의 유효성 검사를 제공하는 방식으로서 사용되는 시스템(100)에서 이용될 수 있다. 보호받는 디지털 콘텐츠(115)는, 음악, 비디오, 텍스트, 또는 종래의 라이센스 협정 등에 의해 관리를 받는 임의의 콘텐츠를 포함할 수 있다.

[0028] 예로 든 장치 인증서(111)는, 장치 식별, 장치 자격 클레임(capability claim), 주요 정보, 공개 키 정보 등을 포함하는 XML 오브젝트일 수 있고, 이러한 데이터를 디지털 방식으로 서명된 하나의 장치 인증서에 나타낸다. 장치 인증서(111)는, DRM 제공자(도시하지 않음)에 의해 서명될 수 있으며, 장치 인증서(111)가 DRM 시스템이 인증서를 갖고 있음을 정확하게 반영하고 있는 그 DRM 제공자에 의한 인증, 및 수반되는 DRM 시스템을 생성하고 인증하도록 DRM 제공자가 인가되어 있음을 인증하는 제삼자의 신뢰받는 기관(도시하지 않음)에 의한 인증으로서 기능할 수 있다. 장치 인증서 및 장치 인증서 템플릿의 예는, 2004년 10월 18일자로 제출한 미국 특허출원번호 제10/18,204호에 제공되어 있으며, 그 내용 전체는 본 명세서에 참고로 포함된다.

[0029] 도 2는 디지털 콘텐츠의 암호화를 전사하거나 변경하는 프로세스에서 2개의 주요 동작을 도시하는 흐름도이다. 전사를 제공하는 방안은, 먼저 암호화된 디지털 콘텐츠를 제공하고, 콘텐츠 상의 암호화(201)(예를 들어, WMDRM이 보호받는 콘텐츠에 적용하는 암호화)를 제거한 후, 새로운 암호화(202)(예를 들어, RC4 암호화)를 콘텐츠에 추가하는 것이다.

[0030] 도 3은 전사 프로세스에서 애플리케이션(301)을 통해 안전하게 전달되는 데이터를 도시하는 블록도이다. 콘텐츠 제공자는 포함 리스트를 제공함으로써 콘텐츠를 규제하고 그 노출을 제한한다. 포함 리스트는, 제1 DRM 시스템으로부터 제2 DRM 시스템으로의 전사를 허용하도록 제공될 수 있다. 콘텐츠 보호 시스템의 일 예에서, 전사는 포함 리스트를 갖는 디지털 콘텐츠를 위해 제공될 수 있고, 콘텐츠 보호 시스템의 다른 예에서, 전사는 포함 리스트를 갖지 않는 디지털 콘텐츠를 위해 제공될 수 있다.

[0031] 제1 DRM 시스템(302)은, 애플리케이션(301)과 같은 애플리케이션에 링크될 수 있는 링크가능 라이브러리(309)를 포함한다. 라이브러리(309)는 애플리케이션(301)에게 제1 DRM 시스템(302)에 대한 액세스를 제공한다. 일 예로, 라이브러리(309)는 ".lib" 파일 등으로서 제공될 수 있다. 다른 예에서, 라이브러리는 ".dll"(동적 링크 라이브러리) 파일 등으로서 제공될 수 있다. 라이브러리(309)는 애플리케이션(301)에게 제1 DRM 시스템(302)의 기능성에 대한 액세스를 제공하도록 다른 형태를 취할 수도 있다.

[0032] 제공자의 루트 또는 인증 기관 키(300)에 의해 서명된 인증서(305)는 애플리케이션(301)에 포함된다. 일 예로,

비밀 키(306)는, 통상적으로 RSA 비밀 키를 포함하며, 통상적으로 시스템이 설치될 때 또는 오서링될 때 인증서(305)와 함께 제공된다.

[0033] 런타임시, 인증서(305)는, 통상적으로 제1 DRM 시스템(302)에 의해 유지되는 디지털 콘텐츠에 액세스하라는 요구에 응답하여, 제1 DRM 시스템(302)에게 전달된다. 제1 DRM 시스템(302)은 난수 또는 초기화 벡터(IV)(308)를 발생시킨다. IV(308)는 통상적으로 보안 방식으로 애플리케이션(301)에 제공되고 저장된다. 일 예로, IV(308)는 보안 채널을 이용하여 시스템들 간에 전달된다. 다른 예에서, IV(308)는 애플리케이션(301)에 제공되기 전에 인증서(305)로부터의 공개 키와 같은 키를 이용하여 암호화된다. IV(308)는 애플리케이션의 비밀 키로 암호화되고 저장된다.

