(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년05월25일
(11) 등록번호 10-1147763
(24) 등록일자 2012년05월14일

(51) 국제특허분류(Int. Cl.)
G11B 20/10 (2006.01)
(21) 출원번호 10-2005-0109694
(22) 출원일자 2005년11월16일
심사청구일자 2010년11월16일
(65) 공개번호 10-2006-0084351
(43) 공개일자 2006년07월24일
(30) 우선권주장
60/644,588 2005년01월19일 미국(US)
(56) 선행기술조사문헌
US20030142827 A1*
WO2004114303 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
엘지전자 주식회사
서울특별시 영등포구 여의대로 128 (여의도동)
(72) 발명자
서강수
경기도 성남시 분당구 중앙공원로 53, 시범단지 삼성아파트 107동 704호 (서현동)
(74) 대리인
김용인, 심창섭

전체 청구항 수 : 총 16 항 심사관 : 장진환

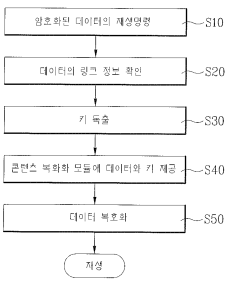
(54) 발명의 명칭 **데이터 복호방법 및 복호장치, 기록매체**

(57) 요 약

본 발명은 암호화된 데이터를 복호화하는 복호방법 및 복호장치, 암호화된 데이터가 저장된 기록매체에 관한 것으로서, 로컬 스토리지(Local storage)에 기록매체와 관련된 키(Key)로 암호화(encryption)된 데이터를 다운로드 하고, 상기 데이터와 키 사이의 링크(link)정보를 이용하여 상기 데이터의 암호화에 사용된 키를 독출하고, 상기 독출된 키를 사용하여 상기 데이터를 복호화하는 것을 특징으로 하는 데이터 복호방법 및 복호장치를 제공한다.

본 발명에 따른 데이터 복호방법 및 복호장치, 기록매체를 통해 콘텐츠의 무단 복제, 배포 등을 방지할 수 있게 됨으로써 콘텐츠 제공자는 안전하게 콘텐츠를 제공할 수 있게 되고, 사용자는 암호화된 데이터를 효율적으로 재생할 수 있게 되는 장점이 있다.

대 표 도 - 도10



특허청구의 범위

청구항 1

로딩된 기록매체와 관련된 데이터를 로컬 스토리지(Local Storage)에 다운로드 받고,

상기 기록매체에 기록된 데이터를 복호화(decryption)하는데 사용되는 제 1 복호키(Decryption key)와 상기 다운로드 된 데이터를 복호화하는데 사용되는 제 2 복호키를 포함하는 키 파일(Key file)을 상기 로컬 스토리지에 다운로드 받고,

상기 기록매체에 기록된 데이터의 재생 정보를 포함하는 제 1 플레이리스트(Playlist)와 상기 다운로드 된 데이터의 재생 정보를 포함하는 제 2 플레이리스트를 바인딩(Binding)하여, 가상 플레이리스트(Virtual playlist)를 생성하고,

상기 기록매체에 기록된 데이터 또는 상기 다운로드 된 데이터의 식별정보를 포함하는 링크정보를 이용하여, 상기 제 1 복호키와 제 2 복호키를 상기 키 파일에서 읽어, 상기 제 1 복호키를 이용하여 상기 기록매체에 기록된 데이터를 복호화하고, 상기 제 2 복호화키를 이용하여 상기 다운로드 된 데이터를 복호화하고,

상기 가상 플레이리스트를 이용하여, 상기 복호화된 기록매체에 기록된 데이터 및 다운로드 된 데이터를 재생하는 것을 특징으로 하는 데이터 재생 방법.

청구항 2

제 1 항에 있어서,

상기 다운로드 된 키 파일은,

상기 로컬 스토리지에 설정되는 보안영역(Secure area)에 저장되는 것을 특징으로 하는 데이터 재생 방법.

청구항 3

제 1 항에 있어서,

상기 링크정보는,

상기 다운로드 된 데이터의 데이터베이스(Database) 정보 내에 기록된 것을 특징으로 하는 데이터 재생 방법.

청구항 4

제 1 항에 있어서,

상기 링크정보는,

'CPS_unit_number'인 것을 특징으로 하는 데이터 재생 방법.

청구항 5

제 4 항에 있어서,

상기 'CPS_unit_number' 마다 별도의 복호키가 정의는 것을 특징으로 하는 데이터 재생 방법.

청구항 6

제 5 항에 있어서,

상기 'CPS_unit_number'는,

타이틀(Title) 단위로 부여되는 것을 특징으로 하는 데이터 재생 방법.

청구항 7

제 1 항에 있어서,

상기 다운로드된 데이터 또는 상기 기록매체에 기록된 데이터는,

타이틀(Title) 단위로 구성되는 것을 특징으로 하는 데이터 재생 방법.

청구항 8

제 7 항에 있어서,

상기 타이틀이 메인패스(Main path)와 서브패스(Sub path)로 이루어진 경우, 상기 메인패스와 서브패스는 동일한 키로 암호화되는 것을 특징으로 하는 데이터 재생 방법.

청구항 9

기록매체로부터 상기 기록매체의 데이터를 독출하는 픽업과,

상기 기록매체와 관련된 데이터와 상기 기록매체에 기록된 데이터를 복호화(decryption)하는데 사용되는 제 1 복호키(Decryption key)와 상기 기록매체와 관련된 데이터를 복호화하는데 사용되는 제 2 복호키를 포함하는 키 파일(Key file)가 다운로드 되어 저장되는 로컬 스토리지(Local storage)와,

상기 기록매체에 기록된 데이터의 재생 정보를 포함하는 제 1 플레이리스트(Playlist)와 상기 다운로드 된 데이터의 재생 정보를 포함하는 제 2 플레이리스트를 바인딩(Binding)하여, 가상 플레이리스트(Virtual playlist)를 생성하고,

상기 기록매체에 기록된 데이터 또는 상기 다운로드 된 데이터의 식별정보를 포함하는 링크정보를 이용하여, 상기 제 1 복호키와 제 2 복호키를 상기 키 파일에서 읽어, 상기 제 1 복호키를 이용하여 상기 기록매체에 기록된 데이터를 복호화하고, 상기 제 2 복호화키를 이용하여 상기 다운로드 된 데이터를 복호화하고,

상기 가상 플레이리스트를 이용하여, 상기 복호화된 기록매체에 기록된 데이터 및 다운로드 된 데이터를 재생하는 제어부를 포함하여 구성되는 것을 특징으로 하는 데이터 재생 장치.

청구항 10

제 9 항에 있어서,

상기 다운로드 된 키 파일은,

상기 로컬 스토리지에 설정되는 보안영역(Secure area)에 저장되는 것을 특징으로 하는 데이터 재생 장치.

청구항 11

제 9 항에 있어서,

상기 링크정보는,

상기 다운로드 된 데이터의 데이터베이스(Database) 정보 내에 기록된 것을 특징으로 하는 데이터 재생 장치.

