(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년07월17일
(11) 등록번호 10-1420886
(24) 등록일자 2014년07월11일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *H04N 7/173* (2011.01)
G11B 20/10 (2006.01) *H04N 7/24* (2011.01)
(21) 출원번호 10-2008-7018785
(22) 출원일자(국제) 2007년01월31일
심사청구일자 2012년01월30일
(85) 번역문제출일자 2008년07월30일
(65) 공개번호 10-2008-0091785
(43) 공개일자 2008년10월14일
(86) 국제출원번호 PCT/FR2007/000179
(87) 국제공개번호 WO 2007/088273
국제공개일자 2007년08월09일
(30) 우선권주장
0600880 2006년01월31일 프랑스(FR)
(56) 선행기술조사문헌
US20050154682 A1
US20030081777 A1
전체 청구항 수 : 총 8 항

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
레리에브르, 실베인
프랑스 에프-35760 몬트거몬트 르 드 하예츠 36
코어테이, 올리버
프랑스 에프-35000 렌 르 뒤 니베르네 19
오노, 스테판
프랑스 에프-35760 세인트 그레그와르 알레 클로드 드뷔시 6
(74) 대리인
백만기, 전경석, 양영준

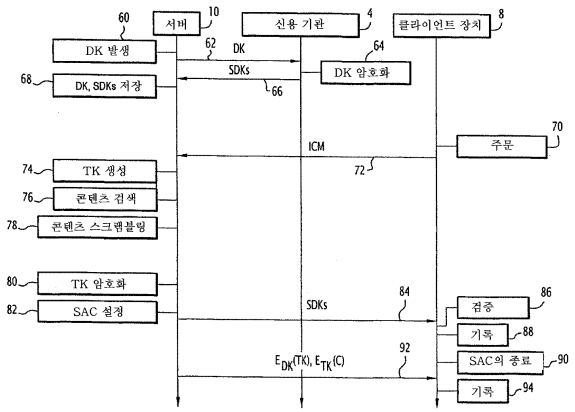
심사관 : 김동성

(54) 발명의 명칭 **디지털 데이터를 기록 및 분배하는 방법 및 관련 장치**

(57) 요 약

본 발명은 클라이언트 장치에 의해 블랭크 디스크 상에 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)를 기록하는 방법에 관한 것이다. 디지털 데이터는 원격 콘텐츠 서버에 의해 클라이언트 장치로 전송된다. 이 방법은 클라이언트 장치에서 수행되는, 콘텐츠 서버와의 보안 인증 채널(SAC)을 설정하는 단계(82); 콘텐츠 서버에 의해 전송된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)를 수신하는 단계(84); 보안 인증 채널(SAC)의 존재를 검증하여(86) 보안 인증 채널(SAC)이 있는 동안 배타적으로 위의 수신된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 기록을 허가하는 단계; 및 블랭크 디스크 상에 위의 수신된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)를 기록하는 단계(88)를 포함한다. 본 발명은 또한 클라이언트 장치 및 디지털 데이터를 분배하는 방법에 관한 것이다.

대 표 도



특허청구의 범위

청구항 1

클라이언트 장치(8)를 통해 블랭크 리드인(blank lead-in) 영역(26) 및 블랭크 데이터 존((blank data zone)(28)을 갖는 디스크(24) 상에 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)를 기록(burning)하는 방법으로서 - 상기 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)는 분배 네트워크(12)를 통해 원격 콘텐츠 서버(10)에 의해 상기 클라이언트 장치(8)에 전송되고, 상기 클라이언트 장치(8)는 네트워크 인터페이스(30), 버너(36), 및 적어도 하나의 콘텐츠 서버(10)와의 보안 인증 채널(SAC)을 설정하며 상기 버너(36)를 제어하는 수단(34)을 포함함 - ,

상기 클라이언트 장치(8)에 의해 수행되는,

- 상기 콘텐츠 서버(10)와의 보안 인증 채널(SAC)을 설정하는 단계(82);

- 상기 보안 인증 채널(SAC)을 통해 상기 콘텐츠 서버(10)에 의해 전송된 상기 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 적어도 일 부분을 수신하는 단계(84) - 상기 수신된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 일 부분은 제1 암호화 데이터 아이템(SDK_S)을 포함함 - ;

- 상기 콘텐츠 서버(10)와의 보안 인증 채널(SAC)의 존재를 검증하여(86), 상기 보안 인증 채널(SAC)이 있는 동안만 수신된 제1 암호화 데이터 아이템(SDK_S)에 대해 상기 디스크(24)의 상기 블랭크 리드인 영역(26) 상에 기록을 허가하는 단계; 및

- 상기 디스크(24)의 상기 블랭크 리드인 영역(26) 상에 상기 수신된 제1 암호화 데이터 아이템(SDK_S)을 기록하는 단계(88)

를 포함하는 디지털 데이터 기록 방법.

청구항 2

제1항에 있어서,

- 상기 콘텐츠 서버(10)에 의해 전송된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 다른 부분을 수신하는 단계(92) - 상기 디지털 데이터의 다른 부분은 스크램블된(scrambled) 콘텐츠($E_{TK}(C)$) 및 제2 암호화 데이터 아이템($E_{DK}(TK)$)을 포함함 - ; 및

- 상기 디스크(24)의 데이터 존(28)에 상기 스크램블된 콘텐츠($E_{TK}(C)$) 및 상기 제2 암호화 데이터 아이템($E_{DK}(TK)$)을 기록하는 단계(94)

를 더 포함하는 디지털 데이터 기록 방법.

