(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년06월13일
(11) 등록번호 10-1407139
(24) 등록일자 2014년06월05일

(51) 국제특허분류(Int. Cl.)
G11B 20/10 (2006.01) *G06F 12/14* (2006.01)
H04N 21/6334 (2011.01)
(21) 출원번호 10-2008-7009168
(22) 출원일자(국제) 2006년10월17일
심사청구일자 2011년10월14일
(85) 번역문제출일자 2008년04월16일
(65) 공개번호 10-2008-0056217
(43) 공개일자 2008년06월20일
(86) 국제출원번호 PCT/FR2006/002328
(87) 국제공개번호 WO 2007/045756
국제공개일자 2007년04월26일
(30) 우선권주장
0510566 2005년10월17일 프랑스(FR)
(56) 선행기술조사문헌
US20030009668 A1*
US20050210261 A1*
J-P. Andreaux et al., 'Copy Protection System for Digital Home Networks' EEE SIGNAL PROCESSING MAGAZINE, MARCH 2004
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
디아스꼰, 장-루이스
프랑스 에프-35830 베뜬 뤼 데 샤따이그니에르스 5
듀란트, 알레인
프랑스 에프-35000 르네스 뤼 데 디난 79
르리브르, 실뱅
프랑스 에프-35760 몽뜨게르몽뜨 뤼 데 헤이예츠, 36
(74) 대리인
백만기, 전경석, 양영준

전체 청구항 수 : 총 13 항 심사관 : 장진환

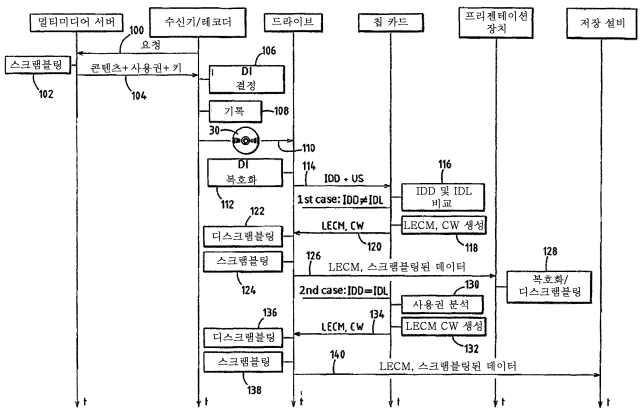
(54) 발명의 명칭 **디지털 데이터의 기록 및 안전한 분배 방법과 액세스 장치및 레코더**

(57) 요 약

본 발명은 디지털 데이터를 수신 및 안전하게 기록하는 방법에 관한 것으로, 몇몇 설비 항목을 포함하고 식별자(IDD)에 의해 정의되는 정해진 보안 영역에 속하는 레코더/수신기(6, 28)에 의해 디지털 데이터를 보안 디스크(30)상에 기록하는 단계(108)와, 멀티미디어 콘텐츠의 재생/복제가 허가되는 유일한 영역으로 이 영역을 정의하기 위해 레코더/수신기(6, 28)의 영역의 식별자(IDD)를 보안 디스크(30)상에 기록하는 단계(108)를 포함하고, 보안 디스크(30)로부터 디스크 키(DK)를 복원하는 선행 단계를 포함하며, 영역 식별자(IDD)는 디스크 키(DK)에 의해 암호화되고, 디지털 데이터는 타이틀 키에 의해 스크램블되며, 타이틀 키는 디스크 키에 의해 암호화되는 것을 특징으로 한다.

본 발명은 또한 디지털 데이터를 안전하게 분배하는 방법, 액세스 장치 및 레코더/수신기에 관한 것이다.

대 표 도 - 도3



특허청구의 범위

청구항 1

멀티미디어 콘텐츠(multimedia content)를 나타내는 디지털 데이터를 수신하고 보안 디스크 상에 보안 기록하는 방법으로서,

상기 방법은,

기록가능 매체를 위한 데이터 보호 시스템에 따라 상기 보안 디스크(30)로부터 디스크 키(DK)를 복원하는 단계 - 상기 디스크는 기록가능 매체를 위한 상기 데이터 보호 시스템에 의해 보안됨 - 및

기록하는 단계를 포함하고,

상기 기록하는 단계는,

영역에서의 데이터 보호 시스템에 따라, 몇몇 설비 항목들을 포함하고 제1 영역 식별자(IDD)에 의해 정의되는 정해진 보안 영역(determined secured domain)에 속하는 레코더(6, 28)에 의해 상기 디지털 데이터를 상기 보안 디스크(30)상에 기록하는 단계(108) - 상기 제1 영역 식별자는 상기 정해진 보안 영역의 모든 설비에 특정적임 - ; 및

상기 멀티미디어 콘텐츠의 재생(reproduction) 또는 복제(copying)가 허가된 유일한 영역으로서 상기 정해진 보안 영역을 정의하기 위해 상기 정해진 보안 영역에 속하는 상기 레코더(6, 28)에 의해 상기 레코더(6, 28)의 상기 제1 영역 식별자(IDD)를 상기 보안 디스크(30)상에 기록하는 단계(108)

영역에서의 상기 데이터 보호 시스템에 따라 제2 영역 식별자에 의해 정의되는 특정 보안 영역에서, 상기 특정 보안 영역의 상기 제2 영역 식별자를 저장하는 수단을 갖는 상기 특정 보안 영역을 액세스하기 위한 액세스 디바이스로부터, 상기 기록된 디지털 데이터를 보안 제공하는 단계 - 를 포함하고,

상기 보안 제공하는 단계는,

상기 보안 디스크 상에서 상기 액세스 디바이스에 의해 상기 정해진 보안 영역의 상기 제1 영역 식별자를 판독하는 단계;

상기 보안 디스크 상에서 판독된 상기 제1 영역 식별자를 상기 액세스 디바이스의 상기 저장 수단에 저장된 상기 제2 영역 식별자와 대비하는 단계;

상기 보안 디스크 상에서 판독된 상기 제1 영역 식별자가 상기 액세스 디바이스의 상기 저장 수단에 저장된 상기 제2 영역 식별자에 대응하지 않는 경우, 상기 디지털 데이터의 제1 동작 모드를 허가하도록 상기 액세스 디바이스에 의해 상기 디지털 데이터를 제공하는 단계; 및

상기 보안 디스크 상에서 판독된 상기 제1 영역 식별자가 상기 액세스 디바이스의 상기 저장 수단에 저장된 상기 제2 영역 식별자에 대응하는 경우, 상기 디지털 데이터의 제2 동작 모드를 허가하도록 상기 액세스 디바이스에 의해 상기 디지털 데이터를 제공하는 단계를 포함하고,

상기 제1 영역 식별자(IDD)는 상기 디스크 키(DK)에 의해 암호화되고, 상기 기록된 디지털 데이터는 타이틀 키들(title keys)에 의해 스크램블(scramble)되며, 상기 타이틀 키들은 상기 디스크 키(DK)에 의해 암호화된 것인, 방법.

청구항 2

제1항에 있어서,

상기 기록하는 단계는,

상기 멀티미디어 콘텐츠에 부여된 재생 권리(US)를 상기 보안 디스크(30)상에 기록하는 단계(108)를 더 포함하고,

상기 재생 권리(US)는 상기 멀티미디어 콘텐츠를 자유롭게 재생 또는 복제가능한 지, 상기 멀티미디어 콘텐츠를 상기 정해진 보안 영역에서만 재생 또는 복제가능한지, 혹은 상기 멀티미디어 콘텐츠를 재생 또는 복제할 수 없는지의 여부를 정의하는, 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 디지털 데이터의 상기 제1 동작 모드를 허가하도록 상기 디지털 데이터를 제공하는 경우, 상기 보안 제공하는 단계는, 상기 멀티미디어 콘텐츠의 재생 또는 복제를 금지하고 또한 상기 액세스 장치(40, 42, 44)가 상기 디지털 데이터를 판독하는 동안에만 상기 특정 보안 영역에 속하는 프리젠테이션 장치(60)상에 상기 멀티미디어 콘텐츠의 프리젠테이션을 허가하기 위한 프로토콜에 따라 상기 액세스 장치(40, 42, 44)에 의해 상기 디지털 데이터를 스크램블하는 단계(124)를 더 포함하는 방법.