청구항 12

제 9 항에 있어서,

상기 링크정보는,

'CPS_unit_number'인 것을 특징으로 하는 데이터 재생 장치.

청구항 13

제 12 항에 있어서,

상기 'CPS_unit_number' 마다 별도의 복호키가 정의는 것을 특징으로 하는 데이터 재생 장치.

청구항 14

제 13 항에 있어서,

상기 'CPS_unit_number'는,

타이틀(Title) 단위로 부여되는 것을 특징으로 하는 데이터 재생 장치.

청구항 15

제 9 항에 있어서,

상기 다운로드된 데이터 또는 상기 기록매체에 기록된 데이터는,

타이틀(Title) 단위로 구성되는 것을 특징으로 하는 데이터 재생 장치.

청구항 16

제 15 항에 있어서,

상기 타이틀이 메인패스(Main path)와 서브패스(Sub path)로 이루어진 경우, 상기 메인패스와 서브패스는 동일한 키로 암호화되는 것을 특징으로 하는 데이터 재생 장치.

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0020] 본 발명은 기록매체의 재생에 관한 것으로, 특히 암호화된 데이터를 포함하는 광 기록매체, 광 기록매체 및 로컬 스토리지에 존재하는 암호화된 데이터를 복호화하는 복호방법 및 재생장치에 관한 것이다.

[0021] 기록매체로서 대용량의 데이터를 기록할 수 있는 광 디스크가 널리 사용되고 있다. 그 중에서도 최근에는 고화질의 비디오 데이터와 고음질의 오디오 데이터를 장시간 동안 기록하여 저장할 수 있는 새로운 고밀도 기록매체, 예를 들어 블루레이 디스크(BD: Blu-ray Disc)가 개발되고 있다.

[0022] 차세대 기록매체 기술인 블루레이 디스크(BD)는 기존의 DVD를 현저하게 능가하는 데이터를 구비할 수 있는 차세대 광기록 솔루션으로 근래에 다른 디지털기기와 함께 이에 대한 개발이 진행되고 있다.

[0023] 관련하여, 블루레이 디스크(BD) 규격을 응용한 광 기록재생장치의 개발도 시작되었으나, 아직 블루레이 디스크(BD) 규격이 완전히 완비되지 못한 관계로 완성된 광 기록재생장치를 개발하는 데 어려움이 따르는 것이 사실이다.

[0024] 특히, 상기와 같은 광 기록재생장치는 블루레이 디스크(BD)를 기록재생하는 기본기능은 물론이거니와, 주변의 관련된 디지털기기와의 통합적 사용을 고려한 부가적인 기능도 고려되어야 하는바, 일반적으로 외부입력신호를 수신하고 이를 디스플레이하거나, 외부입력신호와 내장된 블루레이 디스크(BD)를 함께 활용하여 재생하는 등의 기능은 반드시 구비되어야 할 것으로 여겨진다.

[0025] 그러나, 상기와 같이 외부입력신호 및 블루레이 디스크(BD)를 재생함에 있어, 콘텐츠 제공자에 의해 제공되는

콘텐츠를 보호하기 위한 바람직한 방법 등이 알려진바 없어, 본격적인 블루레이 디스크(BD) 기반의 광 기록재생장치를 개발하는데 많은 제약이 따르는 실정이다.

발명이 이루고자 하는 기술적 과제

[0026] 본 발명은 상기와 같은 문제점을 해결하기 위한 것으로서, 외부로부터 기록매체와 관련된 데이터를 받아 저장할 수 있는 로컬 스토리지를 구비하고, 상기 로컬 스토리지와 기록매체를 이용하여 콘텐츠를 보호하는 데이터 복호방법 및 복호장치, 기록매체를 제공하고자 한다.

발명의 구성 및 작용

[0027] 상기와 같은 목적을 달성하기 위하여 본 발명은 로컬 스토리지(Local storage)에 기록매체와 관련된 암호화(encryption)된 데이터를 다운로드 하고, 상기 기록매체 내에 저장된 키(Key)를 사용하여 상기 암호화된 데이터를 복호(decryption)화하는 것을 특징으로 하는 데이터 복호방법을 제공한다.

[0028] 상기 로컬 스토리지에 다운로드 되는 데이터는 타이틀(Title) 단위로 다운로드 되는 것이 바람직하다.

[0029] 또한, 상기 키는 상기 기록매체 내에 기록된 데이터의 암호화에 사용된 키(Key)인 것이 바람직하다.

[0030] 또한, 상기 키는 다운로드 되는 데이터의 복호화를 위해 상기 기록매체 내에 별도로 저장된 키인 다운로드 되는 것이 바람직하다.

[0031] 또한, 상기 키는 유닛 키 파일(Unit Key file)로 구성되어 상기 기록매체 내에 저장된 것이 바람직하다.

[0032] 본 발명은 로컬 스토리지(Local storage)에 기록매체와 관련된 암호화(encryption)된 데이터를 다운로드 하고, 상기 기록매체에 저장된 키(Key)와는 별도로 상기 로컬 스토리지 내에 저장된 키를 사용하여, 상기 다운로드 되는 데이터를 복호화(decryption)하는 것을 특징으로 하는 데이터 복호방법을 제공한다.

[0033] 상기 로컬 스토리지 내에 저장된 키는 다운로드 된 키인 것이 바람직하다.

[0034] 관련하여, 로컬 스토리지에 저장된 키가 기록매체 외부로부터 다운로드 된 키인 경우, 상기 기록매체 내에 기록된 데이터는 기록매체 내에 저장된 키를 사용하여 복호화되는 것이 바람직하다.

[0035] 상기 로컬 스토리지에 저장된 키는 상기 기록매체 내에 저장된 키를 독출하여 저장된 키인 것이 바람직하다.

[0036] 관련하여, 로컬 스토리지에 저장된 키가 기록매체 내에 저장된 키를 독출하여 저장된 키인 경우, 기록매체 내에 기록된 데이터는 상기 로컬 스토리지에 저장된 키를 사용하여 복호화될 수도 있다.

[0037] 상기 로컬 스토리지 내에 저장된 키는 로컬 스토리지에 설정되는 보안영역(secure area)에 위치하는 것이 바람직하다.

[0038] 본 발명은 로컬 스토리지(Local storage)에 기록매체와 관련된 키(Key)로 암호화(encryption)된 데이터를 다운로드 하고, 상기 데이터와 키 사이의 링크(link)정보를 이용하여 상기 데이터의 암호화에 사용된 키를 독출하고, 상기 독출된 키를 사용하여 상기 데이터를 복호화하는 것을 특징으로 하는 데이터 복호방법을 제공한다.

[0039] 상기 데이터와 키 사이의 링크정보는 상기 다운로드 되는 데이터의 데이터베이스(database) 정보 내에 기록된 것이 바람직하다.

[0040] 또한, 상기 데이터와 키 사이의 링크정보는 로컬 스토리지에 링크정보파일로 구성되는 것이 바람직하다.

[0041] 관련하여, 상기 링크정보파일은 로컬 스토리지에 설정되는 보안영역(secure area) 내에 구성되는 것이 바람직하다.