청구항 3

제1항에 있어서,

상기 제1 암호화 데이터 아이템(SDK_S)을 기록하는 단계(88) 직후 보안 인증 채널(SAC)을 종료하는 단계(90)를 포함하는 디지털 데이터 기록 방법.

청구항 4

제2항에 있어서,

상기 제1 암호화 데이터 아이템(SDK_S)은 복수의 키들(MK)에 의한 제1 암호화 키(DK)의 암호화들의 결과들을 포함하는 세트이고, 상기 제1 암호화 키(DK)는 상기 제2 암호화 데이터 아이템($E_{DK}(TK)$)을 데이터 해독하는데 필요한 것인 디지털 데이터 기록 방법.

청구항 5

제4항에 있어서,

상기 제2 암호화 데이터 아이템은 상기 제1 암호화 키(DK)에 의해 암호화된 하나 이상의 제2 암호화 키들($E_{DK}(TK)$)이고, 상기 하나 이상의 제2 암호화 키들($E_{DK}(TK)$) 각각은 상기 스크램블된 콘텐츠($E_{TK}(C)$)를 디스크램블하는데 필요한 것인 디지털 데이터 기록 방법.

청구항 6

제5항에 있어서,

상기 제1 암호화 키는 디스크 키(DK)이고, 상기 하나 이상의 제2 암호화 키들($E_{DK}(TK)$) 각각은 CSS 프로토콜에서 정의된 타이틀 키(TK)인 디지털 데이터 기록 방법.

청구항 7

분배 네트워크(12)를 통해 적어도 하나의 클라이언트 장치(8)에 원격 콘텐츠 서버(10)를 통해 디지털 데이터를 분배하는 방법으로서 - 상기 원격 콘텐츠 서버(10)는 네트워크 인터페이스(40), 적어도 하나의 난수 발생기(44, 48), 스크램블링 모듈(50), 암호화 모듈(52), 보안 인증 채널(SAC)을 설정하는 모듈(54)을 포함하고, 상기 클라이언트 장치(8)는 네트워크 인터페이스(30), 유저 인터페이스(32), 버너(36), 및 보안 인증 채널(SAC)을 설정하며 상기 버너(36)를 제어하는 수단(34)을 포함하고, 상기 디지털 데이터는, 블랭크 리드인 영역(26) 및 블랭크 데이터 존(28)을 갖는 디스크(24) 상에 상기 클라이언트 장치(8)에 의해 기록되도록 설계됨 - ,

상기 클라이언트 장치(8)에 의해 상기 디스크(24) 상에 기록되도록 의도된 콘텐츠($E_{TK}(C)$)를 나타내는 데이터를 상기 콘텐츠 서버(10)로부터 주문(ordering)하는 단계, 및 제1항 내지 제6항 중 어느 한 항의 기록 방법의 단계들

을 포함하는 디지털 데이터 분배 방법.

청구항 8

블랭크 리드인 영역(26) 및 블랭크 데이터 존(28)을 갖는 디스크(24) 상에 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)를 기록하는 클라이언트 장치(8)로서 - 상기 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)는 분배 네트워크(12)를 통해 원격 콘텐츠 서버(10)에 의해 상기 클라이언트 장치(8)에 전송됨 - ,

- 상기 콘텐츠 서버(10)와의 보안 인증 채널(SAC)을 설정하는 수단(34);

- 상기 보안 인증 채널(SAC)을 통해 상기 콘텐츠 서버(10)에 의해 전송된 상기 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 적어도 일 부분을 수신하는 네트워크 인터페이스(30) - 상기 수신된 디지털 데이터($E_{TK}(C)$, SDK_S, $E_{DK}(TK)$)의 일 부분은 제 1 암호화 데이터 아이템(SDK_S)을 포함하고, 상기 설정하는 수단(34)은 또한 상기 보안 인증 채널(SAC)의 존재를 검사하여, 상기 보안 인증 채널(SAC)이 있는 동안만 수신된 제1 암호화 데이터 아이템(SDK_S)에 대해 상기 디스크(24)의 상기 블랭크 리드인 영역(26) 상에 기록을 허가함 - ; 및

- 상기 디스크(24)의 블랭크 리드인 영역(26) 상에 상기 수신된 제1 암호화 데이터 아이템(SDK_S)을 기록하는 버너(36)

를 포함하는 클라이언트 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 블랭크 디스크 상에 디지털 데이터를 기록(burning)하는데 적합한 기록 방법 및 클라이언트 장치에 관한 것으로, 디지털 데이터는 불법적인 복제로부터 보호되도록 기록된다.

[0002] 특히, 본 발명은 클라이언트 장치에 의해 블랭크 리드인(lead-in) 영역 및 블랭크 데이터 존을 갖는 디스크 상

에 디지털 데이터를 기록하는 방법에 관한 것으로, 디지털 데이터는 분배 네트워크를 통해 원격 콘텐츠 서버에 의해 클라이언트 장치로 전송되고, 클라이언트 장치는 네트워크 인터페이스, 적어도 하나의 콘텐츠 서버와의 보안 인증 채널(secure authenticated channel)을 설정하는 수단, 버너 및 버너를 제어하는 수단을 포함한다.