[0034] 이 때, 디지털 콘텐츠는 통상적으로 제1 DRM 시스템(302)에 의해 작은 청크 또는 샘플로 해독된다. 디지털 콘텐츠의 초기 암호화가 제거되면, 제1 DRM 시스템(302)은 청크가 애플리케이션(301)에 제공될 때 보호를 위해 이 청크에 새로운 암호화를 적용한다. 청크를 애플리케이션(301)으로 전달하기 전에 데이터를 해독하고 청크를 다시 암호화하는 프로세스는, 통상적으로 일시적 암호화라 칭하는 전사의 한 가지 형태이며, 중재자의 공격(307) 등을 최소화할 수 있다.

[0035] 각 디지털 콘텐츠 샘플 또는 청크는, 일반적으로 각 콘텐츠 샘플에 대하여 고유한 경향이 있는 일시적 암호화 키를 이용하여 암호화된다. 일 예로, 이러한 일시적 암호화 키는, 각 디지털 콘텐츠 샘플 또는 청크에 대하여 고유한 솔트(salt)값(304)을 발생시킨 후 이 고유한 솔트값(304)을 IV 값(308)으로 해싱함으로써 형성된다. 청크는, 일시적 암호화 키를 이용하여 암호화되고, 솔트값(304)과 함께 애플리케이션(301)에 제공된다. 일단 청크가 애플리케이션(301)에 도달하게 되면, 애플리케이션(301)은 저장된 IV(308) 및 솔트값(304)으로부터 일시적 암호화 키를 생성하고, 콘텐츠 청크로부터 일시적 암호화를 제거한다. 이 때, 애플리케이션(301)은, 제2 DRM 시스템(303)에 의해 요구되는 통상적으로 암호화를 포함하는 적합한 보호를 적용할 수 있다. 디지털 콘텐츠 샘플 또는 청크는, 제2 DRM에 의해 보호된 후에, 예를 들어, 디지털 오디오 파일로부터 온 것이라면 재생되는 것처럼 시스템(303)에 의해 허용되는 임의의 방식으로 활용될 수 있다.

[0036] 도 4는 전사 프로세스를 이용하여 디지털 콘텐츠를 보호하기 위한 상세한 프로세스의 일 예를 도시하는 블록도이다. (DRM 페이로드(412)라고도 칭하는) 디지털 콘텐츠의 일 예는, 영화로서 제공될 수 있는 것과 같은 디지털 비디오 데이터이다. 이러한 디지털 콘텐츠는 도 4에 나타낸 바와 같이 통상적으로 콘텐츠의 콘텐츠 제공자에 의해 암호화된다. 디지털 콘텐츠의 다른 예로는, 디지털 오디오 데이터, 디지털 이미지, 또는 다큐먼트 등을 포함하는 기타 멀티미디어나 디지털 콘텐츠가 있다. 암호화에 더하여, 이러한 디지털 콘텐츠는 통상적으로 액세스 권한 정보의 소정의 형태를 포함한다. 일 예로, 이러한 액세스 권한은, 디지털 콘텐츠에 액세스 및/또는 디지털 콘텐츠를 전사하는데 어떠한 다른 형태의 콘텐츠 보호 메카니즘을 신뢰하고 활용할 수 있는지를 가리키는 포함 리스트를 포함한다.

[0037] 도 4는 DRM 시스템 B(460)에 의해 전사를 위해 디지털 콘텐츠(412)를 처리하기 위한 여러 요소들 및 단계들을 포함하는 DRM 시스템 A(350)의 일 예를 도시한다. 예로 든 DRM 시스템 B는, 애플리케이션, DRM 시스템 등 간에 분산될 수 있는 여러 요소들 및 단계들을 포함한다. 일 예로, DRM 시스템 B는 DRM 시스템을 갖는 애플리케이션을 포함한다. DRM 시스템 A(450) 및 DRM 시스템 B(460)는 상호작용하여, 콘텐츠 제공자에 의해 제공되는 암호화를 제거하고, 이러한 두 개의 DRM 시스템에 의해 그리고 이 두 개의 DRAM 시스템에 의해 이해되는 일시적 암호화로 콘텐츠를 재 암호화하며, 일시적 암호화 콘텐츠를, 이 콘텐츠가 해독된 후 최종적으로 DRM 시스템 B(460)에 의해 사용되는 임의의 포맷으로 재 암호화되는 DRM 시스템 B(460)에, 안전하게 전달한다.