청구항 5

제1항에 있어서,

상기 제2 동작 모드를 허가하도록 상기 디지털 데이터를 제공하는 경우, 상기 보안 제공 단계는,

상기 멀티미디어 콘텐츠에 부여된 재생 권리(US) - 상기 재생 권리(US)는 상기 멀티미디어 콘텐츠를 자유롭게 재생 또는 복제가능한지, 상기 멀티미디어 콘텐츠를 상기 정해진 보안 영역에서만 재생 또는 복제가능한지, 혹은 상기 멀티미디어 콘텐츠를 재생 또는 복제할 수 없는지의 여부를 정의함 - 를 상기 보안 디스크(30)상에서 판독하는 단계(112); 및

상기 보안 디스크(30)상에서 판독한 상기 재생 권리(US)에 따라 정의된 프로토콜에 따라 상기 액세스 장치(40, 42, 44)에 의해 상기 디지털 데이터를 스크램블하는 단계(132, 138)를 더 포함하는, 방법.

청구항 6

제5항에 있어서,

판독한 상기 재생 권리(US)가 상기 정해진 보안 영역에서만 상기 멀티미디어 콘텐츠의 재생 또는 복제를 허가하는 경우, 상기 액세스 장치(40, 42, 44)에 의해 상기 디지털 데이터를 스크램블하는 단계는, 상기 정해진 보안 영역에 속하는 설비(60, 62)에서만 상기 멀티미디어 콘텐츠의 프리젠테이션 및 재생 또는 복제를 허가하기 위한 프로토콜을 이용하는 단계를 포함하는 방법.

청구항 7

제5항에 있어서,

상기 재생 권리(US)가 상기 멀티미디어 콘텐츠의 재생 또는 복제를 금지하는 경우, 상기 액세스 장치(40, 42, 44)에 의해 상기 디지털 데이터를 스크램블하는 단계는, 상기 멀티미디어 콘텐츠의 재생 또는 복제를 금지시키고, 또한 상기 액세스 장치(40, 42, 44)가 상기 디지털 데이터를 판독하는 동안에 상기 정해진 보안 영역에 속한 프리젠테이션 장치(60)에서의 상기 멀티미디어 콘텐츠의 프리젠테이션만을 허가하기 위한 프로토콜을 이용하는 단계를 포함하는 방법.

청구항 8

제5항에 있어서,

상기 재생 권리(US)가 상기 멀티미디어 콘텐츠의 자유로운 재생 또는 복제를 허가하는 경우, 상기 액세스 장치(40, 42, 44)에 의해 상기 디지털 데이터를 스크램블하는 단계는, 임의 설비(60, 62, 64)에서의 상기 멀티미디어 콘텐츠의 프리젠테이션 및 재생 또는 복제를 허가하기 위한 프로토콜을 이용하는 단계를 포함하는 방법.

청구항 9

제2항에 있어서,

상기 방법은,

원격 서버(10)로부터 상기 레코더(6, 28)로 상기 멀티미디어 콘텐츠에 부여된 상기 재생 권리(US)를 전송하는 단계(104)를 더 포함하고, 상기 전송하는 단계는 상기 재생 권리(US)의 기록 단계의 이전에 수행되는, 방법.

청구항 10

제9항에 있어서,

상기 제1 영역 식별자(IDD) 및 상기 전송된 재생 권리(US)를 암호화하는 단계를 더 포함하고, 상기 암호화하는 단계는, 상기 재생 권리(US)의 기록 단계와 상기 제1 영역 식별자의 기록 단계 이전에 수행되는, 방법.

청구항 11

특정 보안 영역을 액세스하기 위한 장치(40, 42, 44)로서,

기록가능 매체를 위한 데이터 보호 시스템에 의해 보안되는 보안 디스크(30)상에 기록된 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 판독하는 수단(45) - 상기 판독 수단(45)은 상기 보안 디스크(30)상에서 정해진 보안 영역의 제1 영역 식별자(IDD)를 판독함 - ;

상기 액세스 장치(40, 42, 44)가 속한 상기 특정 보안 영역의 제2 영역 식별자(IDL)를 저장하는 수단(56) - 상기 제2 영역 식별자는 영역에서의 데이터 보호 시스템에 의해 정의됨 - ;

상기 저장 수단(56)에 저장된 상기 제2 영역 식별자(IDL)를 상기 보안 디스크(30)상에서 판독한 상기 제1 영역 식별자(IDD)와 비교하고, 또한 디스크 키(DK)를 이용하여 상기 제1 영역 식별자(IDD)를 복호화하는 수단(56); 및

상기 보안 디스크(30)상에서 판독한 상기 제1 영역 식별자(IDD)가 상기 액세스 장치(40, 42, 44)의 상기 저장 수단(56)에 저장된 상기 제2 영역 식별자(IDL)에 대응하지 않는 경우 상기 디지털 데이터의 제1 동작 모드를 허가하도록 디지털 데이터를 제공하고, 또한 상기 보안 디스크(30)상에서 판독한 상기 제1 영역 식별자(IDD)가 상기 액세스 장치(40, 42, 44)의 상기 저장 수단(56)에 저장된 상기 제2 영역 식별자(IDL)에 대응하는 경우 상기 디지털 데이터의 제2 동작 모드를 허가하도록 상기 디지털 데이터를 제공하기 위한 수단(50)

을 포함하며,

상기 액세스 장치(40, 42, 44)는,

기록가능 매체를 위한 상기 데이터 보호 시스템에 따라 상기 보안 디스크(30)로부터 상기 디스크 키(DK)를 복원하고, 또한 상기 디스크 키(DK)를 이용하여 상기 제1 영역 식별자(IDD)를 복호화하기 위한 암호화 또는 복호화 수단(48); 및

상기 디스크 키(DK)를 이용하여 상기 보안 디스크(30)상에 기록된 상기 디지털 데이터를 디스크램블(descramble)할 수 있는 스크램블링 또는 디스크램블링 수단(50)을 더 포함하고,

상기 제1 영역 식별자(IDD)는 상기 디스크 키(DK)에 의해 암호화되고, 상기 기록된 디지털 데이터는 타이틀 키들(title keys)에 의해 스크램블(scramble)되며, 상기 타이틀 키들은 상기 디스크 키(DK)에 의해 암호화된 것인, 액세스 장치.