[0003] 본 발명은 또한 블랭크 디스크 상에 기록되도록 설계된 디지털 데이터를 분배하는 방법에 관한 것이다.

배 경 기 술

[0004] 멀티미디어 또는 소프트웨어 콘텐츠를 디스크 상에 기록하는 방법은 특히 문헌 US 2005-0154682를 통해 알려져 있다. 디스크는 블랭크 데이터 존 및 디스크 키들로 사전기록된 리드인 영역을 갖는다. 이 방법은 원격 서버로부터 스크램블된 디지털 데이터 및 디지털 데이터를 스크램블하는데 사용된 타이틀 키들을 주문할 수 있는 버너를 이용한다. 최종으로, 버너는 디스크 키들로 타이틀 키들을 암호화하고, 스크램블된 디지털 데이터와 암호화된 타이틀 키들을 디스크의 데이터 존에 기록하는데 적합하다.

[0005] 그러나 이 기록 방법은 디스크 키들로 디스크의 리드인 영역을 사전기록하여 다운로드된 콘텐츠가 CSS 등의 데이터 보호 시스템과 부합하도록 복제불가능한 방식으로 기록될 수 있도록 할 필요가 있다.

발명의 상세한 설명

[0006] 본 발명의 목적은 멀티미디어 및 소프트웨어 콘텐츠 소유자의 권리를 보다 잘 보호하는 다른 기록 방법을 제공하는 데 있다.

[0007] 따라서 본 발명의 주제는 전술한 타입의 기록 방법으로서, 클라이언트 장치에 의해 수행되는 다음 단계:

[0008] - 콘텐츠 서버와의 보안 인증 채널을 설정하는 단계;

[0009] - 보안 인증 채널을 통해 콘텐츠 서버에 의해 전송된 디지털 데이터의 적어도 일 부분을 수신하는 단계를 포함하는데, 수신된 디지털 데이터의 일 부분은 제 1 암호화 데이터 아이템을 포함하고;

[0010] - 콘텐츠 서버와의 보안 인증 채널의 존재를 검증하여 보안 인증 채널이 있는 동안만 수신된 제1 암호화 데이터 아이템에 대해 디스크의 블랭크 리드인 영역 상에 기록을 허가하는 단계; 및

[0011] - 디스크의 블랭크 리드인 영역 상에 위의 수신된 제1 암호화 데이터 아이템을 기록하는 단계를 포함하는 것을 특징으로 한다.

[0012] 특정 실시예들에 따르면, 기록 방법은 다음 특징들 중 하나 이상을 포함하고:

[0013] - 이 방법은 또한 다음 단계:

[0014] - 서버에 의해 전송된 디지털 데이터의 다른 부분을 수신하는 단계를 포함하는데, 디지털 데이터의 다른 부분은 스크램블된 콘텐츠 및 제2 암호화 데이터 아이템을 포함하고; 그리고

[0015] - 디스크의 데이터 존 상에 스크램블된 콘텐츠 및 제2 암호화 데이터를 기록하는 단계를 포함하고;

[0016] - 이 방법은 또한 제1 암호화 데이터 아이템을 기록한 직후 보안 인증 채널을 종료하는 단계를 포함하고;

[0017] - 제1 암호화 데이터 아이템은 복수의 키들에 의한 제1 암호화 키의 암호화 결과를 포함하는 세트이고, 제1 암호화 데이터 아이템은 콘텐츠를 디스크램블(descramble)하는데 필요하고;

[0018] - 제2 암호화 데이터 아이템은 제1 암호화 데이터로 암호화된 하나 이상의 제2 암호화 키들이고, 각각의 제2 암호화 키는 콘텐츠를 디스크램블하는데 필요하고;

[0019] - 제1 암호화 키는 디스크 키이고, 상기 각각의 제2 암호화 키는 CSS 프로토콜 의미 내의 타이틀 키이다.

[0020] 본 발명의 다른 주제는 분배 네트워크를 통해 적어도 하나의 클라이언트 장치에 원격 콘텐츠 서버를 통해 디지털 데이터를 분배하는 방법이고, 원격 콘텐츠 서버는 네트워크 인터페이스, 적어도 하나의 난수 발생기(random number benerator), 스크램블링 모듈, 암호화 모듈, 보안 인증 채널을 설정하는 모듈을 포함하고, 클라이언트 장치는 네트워크 인터페이스, 유저 인터페이스, 보안 인증 채널을 설정하는 수단, 버너 및 버너를 제어하는 수단을 포함하고, 디지털 데이터는, 블랭크 리드인 영역 및 블랭크 데이터 존을 갖는 디스크 상에서 클라이언트 장치에 의해 기록되도록 설계되며, 이 방법은 클라이언트 장치에 의해 디스크 상에 기록되도록 의도된 콘텐츠를 나타내는 데이터를 콘텐츠 서버로부터 주문하는 단계, 및 전술한 기록 방법의 단계들을 포함하는 것을 특징으로

한다.