[0038] 예로 든 전사 프로세스의 시작시, 시스템 B는 전사 프로세스를 개시한다. 이러한 개시의 일 예는 디지털 영화 파일을 재생하려는 시도이다. 통상적으로, 인증서 등이 시스템 B로부터 시스템 A(450)로 전송된다. 시스템 A는 인증서를 검사하여 시스템 B가 신뢰받는 것인지 여부 및 시스템 B가 디지털 콘텐츠의 포함 리스트에 열거되어 있는지 여부를 결정한다. 시스템 B가 신뢰받는 것이며 포함 리스트 상에 있는 것이면, 시스템 A는 계속해서 전사 프로세스를 수행한다. 그렇지 않다면, 전사 프로세스는, 시스템 B가 신뢰받지 못하거나 디지털 콘텐츠의 포함 리스트 상에 열거되어 있지 않기 때문에, 계속되지 않는다.

[0039] 계속해서, 시스템 A는 시스템 B로부터 암호 키(401)를 얻는다. 일 예로, 암호화 키는 공개 키이며 시스템 B로부터 얻은 인증서로부터 얻는다. 시스템 A는 초기화 벡터(IV)(403)를 발생시키고 공개 키(401)를 이용하여 IV(403)를 암호화하여, 암호화된 IV(404)가 발생한다. 일 예로, IV(403)는 다른 암호화 키를 발생시키고 해싱하는 데 적합한 난수이다.

[0040] 시스템 A는, 통상적으로 보안 채널을 이용하여, 암호화된 IV(404)를 시스템 B에 제공한다. 시스템 B는 비밀 키(405)를 이용하여 암호화된 IV(404)를 해독함으로써, 초기 IV 값(403)이 발생한다. 시스템 B는 추후 사용을 위해 난독화(obfuscation)를 이용하는 것과 같은 보안 방식으로 IV를 저장한다(403). 이 때, 시스템 A 및 시스템 B 간의 초기화가 완료되며, 일시적 전사가 시작될 수 있다.

[0041] 시스템 A는 이제 디지털 콘텐츠(412)를 판독 및 해독(414)하기 시작한다. 일 예로, 시스템 A는 키(415)를 이용하여 디지털 콘텐츠(412)를 해독(414)한다. 일 예로, 키(415)는, 디지털 콘텐츠(412)에 대한 키(415)를 초기에 암호화하는 콘텐츠 제공자에 의해 사용되는 공개 키에 대응하는 비밀 키를 이용하여 그 키를 해독함으로써 액세스된다. 다른 예로, 시스템 A는, 디지털 콘텐츠(412)를, 작은 청크로, 통상적으로, 청크당 수십, 수백, 또는 수천 바이트로 해독(414)한다. 또다른 예로, 시스템 A는 계속 진행하기 전에 디지털 콘텐츠(412)의 모두를 해독(414)한다. 해독된 각 청크에 따라 (페이로드라고도 알려져 있는) 비암호화된(unencrypted) 디지털 콘텐츠(410)가 발생한다.

[0042] 다음으로, 시스템 A는 솔트값(408)을 발생시킨다. 일 예로, 솔트값(408)은, 다른 암호화 키를 해싱하고 발생시키는 데 사용하기에 적합한, 디지털 콘텐츠 청크(410) 당 발생하는 난수이다. 일 예로, 이러한 암호화 키는 RC4 키일 수 있다. 시스템 A는 솔트값(408) 및 IV(403)를 해싱하여, 암호화 키가 발생한다. 다른 예에서, 해시(419)는 보안 해시 알고리즘(SHA) 해시일 수 있다. 다음으로, 시스템 A는, 암호화되고 있는 콘텐츠 청크에 대응하는 IV(403) 및 솔트(408)의 해시(419)를 통해 발생한 RC4 키를 이용하여 콘텐츠 청크(410)를 암호화(420)하여, 일시적 암호화 콘텐츠 청크(421)가 발생한다. 또다른 예에서, RC4 스트림 사이퍼(stream cipher)는 암호화(420)를 위해 이용되어, (RC4 페이로드(421)라고도 알려진) RC4 암호화 콘텐츠 청크가 발생한다.