[0042] 또한, 상기 링크정보파일은 로컬 스토리지의 AV 데이터(AV data) 기록영역 내에 구성될 수도 있다.

[0043] 상기 링크정보는 'CPS_unit_number'인 것이 바람직하다.

[0044] 관련하여, 상기 'CPS_unit_number' 마다 별도의 키(Key)가 정의되는 것이 바람직하다.

[0045] 또한, 상기 'CPS_unit_number'는 타이틀(Title) 단위로 부여될 수도 있다.

[0046] 본 발명은 콘텐츠(contents)가 기록된 스트림파일 영역과, 상기 콘텐츠의 재생을 관리하는 데이터베이스 영역(Database Area)을 구비하되, 상기 스트림파일 영역은 키(Key)로 암호화(encryption)된 복수의 타이틀(Titl

e)을 포함하고, 상기 복수의 타이틀이 서로 클립의 일부 또는 전부를 공유하는 경우, 상기 클립을 공유하는 타이틀은 동일한 키로 암호화되는 것을 특징으로 하는 기록매체를 제공한다.

[0047] 상기 키로 암호화된 타이틀이 메인패스(main path)와 서브패스(sub path)로 이루어진 경우, 상기 메인패스와 서브패스는 동일한 키로 암호화되는 것이 바람직하다.

[0048] 상기 키는 데이터베이스 영역에 유닛 키 파일(Unit Key file)로 기록되는 것이 바람직하다.

[0049] 관련하여, 상기 유닛 키 파일은 다운로드 되는 타이틀을 위한 키를 별도로 포함하는 것이 바람직하다.

[0050] 본 발명은 콘텐츠(contents)가 기록된 스트림파일 영역과, 상기 콘텐츠의 재생을 관리하는 데이터베이스 영역(Database Area)을 구비하되, 상기 스트림파일 영역은 키(Key)로 암호화(encryption)된 복수의 타이틀(Title)을 포함하고, 기록매체 외부에 존재하는 타이틀(Title)이 상기 기록매체 내의 암호화된 타이틀을 구성하는 클립의 일부 또는 전부를 공유하여 구성되는 경우, 상기 기록매체 내의 암호화된 타이틀은 동일한 키로 암호화되는 것을 특징으로 하는 기록매체를 제공한다.

[0051] 또한, 본 발명은 기록매체 내에 기록된 플레이리스트(PlayList)에 의해 재생되는 클립(Clip)의 일부 또는 전부를 포함하여 가상 플레이리스트(Virtual PlayList)를 생성함에 있어서, 상기 가상 플레이리스트의 생성에 사용되는 클립이 키(Key)로 암호화(encryption)된 경우, 상기 클립은 동일한 키로 암호화된 클립인 것을 특징으로 하는 가상 플레이리스트 생성방법을 제공한다.

[0052] 또한, 본 발명은 로컬 스토리지(Local Storage)에 기록매체의 메인패스(main path)와 관련된 서브패스(sub path) 데이터를 다운로드 하고, 상기 메인패스 데이터와 동일한 키(Key)를 사용하여 상기 서브패스 데이터를 복호화(decryption)하는 것을 특징으로 하는 데이터 복호방법을 제공한다.

[0053] 또한, 기록매체로부터 기록매체의 정보를 독출하는 픽업과, 상기 기록매체와 관련되어 다운로드 되는 암호화된 데이터가 저장되는 로컬 스토리지와, 상기 기록매체 내에 저장된 키와는 별도로 상기 기록매체 내에 저장된 키(Key)를 사용하여 상기 암호화된 데이터를 복호화(decryption)하는 제어부를 포함하는 것을 특징으로 하는 데이터 복호장치를 제공한다.

[0054] 상기 키는 상기 기록매체 내에 기록된 데이터의 암호화에 사용된 키인 것이 바람직하다.

[0055] 상기 키는 다운로드 되는 데이터의 복호화를 위해 상기 기록매체 내에 별도로 저장된 키일 수도 있다.

[0056] 본 발명은 기록매체로부터 기록매체의 정보를 독출하는 픽업과, 데이터 복호화에 사용되는 키(Key)와 상기 기록매체와 관련되어 다운로드 되는 암호화(encryption)된 데이터가 저장되는 로컬 스토리지와, 상기 로컬 스토리지 내에 저장된 키를 사용하여 상기 암호화된 데이터를 복호화(decryption)하는 제어부를 포함하는 것을 특징으로 하는 데이터 복호장치를 제공한다.

[0057] 상기 제어부는 기록매체 내에 기록된 데이터의 복호화에 기록매체 내에 저장된 키를 사용하는 것이 바람직하다.

[0058] 상기 제어부는 기록매체 내에 기록된 데이터의 복호화에 상기 로컬 스토리지 내에 저장된 키를 사용하는 것이 바람직하다.

[0059] 상기 로컬 스토리지 내에 저장된 키는 로컬 스토리지 내에 설정된 보안영역(secure area)에 위치하는 것이 바람직하다.

[0060] 본 발명은 기록매체로부터 기록매체의 정보를 독출하는 픽업과, 데이터 복호화에 사용되는 키(Key)와 상기 기록매체와 관련되어 다운로드 되는 암호화(encryption)된 데이터가 저장되는 로컬 스토리지와, 상기 암호화된 데이터와 키 사이의 링크(link)정보를 확인하고, 상기 링크정보를 사용하여 상기 데이터의 암호화에 사용된 키를 독출하고, 상기 독출된 키를 사용하여 상기 암호화된 데이터를 복호화(decryption)하는 제어부를 포함하는 것을 특징으로 하는 데이터 복호장치를 제공한다.

[0061] 상기 제어부는 상기 링크정보를 상기 다운로드 되는 데이터의 데이터베이스(database)정보에서 확인하는 것이 바람직하다.

[0062] 상기 제어부는 상기 링크정보를 로컬 스토리지에 구성되는 링크정보파일에서 확인하는 것이 바람직하다.

[0063] 상기 제어부는 상기 로컬 스토리지에 다운로드 되는 데이터가 기록매체 내에 기록된 메인패스(main path)와 관련되어 다운로드 되는 서브패스(sub path) 데이터인 경우, 상기 메인패스 데이터와 동일한 키를 사용하여

상기 서브패스 데이터를 복호화하는 것이 바람직하다.

[0064] 본 발명에 의하면, 안전한 콘텐츠의 제공과 데이터의 효율적 재생이 가능하게 되어 사용자에게 더욱 편리한 기능을 제공할 수 있게 된다.

[0065] 이하, 본 발명은 설명의 편의를 위해 기록매체로서 광 디스크(optical disc) 특히 "블루레이 디스크(BD)"를 예로 하여 설명하고자 하나, 본 발명의 기술사상은 다른 기록매체에도 동일하게 적용가능함은 자명하다 할 것이다.