[0021] 최종으로, 본 발명의 다른 주제는 블랭크 리드인 영역 및 블랭크 데이터 존을 갖는 디스크 상에 디지털 데이터를 기록하는데 적합한 클라이언트 장치이고, 디지털 데이터는 분배 네트워크를 통해 원격 콘텐츠 서버에 의해 클라이언트 장치에 전송되며, 이 장치는,

[0022] - 콘텐츠 서버와의 보안 인증 채널을 설정하는 수단;

[0023] - 보안 인증 채널을 통해 콘텐츠 서버에 의해 전송된 디지털 데이터의 적어도 일 부분을 수신하는 네트워크 인터페이스를 포함하는데, 수신된 디지털 데이터의 일 부분은 제 1 암호화 데이터 아이템을 포함하며;

[0024] - 보안 인증 채널의 존재를 검사하여 보안 인증 채널이 있는 동안만 수신된 제1 암호화 데이터 아이템에 대해 디스크의 블랭크 리드인 영역 상에 기록을 허가하는 명령 수단; 및

[0025] - 디스크의 블랭크 리드인 영역 상에 위의 수신된 제1 암호화 데이터 아이템을 기록하는데 적합한 버너를 포함하는 것을 특징으로 한다.

[0026] 본 발명은 예로서만 주어지고 도면을 참조로 하는 이하의 설명을 숙지하면 잘 이해될 것이다.

실 시 예

[0029] 본 발명에 따른 방법들을 적용한 시스템(2)을 도 1에 개략적으로 도시한다.

[0030] 이 시스템(2)은 신용 기관(4), 콘텐츠 제공자(6) 및 클라이언트 장치(8)를 포함하는데, 그 각각은 예를 들어, 인터넷 망 등의 분배 네트워크(12)를 통해 원격 콘텐츠 서버(10)와 데이터를 상호교환하는데 적합하다.

[0031] 종래의 방식에서, 신용 기관(4)은 한 세트의 마스터 키들(MK)을 저장하는 보안 메모리(14), 보안 메모리(14)에 접속된 암호화 모듈(16) 및 네트워크 인터페이스(18)를 포함한다.

[0032] 암호화 모듈(16)은 한 세트의 보안 디스크 키들(SDK_S)을 생성하도록 메모리(14) 내에 저장된 한 세트의 마스터 키들(MK)을 통해 디스크 키(DK)를 암호화하는데 적합하다.

[0033] 보안 디스크 키들(SDK_S)의 각 세트는 콘텐츠 서버(10)에 의해 전송된 특정 디스크 키(DK)를 기반으로 생성되고, 이 특정 디스크 키와 관련되는데, 이하 설명한다.

[0034] 네트워크 인터페이스(18)는 콘텐츠 서버(10)로부터 디스크 키들(DK)을 수신하고, 이 서버에 네트워크 예를 들어, 보안 인증 채널(SAC)을 통해 보안 디스크 키(SDK_S)의 세트들을 전송하는데 적합하다.

[0035] 콘텐츠 서버(6)는 디지털 데이터를 저장하는 데이터베이스(20) 및 네트워크(12) 예를 들어, 보안 인증 채널(SAC)을 통해 콘텐츠 서버(10)에 디지털 데이터의 전송을 허가하는 네트워크 인터페이스(22)를 포함한다.

[0036] 디지털 데이터는 멀티미디어 또는 소프트웨어 콘텐츠를 나타낸다. 이들은 예를 들어, 소프트웨어의 응용에 사용된 오디오, 비디오, 텍스트 데이터 또는 컴퓨터 데이터 파일들의 시퀀스이다. 이들 데이터는 저작권으로 보호되므로 기록 후에 복제나 재생될 수 없다.

[0037] 바람직하게, 디지털 데이터는 압축 형태로 베이스(20)에 저장되어 있다.

[0038] 클라이언트 장치(8)는 보통 블랭크 디스크(24) 상에 멀티미디어 또는 소프트웨어 콘텐츠를 나타내는 디지털 데이터를 다운로드하여 블랭크 디스크(24) 상에 기록을 원하는 유저에 위치한다.

[0039] 블랭크 디스크(24)는 종래의 버너로 판독될 수 있고 기록될 수 없는 리드인 영역(26) 및 종래의 버너로 판독 및 기록될 수 있는 데이터 존(28)을 포함하는 DVD 디스크이다.

[0040] 클라이언트 장치(8)는 예를 들어, 특정 타입의 버너에 접속된 컴퓨터로 구성된다.

[0041] 클라이언트 장치는 콘텐츠 서버(10)로부터 디지털 데이터를 주문하도록 키보드 및/또는 스크린 및/또는 원격 제어 타입의 유저 인터페이스(32)에 접속된 네트워크 인터페이스(30)를 포함한다.

[0042] 클라이언트 장치(8)는 또한 한편으로 네트워크 인터페이스(30)에 접속되고, 다른 한편으로 디지털 데이터 기록 모듈(36)에 접속된 중앙 처리 장치(34)를 포함한다.

[0043] 중앙 처리 장치(34)는 분배 네트워크(12)를 통해 콘텐츠 서버(10)와의 보안 인증 채널(SAC)을 설정하는데 적합

하다.