[0043] 시스템 A는 통상적으로 보안 채널을 이용하여 솔트값(408) 및 대응하는 일시적 암호화 콘텐츠 청크(421)를 시스템 B에 제공한다. 이후, 시스템 B는 이전에 저장한 IV(403) 및 방금 수신한 솔트값(408)을 해싱하여 일시적 해독 키를 발생시키고 방금 수신한 일시적 암호화 콘텐츠 청크(421)를 해독(411)하여, 비암호화된 디지털 콘텐츠(410)가 발생한다. 일 예로, 해독(411) 및 비암호화된 콘텐츠 청크(410)는, 코드 및/또는 데이터 난독화와 같은 보안 방식으로 시스템 B내에서 수행되고 유지된다. 다른 예로, 해시(409)는 보안 해시 알고리즘(SHA) 해시일 수 있다.

[0044] 시스템 B는 이제 모든 전사 프로세스에 의해 지시받음에 따라 콘텐츠 청크(410)를 계속해서 전사한다. 일 예로, 오디오 데이터의 경우에서처럼, 콘텐츠 청크(410)는 더 암호화되어, 미디어 플레이어를 통해 애플리케이션 등을 렌더링하기 위한 코덱에 제공된다. 전술한 프로세스는 디지털 콘텐츠(410)의 각 청크에 대하여, 통상적으로 모든 디지털 콘텐츠(412)가 전사될 때까지 계속된다.

[0045] 도 5는 본 명세서에서 설명하는 시스템 및 방법이 구현될 수 있는 예시적인 컴퓨팅 환경(500)을 도시한다. 예시적인 컴퓨팅 환경(500)은 컴퓨팅 시스템의 일 예일 뿐이며 본 명세서에서 설명하는 예들을 이러한 특정 컴퓨팅 환경으로 제한하려는 것이 아니다.

[0046] 컴퓨팅 환경(500)은 많은 기타 범용 컴퓨팅 또는 전용 컴퓨팅 시스템 구성으로 구현될 수 있다. 잘 알려져 있는 컴퓨팅 시스템의 예로는, 퍼스널 컴퓨터, 핸드헬드 또는 랩탑 장치, 마이크로프로세서 기반 시스템, 멀티프로세서 시스템, 셋톱 박스, 프로그래밍가능 가전 제품, 게이밍 콘솔, 가전 제품, 셀룰러 폰, PDA 등이 있지만, 이러한 예로 한정되지는 않는다.

[0047] 컴퓨터(500)는 컴퓨팅 장치(501)의 형태인 범용 컴퓨팅 시스템을 포함한다. 컴퓨팅 장치(501)의 컴포넌트들은, (CPU, GPU, 마이크로크로세서 등) 하나 이상의 프로세서(507), 시스템 메모리(509), 및 다양한 시스템 컴포넌트들을 결합하는 시스템 버스(508)를 포함할 수 있다. 프로세서(507)는 다양한 컴퓨터 실행가능 명령어들을 처리하여, 컴퓨팅 장치(501)의 동작을 제어하고 다른 전자 장치 및 컴퓨팅 장치(도시하지 않음)와 통신한다. 시스템 버스(508)는, 메모리 버스 또는 메모리 컨트롤러, 주변 버스, 가속 그래픽 버스, 및 다양한 버스 아키텍처 중 임의의 것을 이용하는 프로세서나 로컬 버스를 비롯한 버스 구조들의 임의의 개수의 여러 유형들을 나타낸다.

[0048] 시스템 메모리(509)는 RAM과 같은 휘발성 메모리, ROM과 같은 비휘발성 메모리의 형태인 컴퓨터 판독가능 매체를 포함한다. 기본 입력/출력 시스템(BIOS)은 ROM에 저장된다. RAM은 통상적으로 프로세서(507)들 중 하나 이상에 의해 현재 동작되고 있으며 그리고/또는 즉시 액세스가능한 데이터 및/또는 프로그램 모듈을 포함한다.