[0066] 관련하여, 본 발명에서 "로컬 스토리지(Local Storage)"라 함은, 광기록재생장치(도 1) 내에 구비된 일종의 저장수단으로서, 필요한 정보 및 데이터를 사용자가 임의로 저장하여 활용할 수 있는 요소를 의미한다. 즉, 현재 일반적으로 사용되는 로컬 스토리지로는 "하드디스크(hard disk)", "시스템 메모리(system memory)", "플래쉬 메모리(flash memory)"등이 있을 수 있으나, 본 발명은 반드시 이에 한정되지는 않는다.

[0067] 특히, 본 발명과 관련하여, 상기 "로컬 스토리지(Local Storage)"는 기록매체(예를 들어, 블루레이 디스크)와 연관된 데이터를 저장하는 수단으로도 활용되며, 상기 기록매체와 연관되어 로컬 스토리지 내에 저장되는 데이터는 외부로부터 다운로드(download) 받은 데이터가 일반적이다.

[0068] 관련하여, 기록매체로부터 일부 허용된 데이터를 직접 독출하거나, 또는 기록매체의 기록재생과 관련된 시스템데이터(예를 들어, 메타데이터(metadata) 등)를 생성하여, 로컬 스토리지 내에 저장하는 것도 가능함은 자명하다.

[0069] 관련하여, 본 발명에서는 설명의 편의를 위해, 상기 기록매체 내에 기록된 데이터를 "오리지널 데이터(orginal data)"로 명명하고, 상기 로컬 스토리지 내에 저장된 데이터 중 기록매체와 관련된 데이터를 "어디셔널 데이터(additional data)"로 명명하고자 한다.

[0070] 또한, 본 발명에서 "타이틀(Title)"이라 함은, 사용자와의 인터페이스를 이루는 재생단위로서, 각각의 타이틀은 특정의 오브젝트(Object)와 링크(link)되어 있고, 상기 오브젝트(Object) 내의 컨맨드(command) 혹은 프로그램에 따라 디스크 내 기록된 해당 타이틀에 관련된 스트림이 재생된다. 특히, 본 발명에서는 설명의 편의를 위해 디스크 내에 기록된 타이틀 중 엠펙2(MPEG2) 압축방식에 의한 동영상 영화 및 인터액티브(interactive) 정보가 기록된 타이틀을 특히 "HDMV 타이틀(Title)"이라 명하고, 자바(Java) 프로그램에 의해 실행되는 동영상 영화 및 인터액티브(interactive) 정보가 기록된 타이틀을 "BD-J 타이틀(BD-J Title)"이라 명할 것이다.

[0071] 도 1은 본 발명의 개념적 이해를 돕기 위해 나타낸 것으로, 광 기록재생장치(10)와 주변기기 간의 통합적 사용의 일 예를 보여주기 위해 나타낸 것이다.

[0072] 관련하여, 본 발명의 "광 기록재생장치(10)"는 여러 가지 규격의 광 디스크를 기록하거나 재생 가능한 기기로서, 설계에 따라서는 특정규격(예를 들면, BD)의 광 디스크만을 기록재생 가능하게 할 수도 있으며, 또한 기록은 제외하고 재생만 하는 것도 가능하다 할 것이나, 특히 본 발명에서 해결하고자 하는 블루레이 디스크(BD)와 주변기기와의 연계성을 고려하여 이하 블루레이 디스크(BD)를 재생하는 플레이어(BD-Player) 또는 블루레이 디스크(BD)를 기록재생하는 리코더(BD-Recorder)를 예로 하여 설명하고자 한다. 관련하여, 본 발명의 "광 기록재생장치(10)"는 컴퓨터 등에 내장가능한 "드라이브(driver)"가 될 수 있음은 이미 널리 알려진 자명한 사실이다.

[0073] 본 발명의 광 기록재생장치(10)는 광 디스크(30)를 기록재생하는 기능 이외에도, 외부입력신호를 수신받아 이를 신호처리한 후 또 다른 외부 디스플레이(20)를 통해 사용자에게 화면으로 전달하는 기능을 가지게 된다. 이 경우 입력가능한 외부신호에 대해서는 특별한 제한은 없으나, 디지털 방송(Digital multimedia broadcasting) 및 인터넷(Internet) 등이 대표적인 외부입력신호가 될 것이며, 특히, 인터넷(Internet)의 경우 현재 누구나 손쉽게 접근할 수 있는 매체로서 광 기록재생장치(10)를 통해 인터넷(Internet)상의 특정 데이터를 다운로드(download) 받아 활용할 수 있게 된다.

[0074] 관련하여, 외부입력 소스(external source)로서 콘텐츠(content)를 제공하는 자를 총칭하여 "콘텐츠 제공자(CP:content provider)"로 명명한다.

[0075] 또한, 본 발명에서 콘텐츠(contents)라 함은 타이틀을 구성하는 내용으로서 기록매체의 제작자(author)에 의해 제공되는 데이터(data)를 의미한다.

[0076] 특히, 본 발명에서 해결하고자 하는 바는, 광 기록재생장치(10) 내의 오리지널 데이터 및/또는 인터넷과 같은 광 기록재생장치(10) 외부에 존재하는 상기 오리지널 데이터와 연관된 어디셔널 데이터가 암호화(encryptio

n)된 경우에, 상기 암호화된 데이터를 키(Key)를 이용하여 복호화(decryption)하는 경우가 된다. 상기 키(key)를 이용한 암호화(encryption) 및 복호화(decryption)에 대해서는 도 5 이하에서 후술한다.

[0077] 오리지널 데이터와 어디셔널 데이터에 대해 구체적으로 설명하면, 예를 들어 광 디스크 내에 기록된 오리지널 데이터로는 특정 타이틀용의 멀티플렉싱된(multiplexed) AV스트림을 기록해두고, 인터넷상의 어디셔널 데이터로는 상기 오리지널 데이터의 오디오스트림(예를 들어, 한국어)과 상이한 오디오스트림(예를 들어, 영어)을 제공하면, 사용자에 따라서는 인터넷상의 어디셔널 데이터인 오디오스트림(예를 들어, 영어)을 다운로드 받아, 오리지널 데이터인 AV스트림과 함께 재생하거나, 또는 어디셔널 데이터만 재생하고자 하는 요구가 존재할 것이며, 이를 가능케 하기 위해서는 상기 오리지널 데이터와 어디셔널 데이터 간의 연관성을 규정하고, 이들 데이터들을 사용자의 요구에 따라 관리/재생하는 체계화된 방법이 필요하게 된다.

[0078] 상기에서 설명의 편의를 위해 디스크 내에 기록된 신호를 오리지널 데이터로 하고, 디스크 외부에 존재하는 신호를 어디셔널 데이터라고 명명하였으나, 이는 각각의 데이터를 취득하는 방법에 따라 구분될 따름이지 오리지널 데이터와 어디셔널 데이터가 반드시 특정의 데이터로 한정되는 것은 아니라 할 것이다.