[0044] 이 목적을 위해, 각각의 SAC 채널이 설정될 때, 중앙 처리 장치(34)는 콘텐츠 서버(10)와 상호교환된 암호 데이터를 기반으로 세션 키(KS)를 연산하는데 적합하다. 이 세션 키(KS)는 서버(10)와 상호교환된 데이터를 보호하는데 사용된다.

[0045] 보안 인증 채널(SAC)을 설정하기 위한 프로토콜은 예를 들어, SSL(Secure Sockets Layer) 프로토콜 등의 표준 프로토콜 또는 등록 상표 "스마트 라이트(Smart Right)"를 갖는 보호 시스템의 규격에 기술된 프로토콜 등의 독점 프로토콜이며, 이 프로토콜은 또한 2004년 10월 29일자 출원된 미국 특허출원 제10/978162호에 기술되어 있다.

[0046] 한편으로 보안 인증 채널을 설정함으로써 클라이언트 장치(8)가 인식된 합법적인 콘텐츠 서버(10)와 데이터를 교환하는 것이 보장되고, 다른 한편으로 콘텐츠 서버(10)에 의해 클라이언트 장치(8)가 인식된 합법적인 장치여서 디지털 데이터를 블랭크 디스크 상에 기록하는 동작중 디지털 데이터의 고 수준의 보호를 제공하는 것이 보장된다.

[0047] 동시에, SAC 채널은 상호교환된 데이터를 임의의 인터셉션으로부터 보호하고, 해적 장치(pirate device)에 의한 디코딩으로부터 보호한다.

[0048] 중앙 처리 장치(34)는 보안 인증 채널(SAC)의 설정이 있는지 여부에 따라 블랭크 디스크(24) 상에 디지털 데이터의 기록을 허가 또는 금지하도록 기록 모듈(36)을 제어할 수 있다.

[0049] 기술한 실시예에 따르면, 데이터는 보안 인증 채널(SAC)의 설정이 있은 후 보안 인증 채널이 유효하게 설정된 경우에만 블랭크 디스크의 리드인 영역(26)에 기록될 수 있다.

[0050] 이 실시예에 따르면, 블랭크 디스크(24)의 데이터 존(28)에의 데이터의 기록은 보안 인증 채널의 설정이 없는 경우에도 허가된다.

[0051] 기록 모듈(36)은 블랭크 디스크(24)의 리드인 영역(26) 및 데이터 존(28) 모두에의 데이터 기록에 적합하다.

[0052] 콘텐츠 서버(10)는 콘텐츠 베이스(38), 네트워크 인터페이스(40) 및 프로세서(42)를 구비하여 클라이언트 장치가 주문한 디지털 데이터를 클라이언트 장치(8)에 제공한다.

[0053] 콘텐츠 베이스(38)는 멀티미디어 또는 소프트웨어 콘텐츠를 나타내는 디지털 데이터를 저장할 수 있다.

[0054] 프로세서(42)는 콘텐츠 베이스(38)의 아이디(ICM)를 기반으로 콘텐츠 베이스(38)로부터 디지털 데이터를 페칭할 수 있는데, 이하 기술하는 바와 같다.

[0055] 콘텐츠 베이스(38)가 요구된 디지털 데이터를 포함하지 않는 경우, 프로세서(42)는 이들 데이터에 대한 요구를 콘텐츠 제공자(6)로 전송하고, 이 제공자는 분배 네트워크(12) 예를 들어, 보안 인증 채널(SAC)을 통해 요구한 데이터를 전송하여 이들 데이터가 콘텐츠 베이스(38)에 저장된다.

[0056] 기술한 실시예에서, 콘텐츠 서버(10)는 DVB CSS("Digital Video Broadcasting Content Scrambling System;디지털 비디오 방송 콘텐츠 스크램블링 시스템") 표준에 따라 디지털 데이터를 스크램블링할 수 있다.

[0057] 이 표준에 따라 디지털 데이터를 스크램블하기 위해, 콘텐츠 서버(10)는 또한 암호화 데이터베이스(46) 및 네트워크 인터페이스(40)에 접속된 제1 발생기(44)를 포함한다.

[0058] 제1 발생기(44)는 디스크 키들(DK)을 구성하는데 적합한 난수를 발생해서 이 디스크 키들을 한편으로 인터페이스(40) 및 네트워크(12)를 통해 신용 기관(4)에 전송하고, 다른 한편으로 암호화 데이터베이스(46)에 전송할 수 있다.

[0059] 암호화 데이터베이스(46)는 디스크 키들(DK) 및 보안 디스크 키들(SDK_S)의 세트들을 저장하는데 적합한 매핑 테이블을 포함하고, 보안 디스크 키 각각은 하나의 디스크 키(DK)에 대응하고, 신용 기관(4)에 의한 디스크 키의 암호화에 의해 획득된다.

[0060] 콘텐츠 서버(10)는 또한 스크램블링 모듈(50) 및 암호화 모듈(52)에 접속된 제2 발생기(48)를 포함한다.

[0061] 제2 발생기(48)는 타이틀 키들(TK)을 구성하는데 적합한 난수를 발생할 수 있다.

[0062] 스크램블링 모듈(50)은 콘텐츠 베이스(38) 및 네트워크 인터페이스(40)에 접속되어 발생기(48)로부터 발생하는 타이틀 키들(TK)에 의해 베이스(38)로부터 발생하는 디지털 데이터를 스크램블하고, 스크램블된 디지털 데이터

($E_{TK}(C)$)를 클라이언트 장치(8)에 전송한다.