[0049] 대용량 저장 장치(504)는 컴퓨팅 장치(501)에 결합될 수 있고 또는 버스에 결합됨으로써 컴퓨팅 장치 내에 통합될 수 있다. 이러한 대용량 저장 장치(504)는, 분리식 비휘발성 자기 디스크(예를 들어, 플로피 디스크)에 대

하여 판독 및 기입을 행하는 자기 디스크 드라이브, 또는 CD ROM(506) 등과 같은 분리식 비휘발성 광 디스크에 대하여 판독 및/또는 기입을 행하는 광 디스크 드라이브를 포함할 수 있다. 컴퓨터 판독가능 매체(505, 506)는 통상적으로 플로피 디스크, CD, 휴대용 메모리 스틱 등 상에 공급되는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 등을 구현한다.

[0050] 임의의 개수의 프로그램 모듈은, 예를 들어, 운영 체제, 하나 이상의 애플리케이션 프로그램, 기타 프로그램 모듈, 프로그램 데이터를 비롯하여, 하드 디스크(510), 대용량 저장 장치(504), ROM, 및/또는 RAM(509) 상에 저장될 수 있다. 이러한 운영 체제, 애플리케이션 프로그램, 기타 프로그램 모듈, 프로그램 데이터의 각각(또는 이들의 일부 조합)은, 본 명세서에서 설명하는 시스템 및 방법의 일실시예를 포함할 수 있다.

[0051] 디스플레이 장치(502)는 비디오 아답터(511)와 같은 인터페이스를 통해 시스템 버스(508)에 접속될 수 있다. 사용자는, 키보드, 포인팅 장치, 조이스틱, 게임 패드, 직렬 포트 등과 같은 임의의 개수의 서로 다른 입력 장치들(503)을 통해 컴퓨팅 장치(702)에 인터페이싱할 수 있다. 이러한 입력 장치 및 다른 입력 장치는, 시스템 버스(508)에 결합된 입력/출력 인터페이스(512)를 통해 프로세서(507)에 접속되지만, 병렬 포트, 게임 포트, 및/또는 USB(universal serial bus)와 같은 다른 인터페이스 및 버스 구조에 의해 접속될 수 있다.

[0052] 컴퓨팅 환경(500)은, 하나 이상의 LAN, WAN 등을 통해 하나 이상의 원격 컴퓨터에 대한 접속부를 이용하여, 네트워크화된 환경에서 동작할 수 있다. 컴퓨팅 장치(501)는, 네트워크 아답터(513)를 통해, 또는 다른 방안으로 모뎀, DSL, IDSN 인터페이스 등에 의해, 네트워크(514)에 접속된다.

[0053] 당업자라면 프로그램 명령어를 저장하는 데 활용되는 저장 장치들이 네트워크를 통해 분산될 수 있다는 점을 인식할 것이다. 예를 들어, 원격 컴퓨터는 적응성 기기 런타임 모니터링 및 분석 소프트웨어와 같은 툴을 저장할 수 있다. 로컬 또는 터미널 컴퓨터는 프로그램을 실행하도록 원격 컴퓨터에 액세스하여 소프트웨어의 일부 또는 전부를 다운로드할 수 있다. 다른 방안으로, 로컬 컴퓨터는 필요할 때마다 소프트웨어의 부분들을 다운로드할 수 있고, 또는 로컬 터미널에서 일부 소프트웨어 명령어들을 실행하고 원격 컴퓨터(또는 컴퓨터 네트워크)에서 일부 소프트웨어 명령어들을 실행함으로써 분산 처리를 행할 수 있다. 또한, 당업자라면, 자신에게 알려져 있는 종래 기술들을 활용함으로써, 소프트웨어 명령어들의 일부 또는 전부를, DSP, 프로그래밍가능 로직 어레이 등과 같은 전용 회로에 의해 실행할 수 있다는 것을 인식할 것이다.

도면의 간단한 설명

[0009] 본 발명은 첨부 도면의 관점에서 볼 때 다음에 따른 상세한 설명으로부터 더욱 이해될 것이다.

[0010] 도 1은 포함 리스트를 갖고 디지털 콘텐츠의 전사를 허용하는 콘텐츠 보호 시스템의 일 예의 도면이다.

[0011] 도 2는 디지털 콘텐츠의 암호화를 전사하거나 변경하는 프로세스에서의 2가지 주요 동작들을 도시하는 흐름도이다.

[0012] 도 3은 전사 프로세스에서 애플리케이션을 통해 안전하게 전달되고 있는 데이터를 도시하는 블록도이다.