[0079] 따라서, 어디셔널 데이터로서 일반적인 것은, 오디오(Audio), 프리젠테이션 그래픽(PG:Presentation Graphic), 인터액티브 그래픽(IG:Interactive Graphic), 텍스트 서브타이틀(Text subtitle)등이 될 수 있을 것이나, 이에 한정되지 않으며 상기 열거한 데이터들과 비디오(Video)를 전부 포함하는 멀티플렉싱된(multiplexed) AV스트림이 될 수도 있다. 즉, 광 디스크 외부에 존재하면서, 오리지널 데이터와 연관된 어떠한 속성의 데이터도 어디셔널 데이터로 가능하게 된다.

[0080] 또한, 어디셔널 데이터는 인덱스 파일(index) 또는 플레이리스트 파일(*.m2ts), 클립인포 파일(*,clpi) 별로 각각 다운로드 될 수도 있으나, 콘텐츠(contents) 단위 또는 타이틀(Title) 단위로 다운로드 될 수도 있다.

[0081] 관련하여, 상기 사용자의 요구를 실현 가능케 하기 위하여는 오리지널 데이터와 어디셔널 데이터 상호 간에 연관된 파일구조를 가짐이 필수적이라 할 것인바, 이하 도 2 ~ 도 3을 통해 블루레이 디스크(BD)에서 사용가능한 파일구조 및 데이터 기록구조에 대해 상세히 설명하면 다음과 같다.

[0082] 먼저, 도 2는 디스크 내에 기록된 오리지널 데이터를 재생관리 하기 위한 파일구조 및 파일구조에 따라 특정 타이틀이 재생되는 관계를 나타낸 것이다.

[0083] 즉, 본 발명의 파일구조는, 하나의 루트 디렉토리(root directory) 아래에 AACS디렉토리(AACS)와 적어도 하나 이상의 BD디렉토리(BDMV)가 존재한다. 상기 BD디렉토리(BDMV) 내에는 사용자와의 인터액티브티(interactivity)를 보장하기 위한 일반파일(상위파일) 정보로서 인덱스 파일("index")과 오브젝트 파일("MovieObjet")을 포함함과 아울러, 실제 디스크 내에 기록된 데이터에 대한 정보와 이를 재생하는 방법 등에 대한 정보를 가지는 디렉토리로서, 플레이리스트 디렉토리(PLAYLIST), 클립인포 디렉토리(CLIPINF), 스트림 디렉토리(STREAM), 보조 디렉토리(AUXDATA), BD-J 오브젝트 디렉토리(BDJO), 메타데이터 디렉토리(META) 및 백업 디렉토리(BACKUP)가 구비되어 있다. 이하 상기 디렉토리 및 디렉토리 내에 포함되는 파일에 대해 상세히 설명하면 다음과 같다.

[0084] 메타데이터 디렉토리(META)는 데이터에 대한 데이터(data about a data)인 메타데이터(metadata) 파일을 포함한다. 즉, 서치(Search)파일, 디스크 라이브러리(Disc Library)를 위한 메타데이터 파일 등이 상기 디렉토리에 존재한다.

[0085] BD-J 오브젝트 디렉토리(BDJO)는 BD-J 타이틀을 재생하기 위한 BD-J 오브젝트 파일을 포함한다.

[0086] 보조 디렉토리(AUXDATA)는, 디스크 재생에 필요한 부가적인 데이터 파일을 포함하며, 예를 들어, 인터액티브 그래픽(interactive graphic)의 실행시에 사운드를 제공하는 "Sound.bdmv" 파일, 디스크 재생시 폰트(font) 정보를 제공하는 "11111.otf"파일등이 있다.

[0087] 스트림 디렉토리(STREAM)는, 디스크 내에 특정 포맷으로 기록된 AV 스트림에 대한 파일들이 존재하며, 각각의 스트림은 현재 널리 알려진 MPEG-2 방식의 트랜스포트(Transport) 패킷(packet)으로 기록되는 경우가 가장 일반적이며, 스트림 파일 (01000.m2ts, 02000.m2ts)의 확장명으로 "*.m2ts" 로 사용한다. 특히, 상기 스트림 중에 비디오/오디오/그래픽 정보가 모두 멀티플렉싱된(multiplexed) 스트림을 AV스트림이라 명하고, 적어도 하나 이상의 AV스트림 파일들로서 타이틀(Title)을 구성하게 된다.

[0088] 클립인포 디렉토리(CLIPINF)는 상기 각각의 스트림 파일("*.m2ts")과 일대일 대응하는 클립인포 파일(01000.clpi, 02000.clpi)들로 구성되어 진다. 특히, 클립인포 파일("*.clpi")은 대응하는 스트림 파일

("*.m2ts")의 속성정보 및 타임정보 (timing information)등을 기록하게 된다. 관련하여, 스트림 파일("*.m2ts")과 스트림 파일("*.m2ts")에 일대일 대응하는 클립인포 파일("*.clpi")을 묶어 이를 "클립(clip)"이라고 명명한다. 즉, "클립(clip)"은 스트림 파일("*.m2ts")과 이에 클립인포파일("*.clpi")을 모두 포함한 데이터가 된다.

[0089] 플레이리스트 디렉토리(PLAYLIST)는 플레이리스트 파일("*.mpls")들로 구성되며, 각각의 플레이리스트 파일("*.mpls")은 특정 클립(clip)이 재생되는 시간(playing interval)을 지정하는 적어도 하나 이상의 플레이아이템(PlayItem; PI) 및 서브플레이아이템(SubPlayItem; SPI)을 포함하고 있으며, 플레이아이템(PI) 및 서브플레이아이템(SPI)은 재생을 원하는 특정 클립(clip)의 재생 시작시간(IN-Time)과 재생 종료시간(OUT-Time)에 대한 정보를 가지고 있다.

[0090] 관련하여, 플레이리스트 파일 내에서 상기 적어도 하나 이상의 플레이아이템(PI)에 의해 재생되는 과정을 "메인패스(main path)"라 하고, 각각의 서브플레이아이템(SPI)에 의해 재생되는 과정을 "서브패스(sub path)"라 정의하며, 또한, 플레이리스트 파일 내에서 상기 메인패스(main path)는 존재하여야 하며, 상기 서브패스(sub path)는 서브플레이아이템(SPI) 존재에 따라 적어도 하나 이상 필요에 따라 존재하게 된다.

[0091] 결국, 플레이리스트 파일은 적어도 하나 이상의 플레이아이템의 조합에 의해 원하는 클립의 재생을 수행하는 전체 재생관리 파일구조 내의 기본적 재생관리 파일단위가 된다.

[0092] 백업 디렉토리(BACKUP)는, 상기 파일구조상의 데이터 중 특히 디스크 재생과 관련된 정보가 기록되는 인덱스 파일("index"), 오브젝트 파일(Movie Object, BD-J Object), 유닛 키 파일(Unit Key file), 플레이리스트 디렉토리 (PLAYLIST)내의 모든 플레이리스트 파일("*.mpls") 및 클립인포 디렉토리(CLIPINF) 내의 모든 클립인포 파일("*.clpi")에 대한 복사본(copy) 파일을 저장하게 된다. 이는 상기 파일들의 손실시 디스크 재생에 치명적임을 고려하여 미리 백업(backup)용으로 별도 저장하기 위해서이다.