[0063] 암호화 모듈(52)은 암호화 데이터베이스(46) 및 네트워크 인터페이스(40)에 접속되어 있다. 암호화 모듈은 디스크 키(DK)에 의해 타이틀 키들(TK)을 암호화할 수 있고, 또한 이 암호화된 타이틀 키들($E_{DK}(TK)$)을 클라이언트 장치(8)에 전송할 수 있다.

[0064] 콘텐츠 서버(10)는 또한 클라이언트 장치(8)와의 보안 인증 채널(SAC)을 설정하거나 삭제하는데 적합한 제어 모듈(54)을 포함한다.

[0065] 제어 모듈(54)은 각각의 보안 인증 채널(SAC)의 설정 동안 클라이언트 장치(8)와 상호교환한 암호화 데이터로 새로운 세션 키(KS)를 구성할 수 있다.

[0066] 이 세션 키(KS)는 클라이언트 장치(8)와 상호교환된 데이터를 보호하도록 제어 모듈(54)에 의해 사용된다. 이 세션 키(KS)는 장치(8)에 의해 연산된 세션 키와 동일하다.

[0067] 제어 모듈(54)은 또한 타이틀 키들(TK)을 암호화하는데 사용되었던 디스크 키(DK)와 관련된 모든 보안 디스크 키들(SDK_S)을 암호화 데이터베이스(46)로부터 페치하고, 보안 인증 채널(SAC)이 설정되었을 때 클라이언트 장치에 이 키들을 전송하는데 적합하다.

[0068] 본 발명에 따른 방법의 단계들은 3개의 시간축(t)과, 콘텐츠 서버(10), 신용 기관(4) 및 클라이언트 장치(8)와 이들 장치 아이템들에 의해 수행된 처리 단계들 사이의 교환을 도시하는 화살표로 도시된다.

[0069] 이하 기술하는 단계들(60 내지 68)은 유저에 의한 멀티미디어 또는 소프트웨어 콘텐츠의 임의의 주문 이전에 수행된다.

[0070] 시작 단계(60)에서, 콘텐츠 서버(10)의 제1 난수 발생기(44)는 디스크 키들(DK)을 생성한다.

[0071] 단계 62에서, 생성된 디스크 키들(DK)은 네트워크(12) 예를 들어, 보안 인증 채널(SAC)을 통해 신용 기관의 암호화 모듈(16)에 전송된다.

[0072] 또한, 제1 발생기(44)에 의해 생성된 동일 디스크 키들(DK)이 암호화 데이터베이스(46)에 전송된다.

[0073] 단계 64에서, 암호화 모듈(16)은 메모리(14)에 저장된 마스터 키들(MK)에 의해 수신된 디스크 키들(DK)를 암호화하여 보안 디스크 키들(SDK_S)의 세트들을 생성한다.

[0074] 단계 66에서, 보안 디스크 키들(SDK_S)의 세트들은 암호화 모듈(16)로부터 콘텐츠 서버의 암호화 데이터베이스(46)에 전송된다.

[0075] 단계 68에서, 보안 디스크 키들(SDK_S)의 세트들은 보안 디스크 키들(SDK_S)의 각 소정의 세트가 보안 디스크 키들(SDK_S)의 세트를 생성하는데 사용된 디스크 키(DK)와 관련되도록 매핑 테이블 내의 암호화 데이터베이스(46)에 저장된다.

[0076] 단계 70에서, 블랭크 디스크(24) 상에 기록될 멀티미디어 또는 소프트웨어 콘텐츠의 구매를 바라는 유저는 클라이언트 장치의 유저 인터페이스(32)를 통해 콘텐츠 서버(10)에 접속되고, 유저 선택의 멀티미디어 또는 소프트웨어 콘텐츠를 검색한다.

[0077] 유저가 구매를 원하는 콘텐츠 예를 들어, 비디오 콘텐츠를 찾은 경우, 그는 이 비디오 콘텐츠의 아이디(ICM)를 포함하는 주문을 생성한다.

[0078] 단계 72에서, 클라이언트에 의해 생성된 주문은 클라이언트 장치(8)로부터 네트워크(12)를 통해 콘텐츠 서버(10)로 전송된다.

[0079] 다음 단계 74에서, 콘텐츠 서버(10)의 제2 콘텐츠 발생기(48)는 유저가 주문한 비디오 콘텐츠를 스크램블하는데 사용되는 타이틀 키들(TK)을 생성한다.

[0080] 단계 76에서, 프로세서(42)는 아이디(ICM)에 의해 주문한 비디오 콘텐츠를 콘텐츠 베이스(38)에서 검색한다.

[0081] 단계 78에서, 스크램블링 모듈(50)은 콘텐츠 베이스(38)에서 찾은(76) 비디오 콘텐츠를 검색하여, 제2 발생기(48)에 의해 생성된 타이틀 키들(TK)에 의해 그 비디오 콘텐츠를 스크램블한다.

[0082] 단계 80에서, 암호화 모듈(52)은 암호화 데이터베이스(46)로부터 발생하는 특정 디스크 키(DK)에 의해 타이틀 키들(TK)을 암호화한다.