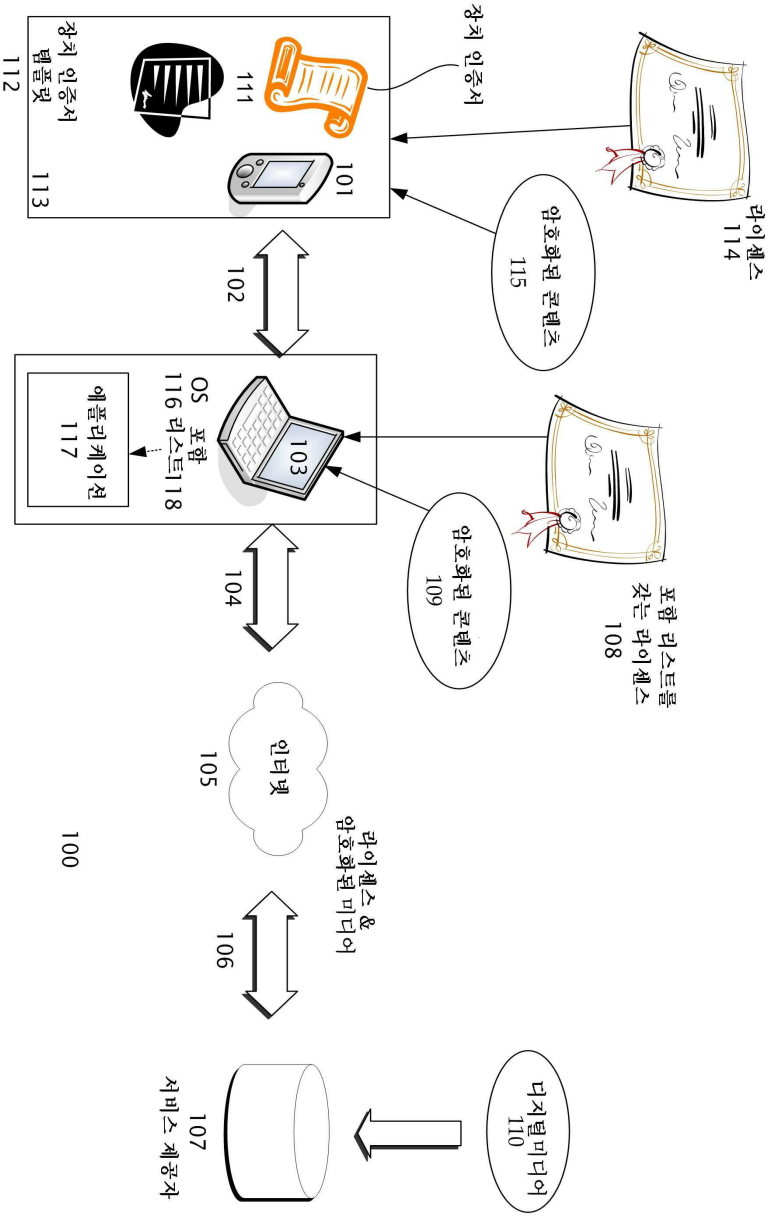
[0013] 도 4는 전사 프로세스를 이용하여 디지털 콘텐츠를 보호하기 위한 상세한 프로세스의 일 예를 도시하는 블록도이다.

[0014] 도 5는 본 출원에서 설명하는 시스템 및 방법을 구현할 수 있는 예시적인 컴퓨팅 환경을 도시한다.

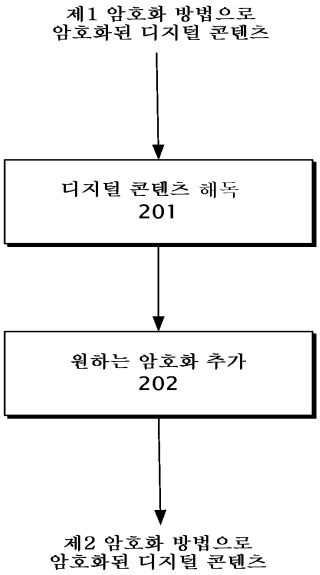
[0015] 유사한 참조 부호들은 첨부 도면에서 유사한 부분들을 지정하는 데 사용된다.