[0093] 상기 AACS디렉토리(AACS)에는 유닛 키 파일(Unit Key file)이 존재하며, 상기 유닛 키 파일(Unit Key file)은 키로 암호화된 데이터에 대한 키 정보가 기록되어진다.

[0094] 관련하여, 도 2의 또 다른 부분은, 전술한 상기 디스크 파일구조에 의해 특정 타이틀(Title)이 재생되는 관계를 도시한 것이다.

[0095] 즉, 인덱스 파일(이를 인덱스 테이블(index table)이라고도 한다.)에 의해 제공되는 타이틀에 대해 사용자의 타이틀 재생명령이 있을 시 해당 타이틀의 재생이 시작될 것인 바, 이를 상세히 설명하면 다음과 같다.

[0096] 인덱스 파일(index.bdmv) 내에는 해당 디스크가 로딩 되면 첫 번째 재생되는 화면에 대한 정보를 가지는 "First Paly" 정보와, 메뉴화면을 제공하는 "Top Menu"정보와, 적어도 하나 이상의 "타이틀(Title #1 ~ Title #n)" 정보가 구성되어 있다.

[0097] 광 디스크(30)가 광 기록재생장치(10) 내로 로딩 되면 상기 인덱스 테이블에 의한 타이틀 메뉴정보가 사용자에게 디스플레이(20)를 통해 제공되고, 사용자가 특정 타이틀 또는 메뉴화면 내의 특정 메뉴를 선택하면, 이후 디스크 제작자(author)가 미리 정의해둔 파일구조에 따라 재생이 시작된다. 즉, 사용자의 특정 타이틀(예를 들어, 타이틀 #1)의 재생명령이 있으면, 재생관리 파일구조상의 오브젝트파일(Movie Object, BD-J Object)내에 구비된 커맨드(command)에 따라 해당하는 플레이리스트 파일이 실행되어 지고, 이후 플레이리스트 파일 정보에 따라, 특정 플레이아이템 및/또는 서브플레이아이템에 의해 상기 타이틀 #1을 구성하는 적어도 하나 이상의 클립(예를 들어, Clip #1 ~ Clip #3)이 재생된다.

[0098] 관련하여, "First Paly", "Top Menu" 또는 "타이틀"이 암호화(encryption)된 경우 상기 "First Paly", "Top Menu", "타이틀"에 의해 재생되는 데이터는 복호화되어야 재생될 수 있다. 따라서, 상기 "First Paly", "Top Menu" 또는 "타이틀" 중 어느 하나의 재생명령이 내려지면 AACS디렉토리(AACS) 내의 유닛 키 파일(Unit Key file)에서 대응하는 키를 독출하고, 상기 독출된 키를 사용하여 데이터를 복호화한 후 재생하게 된다.

[0099] 도 3은 상기 파일구조에 관련된 정보들이, 디스크 내에 기록되는 형태를 간략히 나타낸 것으로, 디스크 내주로부터 보면, 전체 파일을 관리하기 위한 시스템정보로서 파일시스템 정보 영역(File System Information area)과, 기록된 AV스트림 ("*.m2ts")을 재생하기 위한 플레이리스트 파일 및 클립인포 파일이 기록된 영역(이를 "database area"라고도 한다) 및 오디오/비디오/그래픽 등으로 구성된 스트림이 기록되는 AV스트림 영역(AV stream area)이 존재함을 알 수 있다. 특히, 본 발명에서 디스크 내의 상기 AV스트림 영역(AV stream area)에 기록된 데이터를 오리지널 데이터로 명명함은 이미 전술한 바 있다.

[0100] 본 발명은 특히 상기 디스크 내에 기록된 오리지널 데이터(예를 들어, 도 2와 같은 파일구조)와 로컬 스토리지 내에 저장되는 어디셔널 데이터가 암호화된 경우 상기 암호화된 데이터를 복호화하는 복호방법 및 복호장치를 제공하고자 한다.

[0101] 도 4는 본 발명의 광 기록재생장치(10)의 전체 구성에 관한 일 실시 예를 나타낸 것이다.

[0102] 우선 광 디스크에 기록된 오리지널 데이터 및 재생관리 파일정보를 포함한 관리정보를 재생하기 위한 픽업(11)과 픽업(11)의 동작을 제어하는 서보(14), 상기 픽업(11)으로부터 수신된 재생신호를 원하는 신호 값으로 복원해내거나, 기록될 신호를 광 디스크에 기록되는 신호로 변조(modulation)하여 전달하는 신호처리부(13)와 상기 동작을 제어하는 마이컴(16)이 기본적으로 구성된다.

[0103] 또한, 제어부(12)는 사용자명령 등에 의해 광 디스크 외에 존재하는 어디셔널 데이터를 다운로드 받아 이를 로컬 스토리지(15)에 저장함과 아울러, 오리지널 데이터 및/또는 어디셔널 데이터가 암호화된 경우 상기 암호화된 데이터를 복호화하고 사용자의 요구에 따라 재생하게 된다.

[0104] 또한, AV 디코더(17)는 제어부(12)의 제어에 따라 출력데이터(오리지널 데이터 및/또는 어디셔널 데이터)를 최종적으로 디코딩하여 사용자에게 제공하게 된다.

[0105] 또한, AV 인코더(18)는 광 디스크에 신호를 기록하는 기능의 수행을 위해 제어부(12)의 제어에 따라 입력신호를 특정포맷의 신호, 예를 들어 MPEG2 트랜스포트 스트림으로 변환하여 신호처리부(13)에 제공하게 된다.

[0106] 도 5는 본 발명의 데이터의 암호화 및 복호화에 대한 개념적 이해를 돕기 위해 도시한 것이다.

[0107] 우선 데이터의 암호화에 대해 설명하면, 암호화라 함은 특정 알고리즘을 사용하여 데이터를 변형함으로써 콘텐츠 제공자(CP)가 제공하는 콘텐츠의 불법 복제(copy) 및 배포(redistribution), 편집 등을 방지하는 콘텐츠 보호방법을 말한다. 즉, 데이터의 암호화는 데이터로의 인증되지 않은 접근을 막는 일종의 자물쇠 역할을 하게 되며, 상기 특정 알고리즘은 자물쇠를 잠그는 키(Key) 역할을 하게 된다. 이하, 데이터의 암호화에 사용되는 상기 특정 알고리즘을 암호화 키(Key)라 부르기로 한다.

[0108] 상기 암호화된 데이터를 재생하기 위해서는, 상기 암호화에 사용된 특정 알고리즘을 해독할 수 있는 수단이 제공되어야 하고, 상기 특정 알고리즘 해독 수단은 자물쇠를 여는 일종의 키(Key) 역할을 하게 된다. 키(Key)가 제공되면, 상기 키를 사용하여 데이터 암호화에 사용된 알고리즘을 해독하고, 상기 데이터를 원래 형태로 복원하게 되는데, 이러한 데이터의 복원을 데이터의 복호화(decryption)라 한다.