청구항 12

몇몇 설비 항목들을 포함하는 보안 영역에 속하는 레코더(6, 28)로서 - 상기 보안 영역은 영역에서의 데이터 보호 시스템에 따라 제1 영역 식별자(IDD)에 의해 정의되고, 상기 제1 영역 식별자(IDD)는 상기 보안 영역의 상기 설비 모두에 대해 특정된 것이며, 상기 레코더(6, 28)는 기록가능 매체를 위한 데이터 보호 시스템에 의해 보안되는 디스크와 협력함 - ;

상기 레코더는 프로세서를 포함하고,

상기 프로세서는,

멀티미디어 콘텐츠를 나타내는 디지털 데이터를 상기 보안 디스크(30) 상에 기록하는 단계;

상기 멀티미디어 콘텐츠의 재생 또는 복제가 허가되는 유일한 영역으로서 정해진 보안 영역을 정의하기 위해 상기 레코더(6, 28)의 상기 제1 영역 식별자(IDD)를 상기 보안 디스크(30)상에 기록하는 단계;

액세스 디바이스가 속하는 특정 보안 영역의 제2 영역 식별자를 저장하는 단계 - 상기 제2 영역 식별자는 영역에서의 데이터 보호 시스템에 의해 정의됨 -;

상기 보안 디스크 상에서 판독되는 상기 제1 영역 식별자가 상기 액세스 디바이스에 저장되는 제2 영역 식별자에 대응하지 않는 경우 디지털 데이터의 제1 동작 모드를 허가하도록 상기 디지털 데이터를 제공하고, 상기 보안 디스크 상에서 판독되는 상기 제1 영역 식별자가 상기 액세스 디바이스에 저장되는 상기 제2 영역 식별자에 대응되는 경우 상기 디지털 데이터의 제2 동작 모드를 허가하도록 상기 디지털 데이터를 제공하는 단계;

기록가능 매체를 위한 데이터 보호 시스템에 따라 상기 보안 디스크(30)로부터 디스크 키(DK)를 복원하는 단계; 및

상기 디스크 키(DK)에 의해 암호화된 타이틀 키들로 상기 디지털 데이터를 스크램블하고, 상기 디스크 키(DK)를 이용하여 상기 제1 영역 식별자(IDD)를 암호화하고, 상기 스크램블된 디지털 데이터 및 상기 암호화된 제1 영역 식별자(IDD)를 기록하는 단계를 수행하도록 구성되는, 레코더(6, 28).

청구항 13

제12항에 있어서,

상기 프로세서는,

멀티미디어 콘텐츠에 부여된 재생 권리(US) - 상기 재생 권리(US)는 상기 멀티미디어 콘텐츠를 자유롭게 재생 또는 복제가능한지, 상기 멀티미디어 콘텐츠를 정해진 보안 영역에서만 재생 또는 복제가능한지, 혹은 상기 멀티미디어 콘텐츠를 재생 또는 복제할 수 없는지의 여부를 정의함 - 를 기록하는 단계를 수행하도록 더 구성되는, 레코더(6, 28).

청구항 14

제13항에 있어서,

상기 멀티미디어 콘텐츠에 부여된 재생 권리(US)는 상기 멀티미디어 콘텐츠에 대해 허용된 재생 횟수를 포함하는, 레코더(6, 28).

명 세 서

기 술 분 야

[0001] 본 발명은 멀티미디어 콘텐츠(multimedia content)를 나타내는 디지털 데이터를 기록(record), 제공(provision) 및 안전하게 분배(distribute)하는 방법에 관한 것이다.

배 경 기 술

[0002] 멀티미디어 콘텐츠의 불법 복제를 피하기 위하여, 문서 JP 2001/195826은 각 장치에 특정하며 다른 장치의 식별자와 상이한 식별자를 저장하는 메모리를 구비한 장치를 개시한다. 이 장치는 각 기록시에 디지털 데이터 및, 그 자신의 식별자를 저장 매체상에 저장하는데 적합하다. 이는 디지털 데이터를 판독하기 전에 그의 식별자와 저장 매체상에서 읽어낸 식별자를 비교하여 일치할 시에만 디지털 데이터를 프리젠테이션(presentation)하는데 적합하다.

[0003] 이 장치는 저작권을 준수하면서 디지털 데이터가 고유한 장치상에서만 프리젠테이션될 수 있게 한다.

[0004] 디지털 데이터에 부여된 저작권을 준수하면서 디지털 데이터를 보다 널리 분배하기 위하여 콘텐츠 스크램블링 시스템(CSS: content scrambling system) 방법과 같은 데이터 보호법에 의해 보안 DVD상에 기록된 디지털 데이터를 보호하는 것이 알려져 있다.

[0005] 그러나 이 방법에서 임의 허가된 드라이브가 보안 DVD상에 기록된 디지털 데이터를 판독할 수는 있지만 복제하거나 혹은 재생할 수 없다.

[0006] 또한 이 분야에서 문서 "SmartRight Technical white paper, Version 1.7, Janunary 2003, Thomson"에 기술된 등록상표 "스마트라이트(SmartRight)" 방법, 그리고 문서 "xCP: eXtensible Content Protection. 2003. IBM", "xCP Cluster Protocol, IBM Presentation to Copy Protection Technical Working Group, July 18, 2002"에

기술된 등록상표 "확장형 콘텐츠 보호(eXtensible Content Protection)" 방법과 같은 보호 방법이 알려져 있다. 이들 방법에서는 동일한 영역(domain)에 속한 설비만이 해독할 수 있는 암호화 프로토콜에 따라 디지털 데이터를 스크램블할 수 있다. 한 영역에 속한 설비만이 암호화된 디지털 데이터를 프리젠테이션 또는 복제/재생할 수 있다.

[0007] 그러나 이 영역을 액세스하지 않는 사람은 이 디지털 정보를 공유할 수 없다. 따라서 친구 또는 지인과 이 디지털 데이터를 공유할 수 없다.

[0008] 또한 미국 문서 2004/0230532으로부터 명백히 알 수 있는 바와 같이, 디지털 데이터 복제 관리 시스템은 하나의 동일한 레코더(recorder)에 의해 디지털 데이터의 한 번 이상의 재생/복제가 가능하지만 다른 레코더에 의한 복제는 금지시킬 수 있다.

[0009] 이 시스템은 사용자를 위한 인터넷망 및 특정 레코더/드라이브를 통해 액세스 가능한 서버를 구비한다. 각 기록시에, 각 레코더/드라이브는 그에 특정한 식별자, DVD 식별자, 그리고 DVD상에서 판독되는 콘텐츠 식별자를 서버로 전송하는 데 적합하다. 이 서버는 데이터베이스, 레코더에 의해 전송된 식별자를 등록하는 수단, 그리고 레코더에 의해 전송된 식별자가 데이터베이스에 이미 저장된 식별자와 일치하는지의 여부를 검사하기 위하여 그의 데이터베이스에 저장된 식별자와 레코더에 의해 전송된 식별자를 비교하는 수단을 포함한다.

[0010] 그러나 이러한 시스템은 복잡하며 상당량의 데이터를 포함한 데이터베이스 의 관리를 필요로 한다.

발명의 상세한 설명

[0011] 본 발명의 목적은 부여된 저작권을 준수하면서 디지털 데이터의 어느 정도의 공유를 가능하게 하는, 디지털 데이터를 안전하게 분배하는 방법에 관한 것이다.

[0012] 이를 위하여, 본 발명은 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 수신 및 안전하게 기록하는 방법에 관한 것으로, 몇몇 설비 항목을 포함하는 정해진 보안 영역 - 상기 정해진 보안 영역은 그 영역의 모든 설비에 특정된 식별자에 의해 정의됨 - 에 속하는 레코더/수신기에 의해 디지털 데이터를 보안 디스크상에 기록하는 단계 및, 멀티미디어 콘텐츠의 재생/복제가 허가되는 유일한 영역인 이 영역을 정의하기 위하여 레코더/수신기의 영역 식별자를 보안 디스크상에 기록하는 단계를 포함하고, 보안 디스크로부터 디스크 키(disk key)를 복원하는 이전 단계를 더 포함하며, 영역 식별자는 상기 디스크 키에 의해 암호화되고, 기록된 디지털 데이터는 타이틀 키(title keys)에 의해 스크램블되며, 상기 타이틀 키는 상기 디스크 키에 의해 암호화되는 것을 특징으로 한다.