도면

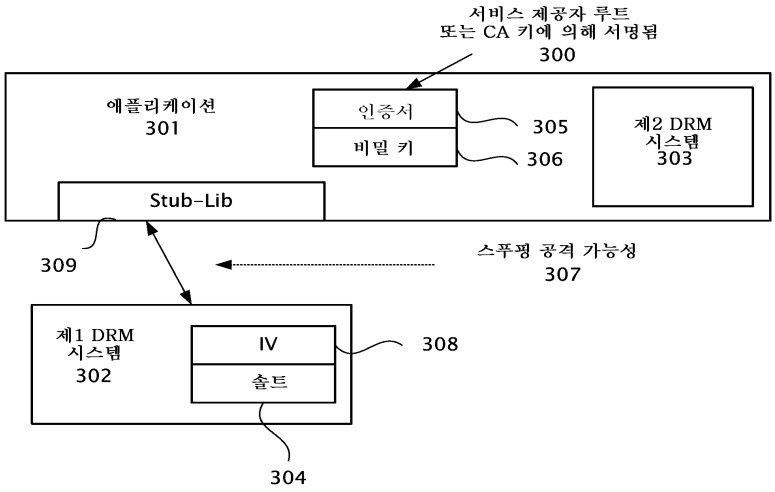
도면1


장치 인증서
111
장치 인증서 템플릿
112
113
101
102
암호화된 콘텐츠
115
라이센스
114
OS 포함 116 리스트118
103
애플리케이션
117
104
암호화된 콘텐츠
109
포함 리스트를 갖는 라이센스
108
인터넷
105
100
라이센스 & 암호화된 미디어
106
디지털미디어
110
107
서비스 제공자