[0109] 관련하여, 본 발명에서는 데이터의 암호화 및 복호화에 사용되는 상기와 같은 알고리즘을 키(Key)라 명하고, 상기 데이터의 암호화는 콘텐츠 단위, 타이틀 단위 등 일정한 단위별로 행해질 수 있는바, 상기 일정한 단위별로 데이터를 암호화하는데 사용되는 키를 "Unit Key"라 명하기로 한다.

[0110] 본 발명에서 "CPS(Content Protection System) Unit"이라 함은 같은 "Unit Key"를 사용하여 암호화된 "First Paly", "Top Menu" 및/또는 "Title"의 그룹을 의미하며 각 "CPS unit"은 "CPS_unit_number"를 갖는다.

[0111] 예를 들면, "First Paly"에 의해 재생되는 모든 AV 스트림 파일은 같은 "Unit Key"를 사용하여 같은 "CPS Unit"에 포함되고, "Top Menu"에 의해 재생되는 모든 AV 스트림 파일은 같은 "Unit Key"를 사용하여 암호화되어 같은 "CPS Unit"에 포함된다. 마찬가지로 하나의 타이틀에 의해 재생되는 모든 AV 스트림 파일은 같은 "Unit Key"로 암호화되고 같은 "CPS Unit"에 해당한다.

[0112] 도 5를 구체적으로 살펴보면, 기록매체인 BD-ROM 디스크에는 타이틀 #1, 2, 3(Title #1, 2, 3)가 기록되어 있고, 로컬 스토리지에 기록매체 외부로부터 다운로드 받은 타이틀 #4가 존재한다. 상기 타이틀(Title #1 ~ #4)을 구성하는 데이터는 암호화된 데이터이며, 상기 데이터의 암호화에 사용된 키에 대한 정보가 디스크 내의 유닛 키 파일(Unit Key file)로 존재한다. 상기 유닛 키 파일은 디스크 외부에 존재할 수도 있으나, 해킹(hacking) 등에 의한 정보누출을 막기 위해 디스크 내에 존재하는 것이 바람직할 것이다.

[0113] 사용자가 디스크 내에 기록된 타이틀 #3을 재생하도록 선택한 경우를 예를 들면, 상기 타이틀 #3을 복호화하기 위해서는 상기 타이틀 #3를 암호화하는데 사용된 키가 콘텐츠 복호화 모듈(Contents Decryption Module)에 제공되어야 한다.

[0114] 타이틀 #3를 암호화한 키가 제공되면, 상기 콘텐츠 복호화 모듈에서는 상기 제공된 키를 사용하여 상기 타이틀 #3을 암호화되기 전의 데이터 형태로 복호화하게 되며, 상기 복호화된 데이터가 디코더(17)를 통해 재생된다.

[0115] 도 5의 로컬 스토리지에 다운로드 된 어디셔널 데이터는 타이틀(Title) 단위로 다운로드 된 것으로서, 상기 다운로드 된 데이터를 포함하여 구성된 인덱스 테이블(Index Table)에서는 타이틀 #4로 표현되어 사용자에게 제공된다.

[0116] 사용자가 타이틀 #4의 재생을 명령하면, 상기 타이틀 #4를 암호화하는데 사용된 키가 상기 유닛 키 파일(Unit Key file)로부터 독출되며, 상기 독출된 키가 타이틀 #4와 함께 콘텐츠 복호화 모듈(Contents Decryption Module)에 제공되어 타이틀 #4를 복호화하게 된다.

[0117] 도 6 ~ 도 8b는 본 발명에 따른 키(Key)를 사용한 데이터 복호방법의 실시예를 도시한 것이다.

[0118] 도 6와 도 7은 디스크 내에 존재하는 키를 사용하여, 다운로드 된 데이터를 복호화하는 경우로서, 다운로드 된 데이터를 복호화하는데 사용하는 키가 도 6은 디스크 내에 기록된 데이터를 암호화하는 데 사용되는 키인 경우이고, 도 7은 다운로드 된 데이터를 위해 디스크 내에 별도로 저장된 경우이다. 도 8a와 도 8b는 로컬 스토리지에 키를 두고 상기 로컬 스토리지의 키로 데이터를 복호화하는 경우로서, 도 8a는 다운로드 된 데이터만 로컬 스토리지의 키를 사용하는 경우이고 도 8b는 다운로드 된 데이터뿐만 아니라 디스크 내에 기록된 데이터 역시 로컬 스토리지의 키를 사용하는 경우이다.

[0119] 도 6은 본 발명의 데이터 복호방법의 제 1 실시예로서, 디스크에 기록된 데이터의 복호화에 사용되도록 디스크 내에 저장된 키를 사용하여 다운로드 된 데이터를 복호화하는 예를 도시한 것이다.

[0120] 상기 디스크 내에 저장된 키는 디스크 내에 기록된 데이터의 암호화에 사용된 키이며, 데이터를 암호화한 키가 제공되어야 암호화된 데이터를 복호화할 수 있다.

[0121] 디스크에는 인덱스 테이블(Index Table : 610)과 유닛 키 파일(Unit Key file)이 존재하며, 상기 디스크 내에 존재하는 인덱스 테이블은 "First Paly" 과, "Top Menu", "타이틀(Title #1, 2, ...)"로 구성되어 있다.

[0122] 디스크 내에서 상기 유닛 키 파일은 타이틀을 구성하는 데이터를 암호화하는 데 사용된 키에 대한 정보가 저장된다. 이하에서는 타이틀 #n을 구성하는 데이터를 암호화하는 데 사용된 키를 "Key for Title #n"으로 나타낸다. 즉, Key for Title #1"(620a)은 디스크 내 타이틀 #1(610a)에 대한 키를 나타내고, "Key for Title #2"(620b)은 타이틀 #2(610b)에 대한 키를 나타낸다.

[0123] 디스크 외부로부터 로컬 스토리지에 암호화된 데이터가 다운로드 될 수 있고 상기 다운로드 된 데이터를 재생할 수 있는 새로운 인덱스 테이블(630)이 사용자에게 제공될 수 있다. 상기 인덱스 테이블(630) 상의 타이틀 #1(630a)은 디스크 내의 타이틀 #1(Title on Disc : 610a)을 나타내고 타이틀 #2(630c)는 다운로드 된 데이터를 포함하는 타이틀(Downloaded Title)을, 타이틀 #3(630b)는 디스크 내의 타이틀 #2((Title on Disc : 610b)를 나타낸다.

[0124] 상기 다운로드 된 타이틀 #2(630c)가 암호화(encrypiton)된 데이터로 이루어진 경우, 상기 타이틀 #2을 재생하기 위해서는 상기 암호화된 데이터가 복호화(decryption)되어야 한다.

[0125] 도 6에서는 상기 다운로드 된 데이터의 복호화에 사용되는 키(Key)가 디스크 내에 존재하는 경우로서, 상기 키는 디스크 내에 존재하는 다른 데이터의 암호화에 사용된 키이다. 즉, 새로운 인덱스 테이블 상의 타이틀 #2(630c)는 "Key for Title #1"(620a)로 복호화될 수 있는데, 상기 "Key for Title #1"(620a)는 디스크 내에 기록된 타이틀 #1(610a = 630a)의 암호화에 사용된 키이다.