[0013] 특정 실시예에 따라서, 수신 및 기록 방법은 멀티미디어 콘텐츠에 부여되어 멀티미디어 콘텐츠를 자유롭게 재생/수신가능한지, 멀티미디어 콘텐츠를 정해진 영역에서만 자유롭게 재생/복제가능한지, 혹은 멀티미디어 콘텐츠를 재생/복제할 수 없는지의 여부를 정의하는 재생 권리(reproduction rights)를 보안 디스크상에 기록하는 단계를 더 포함한다.

[0014] 본 발명의 두 번째 양상은 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 안전하게 분배하는 방법에 관한 것으로,

[0015] - 레코더/수신기에 의해 보안 디스크상에 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 수신 및 기록하는 단계로서, 상기 기록 단계는 전술한 수신 및 기록 방법에 의해 수행되고,

[0016] - 식별자에 의해 정의된 특정 보안 영역에서, 이 특정 영역의 식별자를 저장하는 수단을 포함한 특정 보안 영역은 액세스하려는 장치로부터 상기 기록된 디지털 데이터를 안전하게 제공하는 단계로서, 상기 제공 단계는:

[0017] - 액세스 장치가 보안 디스크상에서 정해진 보안 영역의 식별자를 판독하는 단계,

[0018] - 보안 디스크상에서 판독한 식별자와 액세스 장치의 저장 수단에 저장된 식별자를 비교하는 단계,

[0019] - 보안 디스크상에서 판독한 식별자가 액세스 장치의 저장 수단에 저장된 식별자와 일치하지 않을 때, 액세스 장치에 의해 디지털 데이터의 제1 동작 모드를 허가하도록 디지털 데이터를 제공하는 단계,

[0020] - 보안 디스크상에서 판독한 식별자가 액세스 장치의 저장 수단에 저장된 식별자와 일치할 때, 액세스 장치에 의해 디지털 데이터의 제2 동작 모드를 허가하도록 디지털 데이터를 제공하는 단계를 포함한다.

[0021] 특정 실시예에 따라서, 분배 방법은 하나 이상의 다음 특징을 포함한다:

[0022] - 디지털 데이터의 제1 동작 모드를 허가하기 위해 디지털 데이터를 제공할 때, 제공 단계는 멀티미디어 콘텐츠의 재생/복제를 금지하고, 액세스 장치가 디지털 데이터를 판독하는 동안에만 특정 영역에 속한 프리젠테이션 장치상에 멀티미디어 콘텐츠의 프리젠테이션을 허가하도록 적합한 프로토콜에 따라 액세스 장치에 의해 디지털 데이터를 스크램블하는 단계를 포함하고,

[0023] - 제2 동작 모드를 허가하도록 디지털 데이터를 제공시에, 상기 제공 단계는,

[0024] - 액세스 장치가 보안 디스크상에 사전기록된 재생 권리를 판독하는 단계,

[0025] - 보안 디스크상에서 멀티미디어 콘텐츠에 부여된 재생 권리를 판독하는 단계로서, 상기 재생 권리는 멀티미디어 콘텐츠를 자유롭게 재생/복제가능한지, 정해진 영역에서 멀티미디어 콘텐츠를 재생/복제할 수 있는지, 혹은 멀티미디어 콘텐츠를 재생/복제할 수 없는 지의 여부를 정의하고,

[0026] - 보안 디스크상에서 판독한 재생 권리에 따라 정의된 프로토콜에 따라서 액세스 장치에 의해 디지털 데이터를 스크램블하는 단계를 포함하고,

[0027] - 판독된 재생 권리가 단지 정해진 영역에서의 멀티미디어 콘텐츠의 재생/복제를 허가할 때, 상기 제공 단계는 정해진 영역에 속한 설비에서만 멀티미디어 콘텐츠의 재생/복제 및 프리젠테이션을 허가하도록 적합한 프로토콜에 따라 액세스 장치에 의해 디지털 데이터를 스크램블하는 단계를 포함하고,

[0028] - 재생 권리가 멀티미디어 콘텐츠의 재생/복제를 금지할 때, 상기 제공 단계는 액세스 장치가 디지털 데이터를 판독하는 동안에 멀티미디어 콘텐츠의 재생/복제를 금지하고, 정해진 영역에 속한 프리젠테이션 장치상에서의 멀티미디어 콘텐츠의 프리젠테이션만을 허가하도록 적합한 프로토콜에 따라 액세스 장치에 의해 디지털 데이터를 스크램블하는 단계를 포함하고,

[0029] - 재생 권리가 멀티미디어 콘텐츠의 자유로운 재생/복제를 허가할 때, 상기 제공 단계는 임의 설비상에서 멀티미디어 콘텐츠의 재생/복제 및 프리젠테이션을 허가하도록 적합한 프로토콜에 따라 액세스 장치에 의해 디지털 데이터를 스크램블하는 단계를 포함하고,

[0030] - 재생 권리의 기록 단계에 앞서서, 원격 서버로부터 상기 레코더/수신기로 멀티미디어 콘텐츠에 부여된 재생 권리를 전송하기 위한 단계를 더 포함하고,

[0031] - 기록 단계에 앞서서, 식별자 및 재생 권리를 암호화하는 단계를 포함한다.

[0032] 본 발명의 제3 양상은 특정 보안 영역을 액세스하기 위한 장치에 대한 것으로, 액세스 장치는:

[0033] - 보안 디스크상에 기록된 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 판독하기 위한 것으로, 보안 디스크상에서 정해진 보안 영역의 식별자를 판독하는 데 적합한 수단,

[0034] - 액세스 장치가 속한 특정 영역의 식별자를 저장하기 위한 수단,

[0035] - 보안 디스크상에서 판독한 식별자와 저장 수단에 저장된 식별자를 비교하고, 디스크 키를 이용하여 영역 식별자를 복호화하는 수단,

[0036] - 보안 디스크상에서 판독한 식별자가 액세스 장치의 저장 수단에 저장된 식별자와 일치하지 않을 시에는 디지털 데이터의 제1 동작 모드를 허가하도록 디지털 데이터를 제공하고, 보안 디스크상에서 판독한 식별자가 액세스 장치의 저장 수단에 저장된 식별자와 일치할 시에는 디지털 데이터의 제2 동작 모드를 허가하도록 디지털 데이터를 제공하기에 적합한 수단을 포함하고, 상기 액세스 장치는,

[0037] - 보안 디스크로부터의 디스크 키를 복원하고, 디스크 키를 이용하여 영역 식별자를 복호화하는데 적합한 암호화/복호화 수단,

[0038] - 디스크 키를 이용하여 보안 디스크상에 기록된 디지털 데이터를 디스크램블(descramble)할 수 있는 스크램블링/디스크램블링 수단을 포함한다.

[0039] 본 발명의 제 4 양상은 몇몇 설비 항목을 포함하는 보안 영역 - 상기 보안 영역은 그 영역의 모든 설비에 특정된 식별자에 의해 정의됨 - 속하는 레코더/수신기에 관한 것으로, 상기 레코더/수신기는 보안 디스크상에 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 기록하기에 적합하며, 멀티미디어 콘텐츠의 재생/복제가 허가되는 영역에서만 이 영역을 정의하도록 레코더/수신기의 영역 식별자를 정의하도록 레코더/수신기의 영역 식별자를 보안 디스크상에 기록하기에 적합하고, 또한 상기 레코더/수신기는 보안 디스크로부터 디스크 키를 복원하고,

디스크 키에 의해 암호화된 타이틀 키로써 디지털 데이터를 스크램블하고, 디스크 키를 이용하여 식별자를 암호화하고, 그리고 상기 스크램블된 디지털 데이터와 상기 암호화된 식별자를 기록하기에 적합한 것을 특징으로 한다.