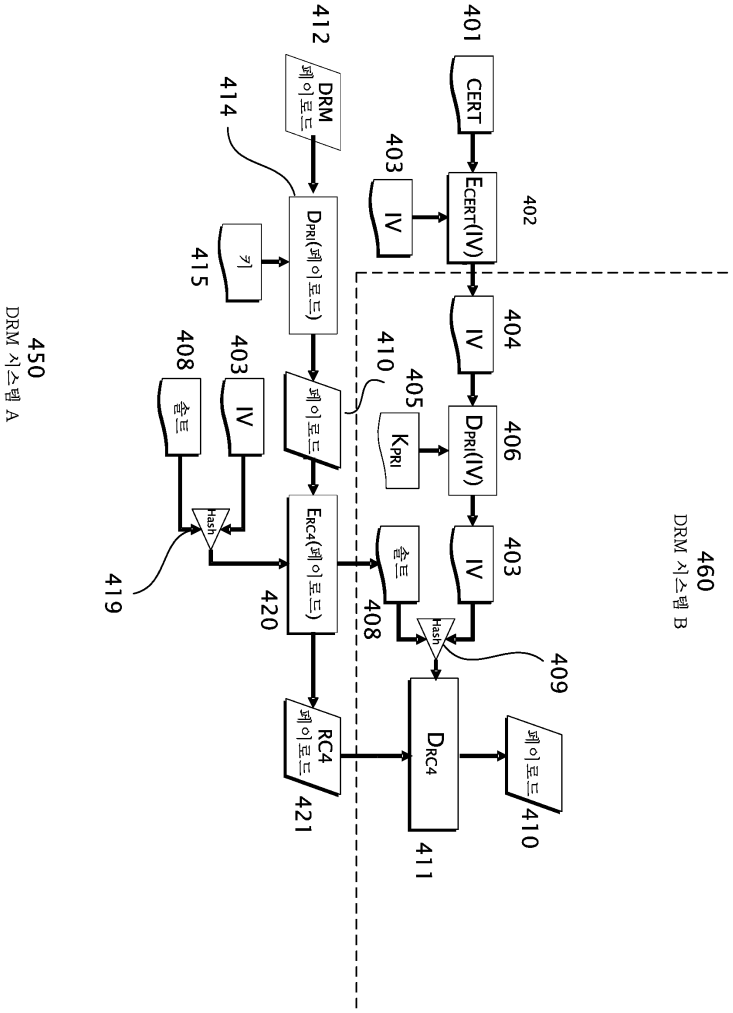
도면2


제1 암호화 방법으로
암호화된 디지털 콘텐츠
디지털 콘텐츠 해독
201
원하는 암호화 추가
202
제2 암호화 방법으로
암호화된 디지털 콘텐츠

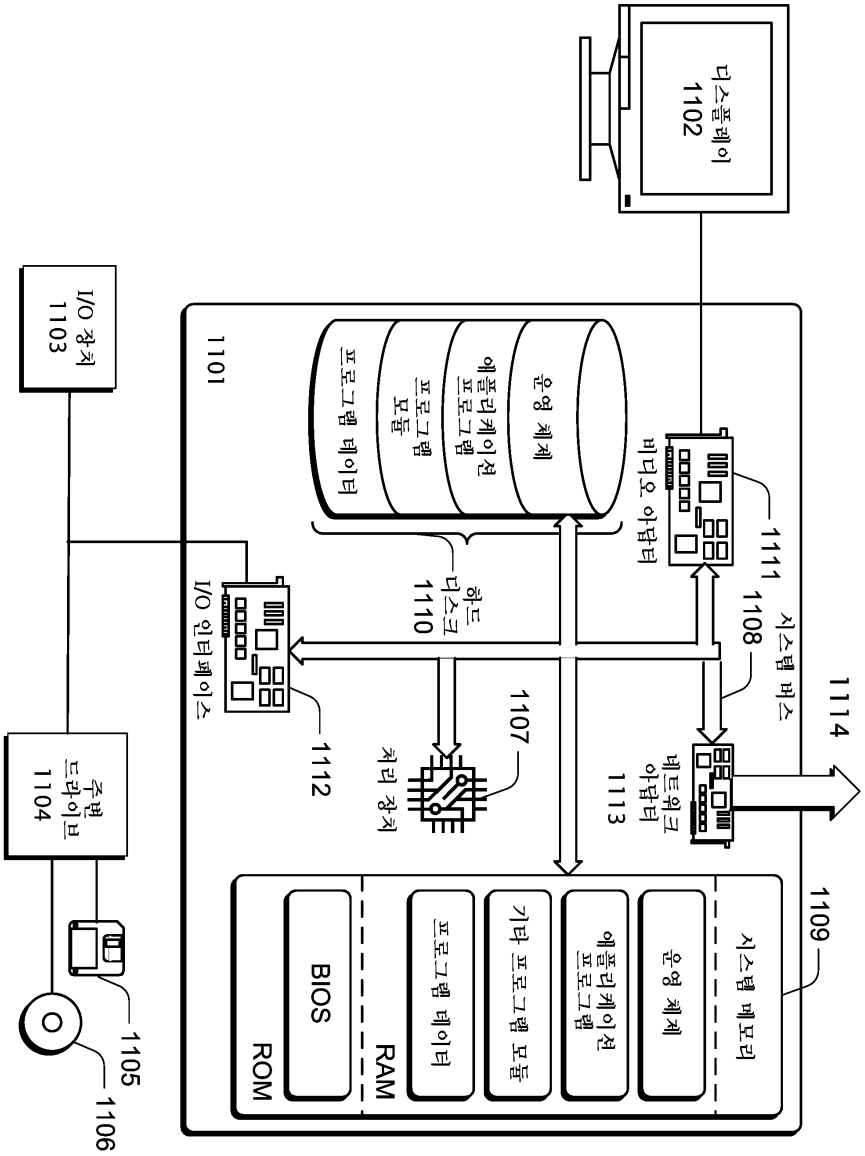
도면3


서비스 제공자 루트
또는 CA 키에 의해 서명됨
300
애플리케이션
301
인증서
비밀 키
305
306
제2 DRM
시스템
303
Stub-Lib
309
스푸핑 공격 가능성
307
제1 DRM
시스템
302
IV
솔트
308
304

도면4


401
CERT
402
ECERT(IV)
403
IV
404
IV
405
KPRI
406
DPRI(IV)
403
IV
409
Hash
410
페이로드
411
DRC4
408
솔트
410
페이로드
420
ERC4(페이로드)
419
Hash
408
솔트
403
IV
415
키
414
412
DRM 페이로드
DPRI(페이로드)
421
RC4 페이로드
460
DRM 시스템 B
450
DRM 시스템 A

도면5


디스플레이
1102
I/O 장치
1103
1101
운영 체제
애플리케이션 프로그램
프로그램 모듈
프로그램 데이터
하드 디스크
1110
비디오 아답터
1111
시스템 버스
1108
1114
I/O 인터페이스
1112
처리 장치
1107
네트워크 아답터
1113
주변 드라이브
1104
시스템 메모리
1109
운영 체제
애플리케이션 프로그램
기타 프로그램 모듈
프로그램 데이터
RAM
BIOS
ROM
1105
1106