[0083] 단계 82에서, 제어 모듈(54)은 클라이언트 장치(8)를 인증한다. 클라이언트 장치의 중앙 처리 장치(34)는 클라이언트 장치(8)와 콘텐츠 서버(10) 사이에 보안 인증 채널(SAC)을 설정하도록 콘텐츠 서버(10)를 인증한다. 이 단계에서, 클라이언트 장치의 중앙 처리 장치(34)와 콘텐츠 서버의 제어 모듈(54)은 각기 동시에 세션 키(KS)를 연산한다. 이 세션 키(KS)는 전송될 데이터를 암호화하여 이들 데이터를 보안 인증 채널에서 전송하도록 모듈(54)에 의해 사용되게 된다. 동일한 세션 키가 중앙 처리 장치(34)에 의해 사용되어 서버(10)가 전송한 수신 데이터를 해독한다.

[0084] 단계 84에서, 콘텐츠 서버의 제어 모듈(54)은 단계 80에서 타이틀 키들(TK)을 암호화하는데 사용된 디스크 키(DK)에 대응하는 모든 보안 디스크 키들(SDK_S)을 암호화 데이터베이스(46)에서 검색한다.

[0085] 이어서 제어 모듈(54)은 모든 보안 인증 디스크 키들(SDK_S)을 클라이언트 장치(8)로 전송한다.

[0086] 단계 86에서, 중앙 처리 장치(34)는 보안 인증 채널이 적절하게 설정되었는지 여부를 검증하고, 보안 인증 채널이 적절하게 설정되었을 경우에만, 클라이언트 장치(8)에 의해 수신된 모든 보안 디스크 키들(SDK_S)에 대한 데이터 존(28)에의 기록을 허가한다.

[0087] 단계 88에서, 기록 모듈(36)은 모든 보안 디스크 키들(SDK_S)을 블랭크 디스크(24)의 리드인 영역(26) 상에 기록한다. 모든 보안 디스크 키들(SDK_S)은 점진적으로 또한 중앙 처리 장치(34)의 데이터 수신 동안 기록된다. 이러한 기록 동안, 중앙 처리 장치(34)는 보안 인증 채널이 적절하게 설정되었는지 여부를 계속하여 검사한다.

[0088] 단계 90에서, 클라이언트 장치의 중앙 처리 장치(34)는 보안 인증 채널(SAC)을 종료한다.

[0089] 단계 92에서, 타이틀 키들($E_{TK}(C)$)에 의해 스크램블된 비디오 콘텐츠 및 디스크 키($E_{DK}(TK)$)로 암호화된 타이틀 키들이 콘텐츠 서버(10)로부터 클라이언트 장치(8)로 전송된다.

[0090] 단계 94에서, 클라이언트 장치의 중앙 처리 장치(34)는 기록 모듈(36)이 디스크의 데이터 존(28)에 데이터를 기록하는 것을 허가한다. 스크램블된 비디오 콘텐츠($E_{TK}(C)$) 및 암호화된 타이틀 키들($E_{DK}(TK)$)이 기록 모듈(36)에 의해 데이터 존상에 기록된다. 콘텐츠 서버(10)와 클라이언트 장치(8) 사이에 보안 인증 채널(SAC)이 없더라도, 디스크의 데이터 존에 스크램블된 콘텐츠 및 암호화된 타이틀 키들을 기록할 수 있음을 일러둔다.

[0091] 한편, 보안 인증 채널이 더 이상 설정되지 않는다면, 클라이언트 장치(8)의 중앙 처리 장치(34)는 기록 모듈(36)이 디스크의 리드인 영역(26) 상에 임의의 데이터를 기록하는 것을 금지시킨다.

[0092] 변형 예로서, 클라이언트 장치(8)는 맨-머신(man-machine) 인터페이스 및 중앙 처리 장치를 구비하는 버너이다.

[0093] 변형 예로서, 클라이언트 장치는 중앙 처리 장치에 접속되어 리드인 영역에만 그리고 보안 인증 채널(SAC)이 있을 동안만 데이터를 기록할 수 있는 제1 기록 모듈 및 역시 중앙 처리 장치에 접속되어 보안 인증 채널(SAC)이 없을 경우에도 데이터 존 내에 데이터를 기록할 수 있는 제2 기록 모듈을 포함한다. 이 경우, 중앙 처리 장치는 그가 수신한 데이터의 타입에 따라 제1 또는 제2 기록 모듈에 디지털 데이터를 전송하도록 되어있다.

[0094] 변형 예로서, DVD 디스크는 DVD-R, DVD-RW, DVD+R, DVD+RW 또는 DVD-RAM 타입을 갖는다.

[0095] 위의 설명에서, 보호 시스템(CSS;Content Scrambling System)이 블랭크 디스크 상에 기록된 디지털 데이터를 보호하는데 사용된다. 변형 예로서, 예를 들어, 기록 매체 콘텐츠 보호(Content Protection for Prerecorded Media(CPPM)) 시스템, 기록가능 매체 콘텐츠 보호(Content Protection for Recordable Media(CPRM)) 시스템, 블루 레이 디스크 복사 방지 시스템(Blue-ray Disk Copy Protection System(BD-CPS)), 고밀도 디스크(HD DVD)용 어드밴스드 액세스 콘텐츠 시스템 (Advanced Access Content System(AACS)) 및 DVD+R+RW 타입 디스크용 "Vidi" 시스템 등의 다른 저장 매체 및 다른 보호 시스템이 또한 사용될 수 있다.