[0040] 특정 실시예에 따라서, 레코더/수신기는 다음의 하나 이상의 특징을 포함한다:

[0041] - 멀티미디어 콘텐츠에 부여된 재생 권리를 기록하는데 적합하고, 재생 권리는 멀티미디어 콘텐츠를 자유롭게 재생/복제가능한지, 멀티미디어 콘텐츠를 정해진 영역에서만 재생/복제가능한지, 혹은 멀티미디어 콘텐츠를 재생/복제할 수 없는지의 여부를 정의하고,

[0042] - 멀티미디어 콘텐츠에 부여된 재생 권리가 멀티미디어 콘텐츠의 허용된 재생 횟수를 포함한다.

실 시 예

[0046] 본 발명은 후속된 예 및 도면을 참조한 다음의 상세한 설명으로부터 보다 명백히 이해될 것이다.

[0047] 본 발명에 따른 방법이 구현된 시스템(2)이 도 1 및 도 2에 도시되어 있다. 이 시스템(2)은 DVD를 교류할 것 같은 상이한 사용자들에게 속한 DVD 레코더 또는 DVD 드라이브를 가진 IT 설비 항목 집합에 관한 것이다. 이 설비 항목은 상이한 보안 영역들간에 분산된다.

[0048] 하나의 보안 영역에 속한 설비 항목의 각각은 메모리에 이 영역을 나타내는 하나의 동일한 식별자 및 영역 키를 가진다. 이 영역에서의 설비는 이 영역 키에 의해 스크램블된 디지털 데이터를 네트워크를 통해 통신할 수 있다. 이 보안 영역에 속하지 않거나 혹은 다른 보안 영역에 속한 설비는 이 네트워크를 통해 스크램블된 데이터 또는 네트워크의 설비상에 보호된 스크램블 데이터를 판독할 수 없다.

[0049] 도 1에서 알 수 있는 바와 같이, 시스템(2)은 인터넷망과 같은 분산망(8)을 통하여 디지털 데이터를 수신 장치(6)로 제공하는데 적합한 콘텐츠 제공자(4)를 포함한다.

[0050] 콘텐츠 제공자(4)는 데이터베이스(12)에 연결된 멀티미디어 서버(10)를 구비한다.

[0051] 데이터베이스(12)는 예를 들면 오디오, 비디오 또는 문자 데이터열, 또는 소프트웨어를 셋업하는데 사용되는 컴퓨터 데이터파일과 같은 멀티미디어 콘텐츠를 나타내는 디지털 데이터를 저장하는데 적합하다.

[0052] 디지털 데이터는 예를 들면 MPEG-2 표준(ISO/IEC 13818-1)에 따른 패킷 형태로 암호화된다.

[0053] 데이터베이스(12)에서, 각 멀티미디어 콘텐츠는 하나 이상의 사용권(usages) 또는 재생 권리, 그리고 이들 사용권 또는 권리에 따라 가변적인 비용과 관련 있다.

[0054] 사용권은 멀티미디어 콘텐츠의 복제 또는 재생에 부여된 보호 유형을 식별한다. 전술한 실시예에서, 사용권은 멀티미디어 콘텐츠를 자유롭게 복제/재생가능한지, 이를 보안 DVD로 복제할 수 있는지, 혹은 보안 DVD로 복제할 수 있으면서 보안 DVD상의 콘텐츠를 기록한 레코더가 속한 영역에 대응한 단일 영역에서 복제/재생가능한지를 정의한다.

[0055] 멀티미디어 서버(10)는 분산망(8)으로/으로부터 디지털 데이터를 송신/수신하기 위한 수단(14)과, 이 디지털 데이터를 스크램블하기 위한 모듈(16)을 포함한다.

[0056] 스크램블링 모듈(16)은 CSS 시스템에 따라서 데이터를 스크램블링하기에 적합하다.

[0057] 수신 장치(6)는 컴퓨터 또는 셋탑 박스(set-top box)이다. 이것은 분산망(8)을 통하여 비디오 프로그램을 액세스하길 원하는 사용자의 가정에 정상적으로 설치된다.

[0058] 수신 장치(6)는 예를 들면 등록상표인 스마트라이트(SmartRight)를 가진 시스템과 같은 보안 시스템에 의해 보호되는 영역에 속한다.

[0059] 이 보안 영역에 속하는 설비 항목들의 각각은 메모리에 이 영역을 나타내는 하나의 동일한 식별자(IDD) 및 영역 키(DIK)를 가진다.

[0060] 수신 장치(6)는 프로세서(18), 암호화/복호화 모듈(20), 키보드, 스크린 또는 원격제어 유형의 사용자 인터페이스(22), 그리고 데이터를 송수신하기 위한 네트워크 인터페이스(24)를 가진다.

[0061] 프로세서(18)는 스마트라이트 데이터 보안 시스템의 프로토콜 및, 스크램블링 모듈(16)에 의해 사용되는 보안 시스템에 대응하는 CSS 보안 시스템의 프로토콜을 실행하는데 적합하다. 이를 위하여 특히 수신 장치(6)가 속

한 영역의 식별자(IDD) 및 마스터 키(MK)를 포함한다.

[0062] 인터페이스(24)는 실시간 다운로드(또는 스트리밍)에 의해, 즉 로딩하면서 콘텐츠를 보거나, 혹은 콘텐츠를 오프라인으로 볼 수 있도록 미리 다운로드함으로써 분산망(8)으로부터 데이터 스트림을 수신하는데 적합하다.

[0063] 수신 장치(6)는 예를 들면 DVD-R, DVD-RW, DVD+R, DVD+RW 또는 DVD-RAM 형의 DVD(30)의 레코더(28)에 연결된다.

[0064] DVD(30)는 CSS 보안 시스템의 프로토콜에 따라 보호되는 디스크 키 집합으로써 사전기록된 시작 영역(32), 저장 영역(34) 및 디지털 데이터 기록 영역(36)을 포함한다.

[0065] 저장 영역(34)은 임의 레코더에 의해 기록될 수 있는 특정한 DVD 영역이다. DVD-R형 DVD인 경우, 저장 영역(34)은 예를 들면 RMD 필드(2)로 불리는 필드를 포함한다. 이 필드는 문서 "DVD Specifications for Recordable Disk for General, Part 1, Physical Specifications, Version 2.0, May 2000"에 정의되어 있다.

[0066] 도 2에서 알 수 있는 바와 같이, 본 발명에 따른 시스템(2)은 또한 스마트라이트 보안 시스템에 의해 보호되는 영역을 액세스하기 위한 장치를 형성하는 DVD 드라이브(40)를 포함한다. 드라이브(40)는 칩 카드(44)를 수신하도록 설계된 칩 카드 판독기(42)에 연결된다.

[0067] 드라이브(40)는 DVD 판독수단(45), 그리고 암호화/복호화 모듈(48)에 연결되어 마스터 키(MK')를 저장하는 수단(46)을 포함한다.

[0068] 또한 드라이브(40)는 스크램블링/디스크램블링 모듈(50), 그리고 예를 들면 국내망, 인트라넷망 또는 인터넷망과 같은 분산망(54)을 통하여 디지털 데이터를 송신 및 수신하기 위한 네트워크 인터페이스(52)를 포함한다.

[0069] 칩 카드(44)는 보안 프로세서(56)를 포함한다. 이 프로세서(56)는 드라이브(40)가 속한 영역에 특정적인 식별자(IDL)와 이 영역의 암호화 키(DOK)를 안전하게 저장하기에 적합하다.

[0070] 프로세서(56)는 데이터를 비교하고 드라이브(40)로/로부터 데이터를 전송 및 수신하기에 적합한데, 스마트라이트 보안 프로토콜에 따라 난수를 생성하여 이들을 암호화한다.