[0096] 바람직하게 이러한 기록 방법은 더 보안성을 갖는다.

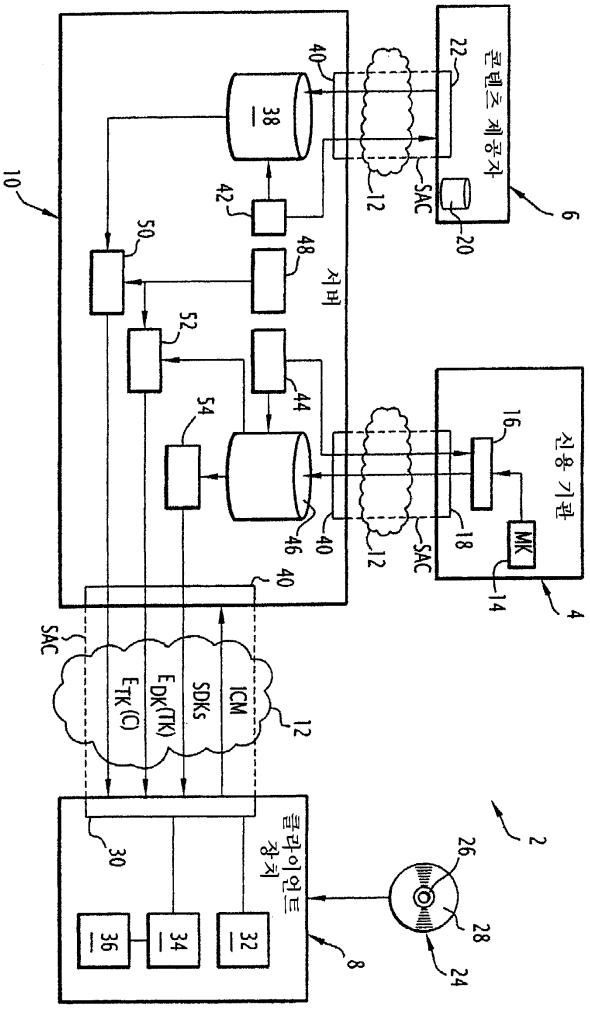
도면의 간단한 설명

[0027] 도 1은 본 발명에 따른 방법들을 적용한 시스템의 기능 블록도이다.

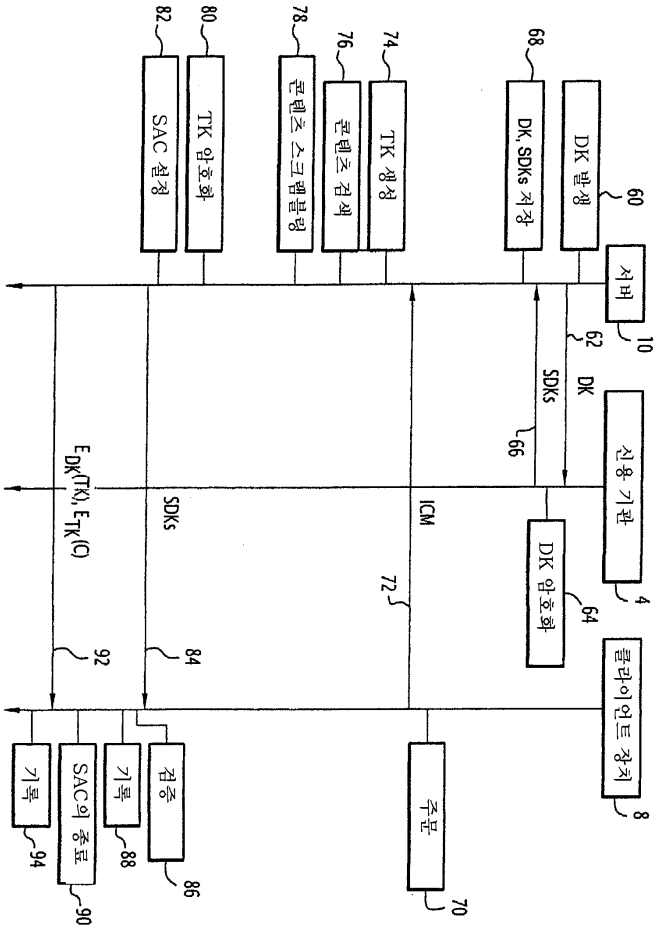
[0028] 도 2는 도 1에 도시된 장치에 의해 수행된 동작을 설명하는 도면이다.

도면

도면1



도면2


서버
10
DK 발생
60
DK, SDKs 저장
68
콘텐츠 검색
76
TK 생성
74
콘텐츠 스크램블링
78
TK 암호화
80
SAC 설정
82
DK
62
SDKs
66
신용 기관
4
DK 암호화
64
클라이언트 장치
8
ICM
72
SDKs
84
$E_{DK}(TK), E_{TK}(C)$
92
주문
70
검증
86
기록
88
SAC의 종료
90
기록
94