[0071] 또한 시스템(2)은 털레비젼형 프리젠테이션 장치(60), 레코더(62) 및 저장 설비(64)를 포함한다.

[0072] 프리젠테이션 장치(60) 및 레코더(62) 각각은 드라이브(40)로부터 디지털 데이터를 수신하거나, 혹은 저장 설비(64)상의 디지털 데이터를 검색하기 위한 네트워크 인터페이스(70, 72)를 포함한다.

[0073] 프리젠테이션 장치(60)는 디스크램블링 모듈(66)을 구비한다. 이것은 보안 프로세서(57)에서 이 영역의 식별자(IDL) 및 암호화 키(DOK)를 저장하는 칩 카드(47)를 수신하는 칩 카드 판독기(43)에 연결된다.

[0074] 분산망(54)에 연결된 임의 설비, 특히 식별자(IDL)에 의해 정의된 영역에 속하지 않는 설비가 저장 설비(64)를 액세스할 수 있다.

[0075] 도 3에서, 수직축은 시간축을 나타내고, 수평선은 도 1 및 도 2에 도시된 시스템의 설비 항목들간의 교환(exchange)을 도시한다.

[0076] 제1 단계(100)에서, 사용자는 비디오 시퀀스, 예를 들면 필름 또는 DVD(30)상에 기록하길 원하는 특정 전송을 선택하기 위하여 수신 장치의 사용자 인터페이스(22)를 사용한다.

[0077] 레코더(28)는 DVD의 시작 영역(32)상에 기록된 모든 보안 디스크 키를 판독하고, 이 보안 디스크 키 집합을 수신 장치(6)로 전송한다.

[0078] 수신 장치(6)의 암호화/복호화 모듈(20)은 이 보안 키 집합으로부터 디스크 키(DK) 및 마스터 키(MK)를 복원한다.

[0079] 그 후, 수신 장치(6)는 멀티미디어 서버(10)의 주소로 전송할 비디오 콘텐츠 요청 메시지를 구성한다. 이 요청은 주문한 비디어 시퀀스의 식별자, 수신 장치(6)의 식별자, 구한 디스크 키(DK), 요청된 사용권 표시 및 지불 지시사항을 포함한다.

[0080] 다음 단계(102)에서, 멀티미디어 서버(10)는 데이터베이스(12)에서 요청된 비디어 콘텐츠를 검색하고, 타이틀 키를 이용하여 이를 스크램블하고, 그리고 CSS 프로토콜에 따라 수신한 디스크 키(DK)를 이용하여 타이틀 키를 암호화한다.

[0081] 단계(104)에서, 멀티미디어 서버(10)는 타이틀 키에 의해 스크램블된 비디오 콘텐츠, 디스크 키(DK)에 의해 암호화된 타이틀 키, 그리고 사용자가 구입한 사용 표시를 수신 장치(6)로 전송한다.

[0082] 단계(106) 동안에, 수신 장치의 암호화/복호화 모듈(20)은 영역 정보(DI)를 결정 및 암호화한다. 이 영역 정보(DI)는 사용자가 구입한 사용권, 수신 장치가 속한 영역의 식별자(IDD)를 포함한다.

[0083] 예를 들면, 영역 정보(DI)는 다음의 형태를 가진다:

[0084] DI=AES[DDK](IDD‖US)

[0085] - AES는 암호화 표준(Advanced Encryption Standard);

[0086] - "‖"는 연결 연산자;

[0087] - DDK는 AES에 의해 요구되는 크기의 키를 얻기 위하여 예를 들면, 키 DK의 하위 비트와 "0"을 연결시킴으로써 디스크 키(DK)로부터 도출한 AES 암호화 표준에 적합한 키;

[0088] - IDD는 수신 장치 영역의 식별자;

[0089] - US는 비디오 콘텐츠에 부여된 사용권의 스마트라이트 포맷 전사.

[0090] 단계(108)에서, 레코더(28)는 데이터 기록 영역(36)상에 스크램블된 비디오 콘텐츠를, 저장 영역(34)상에 영역 정보(DI)를 기록한다.

[0091] 따라서 사용자는 CSS 명세에 따라 보호된 비디오 콘텐츠와, 멀티미디어 콘텐츠가 기록되었고 DVD에 부여되는 특정 영역을 특징짓는 식별자(IDD)를 포함한 DVD(30)를 가진다.

[0092] 단계(110) 동안에, 사용자는 다운로드한 비디오 콘텐츠를 식별자(IDL)에 의해 정의된 영역의 설비로 이용할 수 있기를 원한다.

[0093] 이를 위하여 DVD(30)를 이 영역에 속한 드라이브(40)로 삽입한다. 드라이브의 판독 수단(45)은 DVD의 시작 영역(32)에서의 모든 보안 디스크 키와 DVD의 저장 영역(34)에 저장된 영역 정보(DI)를 판독한다.

[0094] 단계(112) 동안에, 암호화/복호화 모듈(48)은 (CSS 명세 원리에 따라) 보안 디스크 키 집합으로부터 디스크 키(DK)와, 드라이브(40)에 포함된 마스터 키(MK')를 복원한다. 이 디스크 키(DK)로부터 키(DDK)를 추론하고, 이 키(DDK)를 이용하여 복호화하고, 영역 정보(DI)를 사용하여 사용권(US) 및, DVD(30)가 기록되었던 영역의 식별자(IDD)를 복원한다.

[0095] 단계(114) 동안에, 드라이브(40)는 사용권(US) 및 식별자(IDD)를 칩 카드(44)로 전송한다.

[0096] 단계(116) 동안에, 칩 카드의 프로세서(56)는 저장한 식별자(IDL)와 DVD에 기록된 식별자(IDD)가 일치하는 지의 여부를 검사한다.

[0097] DVD(30)상에 기록된 식별자(IDD)가 칩 카드의 식별자(IDL)와 일치하지 않는 다면, DVD(30)는 드라이브(40)와 동일한 영역에 속하는 레코더에 의해 기록되지 않는다.

[0098] 이 경우에 단계(118) 동안, 칩 카드의 프로세서(56)는 통상 CW로 표기되는 제어 단어, LECM으로 표기되는 제어 메시지(로컬 자격 제어 메시지)를 생성한다. 제어 메시지(LECM)는 영역키(DOK), 드라이브(40)의 영역 식별자(IDL), 보전성 검사(integrity check), 그리고 보전성 계산에 의해 보호되는 사용권(US)만을 사용하여 복호화할 수 있도록 암호화된 제어 단어(CW)를 포함한다. 이들 제어 메시지(LECM)는 드라이브(40)와 동일한 영역에 속한 설비에 의해서만 복호화될 수 있다.

[0099] 식별자(IDD)가 식별자(IDL)와 상이할 때, 제어 메시지(LECM)에 포함된 제어 단어(CW)는 수퍼암호화된다(superencrypt).

[0100] 스마트라이트 영역 보호 프로토콜에 따라서, 수퍼암호화된 제어 단어(CW)를 포함한 제어 메시지(LECM)는 이들 제어 메시지(LECM) 및, 부여된 디지털 메시지를 수신하는 임의 장치를 가리키며, 디지털 데이터는 DVD를 판독하는 동안에만 프리젠테이션될 수 있고 복제 또는 재생될 수 없다.

[0101] 단계(120) 동안에, 칩 카드의 프로세서(56)는 제어 메시지(LECM) 및 발생된 제어 단어(CW)를 드라이브(40)로 전송한다.

[0102] 단계(122) 동안에, 드라이브의 스크램블링/디스크램블링 모듈(50)이 단계(112) 동안에 얻은 키(DK)를 이용하여

DVD의 영역(36)에 기록된 디지털 데이터를 디스크램블한다.

[0103] 단계(124) 동안에, 드라이브의 스크램블링/디스크램블링 모듈(50)은 칩 카드의 프로세서(56)에 의해 생성된 제어 단어(CW)를 사용하여, 단계(122) 동안에 디스크램블된 디지털 데이터를 스크램블한다.

[0104] 단계(126) 동안에, 드라이브(40)는 제어 단어(CW)를 사용하여 스크램블된 디지털 데이터 및, 프로세서(56)에 의해 생성된 제어 메시지(LECM)를 분산망(54)을 통하여 프리젠테이션 장치(60)로 전송한다.

[0105] 단계(128) 동안에, 장치가 네트워크(54)를 통하여 전송된 비디오를 디스플레이하도록, 프리젠테이션 장치(60)에 연결된 칩 카드의 프로세서(57)는 제어 메시지(LECM)를 복호화하고, 디스크램블링 모듈(66)은 수신한 디지털 데이터를 디스크램블한다.

[0106] 따라서 드라이브(40)가 DVD(30)를 판독함과 동시에 프리젠테이션 장치(60)가 비디오 콘텐츠를 디스플레이한다.

[0107] 또한 레코더(62)는 분산망(54)을 통하여 전송되는 이 디지털 데이터를 액세스한다. 그러나 복제가 행해진다면 수퍼암호화된 제어 단어(CW)로 인하여 사용할 수 없을 것이기 때문에, 레코더(62)는 사용자의 편리성을 위하여 DVD로 이 데이터를 복제 또는 재생하는 것을 금지할 수 있다.

[0108] 이 디지털 데이터 프리젠테이션 모드는 프로토콜명 "보기 전용(view only)"으로서 스마트라이트 프로토콜에 알려져 있으며, 특히 문서"SmartRight Technical white paper, Version 1.7, January 2003, Thomson"에 기술되어 있다.

[0109] 식별자(IDD)가 식별자(IDL)와 동일한 경우, 칩 카드의 프로세서(56)는 단계(130) 동안에 DVD를 기록시에 구입한 사용권(US)을 분석한다.

[0110] 이들 사용권이 비디오 콘텐츠를 하나의 영역에서만 복제 또는 재생되도록 허용될 때, 단계(132) 동안에 제어 메시지(LECM)가 드라이브(40)와 동일한 영역, 즉 식별자(IDL=IDD)의 영역에 속하며 영역 키(DOK)를 포함한 설비에 의해서만 복호화될 수 있도록, 프로세서(56)는 영역 키(DOK)에 의해 암호화된 제어 단어(CW) 및 이들 제어 단어(CW)를 포함한 제어 메시지(LECM)를 생성한다.

[0111] 단계(134) 동안에, 제어 메시지(LECM) 및 제어 단어(CW)는 드라이브(40)로 전송된다.

[0112] 단계(136) 동안에, 단계(122)에서 기술한 방법과 동일한 방법에 따라서 DVD상에서 판독한 디지털 데이터를 디스크램블한다.

[0113] 단계(138) 동안에, 단계(136) 동안 디스크램블된 디지털 데이터를, 단계(132) 동안에 생성된 제어 단어(CW)에 의해 스크램블한다.

[0114] 단계(140) 동안에, 스크램블된 디지털 데이터 및 제어 메시지(LECM)를 분산망(54)을 통하여 기록할 저장 설비(64)로 전송한다.

[0115] 드라이브(40)와 동일한 영역에 속한 설비만이 제어 메시지(LECM)를 복호화할 수 있고, 설비(64)에 저장된 디지털 데이터를 재생/복제 또는 프리젠테이션할 수 있다.

[0116] 만약 단계(130) 동안에 분석된 사용권이 디지털 데이터를 자유롭게 복제/재생가능하다고 정의한다면, 칩 카드의 프로세서(56)는 암호화되지 않은 제어 단어를 포함한 제어 메시지(LECM)를 생성한다.

[0117] 그 후, 단계(134) 내지 단계(136)가 반복된다. 그러나 이 경우에 디지털 데이터를 보안 암호키로써 스크램블하지 않으므로, 임의 설비 및 심지어 식별자(IDD=IDL)의 영역에 속하지 않는 설비도 디지털 데이터를 판독, 프리젠테이션 또는 복제할 수 있다.

[0118] 단계(130) 동안에 프로세서(56)가 디지털 데이터를 재생/복제할 수 없다고 결정한다면, 수퍼암호화된 제어 단어(CW) 및 제어 메시지(LECM)를 생성하고, 단계(120) 내지 단계(128)가 반복된다. 이 경우에, 디지털 데이터는 식별자(IDL)에 의해 식별되는 영역에 속한 프리젠테이션 장치에 의해서만 여전히 프리젠테이션될 것이다.

[0119] 또한 본 발명에 따르는 방법은 문서 "xCP: eXtensible Content Protection. 2003. IBM"와 문서 "xCP Cluster Protocol, IBM Presentation to Copy Protection Technical Working Group, July 18, 2002"에 기술된 등록상표 xCP(Extensible Content Protection) 방법에 따라 보호되는 영역 보안 시스템으로 구현될 수 있다.

[0120] 이 영역 보안 방법에 따라서, 각 영역 또는 설비 그룹은 "클러스터 ID(cluster ID)"로 불리는 그룹 식별자 ID에 의해 정의된다.

[0121] 레코더는 그룹 식별자 ID를 저장하기 위한 수단을 포함하고, 영역 정보(DI)를 계산하는데 적합한 수단을 포함한다. 이 정보(DI)는 DVD의 디스크 키(DK), 그룹 식별자 ID, 그리고 복제의 허가 여부에 따라 값 0 또는 1을 취할 수 있는 복제 표시기를 포함한 연결 데이터에 해싱 함수(hashing function)를 적용함으로써 얻어진다.

[0122] 레코더는 DVD상에 영역 정보(DI)를 기록하는데 적합하다.

[0123] 기록된 DVD를 수신하는 수신 장치는 그 자신의 영역 정보(DI')를 구성함으로써 DVD가 그 영역에서 기록되었는지의 여부를 결정한다. 이를 위하여, 그 자신의 영역의 식별자를 재사용하고, 허가된 복제에 대응하는 값으로 복제 표시기를 설정하고, 그리고 DVD상에서 판독한 디스크 키(DK)를 재사용한다.

[0124] 이런 식으로 구성된 수신 장치의 영역 정보(DI')와 DVD 영역 정보(DI)가 일치한다면, 복제가 허가되고, 수신 장치는 이 영역의 xCP 프로토콜에 따라 디지털 데이터를 디스크램블한 후 스크램블한다.

[0125] 이런 식으로 구성된 수신 장치의 영역 정보(DI')와 DVD의 영역 정보(DI)가 일치하지 않는다면, 복제 동작은 금지된다.

[0126] 그 변형례로서, 이 보안 분배 방법이 CPPM(Content Protection for Prerecorded Media) 시스템, CPRM(Content Protection for Recordable Media) 시스템, 블루 레이 디스크를 위한 BDCPS 시스템(Blue ray disk copy protection system) 또는 DVD+R/DVD+RW 디스크를 위한 비디 시스템(Vidi system)에 따라서 보호되는 DVD와 사용될 수 있다.

[0127] 또한, 그 변형례로서, 레코더가 디지털 데이터 및 영역 식별자만을 DVD상에 기록하고 디지털 데이터에 부여된 사용권 또는 재생 권리는 기록하지 않을 수 있다. 이 경우에는 드라이브가 식별자를 판독시에, 칩 카드는 디스크상에 식별되는 영역에서의 복제/재생만을 허용하는 프로토콜에 따라서 제어 단어 및 제어 메시지를 생성한다. DVD가 식별자는 포함하지 않을 때, 칩 카드는 임의 설비에 의한 복제/재생을 금지하는 프로토콜에 따라서 수퍼 암호화된 제어 단어 및 제어 메시지를 생성한다. 이 경우에, 디지털 데이터는 영역에 속한 프리젠테이션 장치에 의해 여전히 프리젠테이션될 수 있다.

[0128] 또한, 그 변형례로서, 멀티미디어 콘텐츠를 나타내는 디지털 데이터 및 관련 사용권을 포함한 형태로 DVD를 사전기록하여 마케팅한다. 이 DVD의 첫 사용전에, 설비 항목이 DVD를 판독할 수 있도록, 레코더가 속한 영역의 식별자를 기록하는데 적합한 레코더에 DVD를 위치시켜야 한다. 이 경우에, DVD가 영역 식별자를 포함할 때에만 DVD 또는 드라이브를 동작시킬 수 있도록 조절한다.

[0129] 유리하게도, 이 안전한 분배 방법은 친구 또는 지인과 디지털 데이터를 공유할 때 일정한 자유를 허용하고, 디지털 데이터에 부여된 지적 재산권을 보호하는 동안 동일한 영역에 연결된 설비와의 공유를 허용한다.

[0130] 유리하게도, 멀티미디어 콘텐츠의 복제/재생이 기록된 보안 디스크는, 멀티미디어 콘텐츠의 다운로드 버전 및 영역 식별자가 기록되었던 보안 디스크상의 기록된 식별자에 의해 정의되는 영역에서 판독 및 프리젠테이션될 수 있다. 그러나 후자인 보안 디스크, 즉 멀티미디어 콘텐츠의 다운로드 버전 및 영역 식별자를 포함한 디스크는 임의 영역에서 허가된 임의 CSS 프리젠테이션 장치상에서 판독 및 프리젠테이션될 수 있다.

도면의 간단한 설명

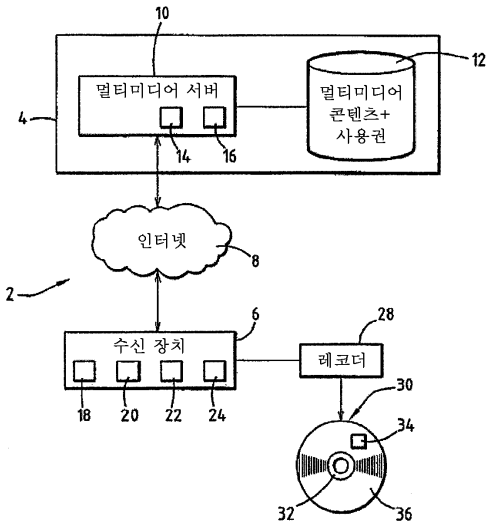
[0043] 도 1은 본 발명에 따른 분배 방법을 구현할 수 있는 시스템 일부의 기능 블록도.

[0044] 도 2는 본 발명에 따른 분배 방법을 구현할 수 있는 다른 시스템 부분의 기능 블록도.

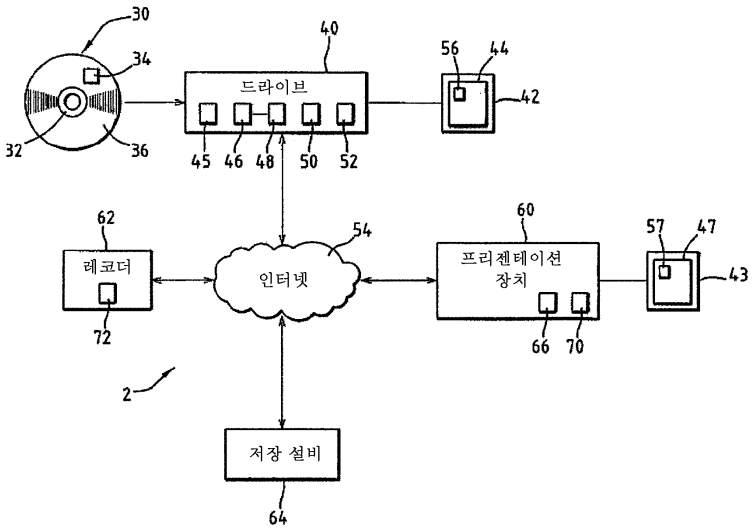
[0045] 도 3은 본 발명에 따른 분배 방법의 단계를 나타내는 도면.

도면

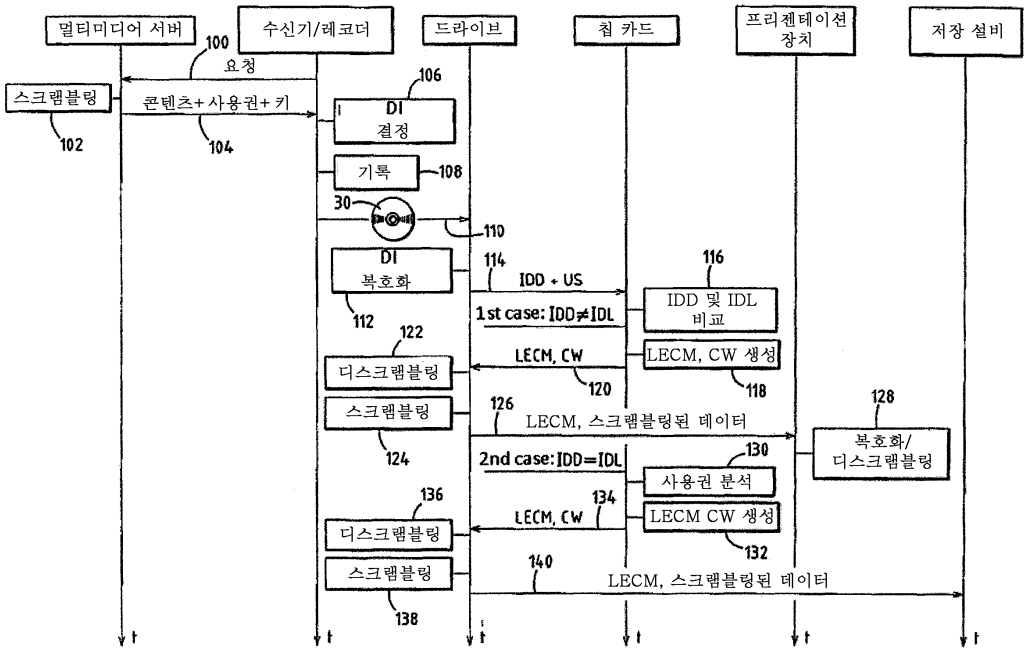
도면1


10
12
멀티미디어 서버
멀티미디어
콘텐츠+
사용권
4
14
16
인터넷
8
2
6
28
수신 장치
레코더
30
34
18
20
22
24
32
36

도면2


30
34
40
56
44
드라이브
42
32
36
45
46
48
50
52
62
60
57
47
54
레코더
인터넷
프리젠테이션
장치
43
72
66
70
2
저장 설비
64

도면3


멀티미디어 서버
수신기/레코더
드라이브
칩 카드
프리젠테이션 장치
저장 설비
100
요청
스크램블링
콘텐츠+사용권+키
102
104
106
DI 결정
기록
108
30
110
DI 복호화
112
114
IDD + US
116
IDD 및 IDL 비교
1st case: IDD≠IDL
122
디스크램블링
LECM, CW
120
LECM, CW 생성
118
스크램블링
124
126
LECM, 스크램블링된 데이터
128
복호화/ 디스크램블링
2nd case: IDD=IDL
130
사용권 분석
136
134
LECM, CW
LECM CW 생성
132
디스크램블링
스크램블링
138
140
LECM, 스크램블링된 데이터
t