[0126] 콘텐츠 제공자(CP)는 디스크 내에 기록된 데이터를 암호화하는데 사용된 키(620a, 620b 등)를 사용하여 데이터를 암호화하여 사용자에게 제공하여야 하며, 사용자가 상기와 같이 암호화된 데이터를 다운로드 받은 경우 플레이어는 디스크에서 상기 다운로드 받은 데이터를 암호화한 키를 독출하여 데이터를 복호화하고 재생하게 된다.

[0127] 도 7은 본 발명의 데이터 복호방법의 제 2 실시예로서, 다운로드 된 데이터를 위해 디스크 내에 별도로 저장된 키를 사용하여 다운로드 된 데이터를 복호화하는 예를 도시한 것이다.

[0128] 도 7의 디스크 내에 기록된 인덱스 테이블과 다운로드 된 데이터를 재생할 수 있는 새로운 인덱스 테이블은 도 6에서 전술한 인덱스 테이블(610,630)과 같다. 다만, 도 7의 실시예는 디스크 내에 기록된 데이터를 암호화한 키(721)와는 별도로 디스크 내에 다운로드 된 데이터를 위한 키(722)를 저장하고, 암호화된 데이터가 다운로드 된 경우 상기 별도로 저장된 키로 상기 암호화된 데이터를 복호화하는 차이가 있다.

[0129] 즉, 디스크 내에 기록된 타이틀(630a = 610a, 630b = 610b)은 디스크 내에 기록된 데이터를 암호화한 키(72

1)를 사용하여 복호화되고, 다운로드 된 데이터를 포함하여 구성된 타이틀(630c : 이하 다운로드 된 타이틀)은 다운로드 된 데이터를 위한 키(722)를 사용하여 복호화된다.

[0130] 구체적으로, 새로운 인덱스 테이블(630)의 타이틀 #1(630a)의 재생명령이 내려지면 디스크 내에 기록된 타이틀을 암호화한 키(721) 중에서 "Key Title for #1"(721a)가 상기 타이틀 #1과 함께 콘텐츠 복호화 모듈(Content Decryption Module)에 제공되고, 상기 "Key Title for #1"(721a)에 의해 타이틀 #1이 복호화(decrypiton)되게 된다. 타이틀 #3(630b)의 복호화에 사용되는 키인 "Key Title for #2"(721b) 역시 상기 디스크 내에 기록된 타이틀을 암호화하는데 사용된 키(721) 중 하나이다.

[0131] 디스크 제작자(author)는 다운로드 되는 데이터를 고려하여 여분의 키를 디스크 내에 저장할 수 있으며, 상기 키 중 하나로 데이터를 암호화하여 사용자에게 제공할 수 있다. 즉, 상기 새로운 인덱스 테이블(630) 상의 타이틀 #2(630c)는 다운로드 되는 데이터를 위해 디스크에 여분으로 저장된 키(722) 중 하나(Key for Title #n : 722a)로 암호화되어 제공된 것이다. 사용자가 상기 타이틀 #2(630c)의 재생명령을 내리면 플레이어는 디스크에서 다운로드 되는 데이터를 위해 저장된 키(722) 중 "Key for Title #n" 키를 독출하고 상기 키를 사용하여 타이틀 #2를 복호화하게 된다.

[0132] 도 8a은 본 발명의 데이터 복호방법의 제 3 실시예로서, 로컬 스토리지에 디스크에 저장된 키와는 별도로 키를 두고 상기 로컬 스토리지의 키를 사용하여 다운로드 된 데이터를 복호화하는 예를 도시한 것이다.

[0133] 해킹(hacking) 등에 의한 암호화 정보의 누출을 피하기 위해 데이터의 복호화에 사용되는 키는 디스크 내에 존재하는 것이 바람직할 것이나, 로컬 스토리지 내에 권한 없는 사용자의 접근이 차단되는 보안영역(Secure Area)를 설정하고 상기 보안영역에 키를 저장할 수도 있다.

[0134] 본 실시예에 따르면 디스크 내에 저장된 키(620) 외에 로컬 스토리지 내에 키(820)를 저장한 경우를 도시한 것으로서, 디스크와 로컬 스토리지에 각각 유닛 키 파일(Unit Key file)이 존재하게 된다. 상기 로컬 스토리지 내에 저장되는 키는 디스크 외부로부터 다운로드 된 것일 수도 있고 디스크로부터 독출된 것일 수도 있다.

[0135] 관련하여, 데이터를 복호화함에 있어서, 디스크 내에 저장된 데이터는 디스크 내에 저장된 키를 사용하여 복호화하고 다운로드 된 데이터는 로컬 스토리지 내에 저장된 키를 사용하여 복호화할 수도 있다.

[0136] 새로운 인덱스 테이블(630) 상의 타이틀 #1 또는 타이틀 #3의 재생명령이 내려지면, 플레이어는 디스크 내에 저장된 키(620) 중에서 해당 타이틀에 대응하는 키를 독출하고 이를 콘텐츠 복호화 모듈에 제공한다. 즉, 타이틀 #1에 대해서는 디스크 내에 저장된 키(620) 중 "Key for Title #1"(620a)이 독출되고, 타이틀 #3에 대해서는 "Key for Title #2"(620b)가 독출된다.

[0137] 반면, 다운로드 된 타이틀 #2의 재생명령이 내려지면, 상기 타이틀 #2의 복호화 과정에서는 디스크 내에 저장된 키를(620) 독출하는 대신 로컬 스토리지 내에 저장된 키(820) 중에서 대응하는 키(820a)를 독출하여 타이틀 #2를 복호화한다.

[0138] 도 8b는 본 발명의 데이터 복호방법의 제 4 실시예로서, 로컬 스토리지에 키를 두고 상기 로컬 스토리지의 키를 사용하여 디스크에 기록된 데이터와 다운로드 된 데이터를 도시한 것이다.

[0139] 도 8b는 도 8a와 마찬가지로 로컬 스토리지에 키가 저장되어 디스크와 로컬 스토리지에 각각 키가 존재하게 되나, 도 8a에서는 로컬 스토리지에 저장된 키를 다운로드 된 데이터의 복호화에만 사용하는 반면, 도 8b에서는 다운로드 된 데이터뿐 아니라 디스크 내에 기록된 데이터의 복호화에도 사용하는 차이가 있다.

[0140] 즉, 타이틀 #1, 2, 3(630a, 630c, 630b)의 복호화가 디스크 내에 저장된 키(620)에 이루어지는 것이 아니라, 로컬 스토리지에 저장된 키(820)에 의해 이루어진다. 다운로드 된 타이틀인 타이틀 #2(630c)의 복호화가 로컬 스토리지 내의 "Key for Title #n"(832a)를 사용하여 이루어짐은 물론 디스크 내에 기록된 타이틀인 타이틀 #1(630a)과 타이틀 #3(630b) 역시 로컬 스토리지 내의 "Key for Title #1"(831a)과 "Key for Title #2"(831b)를 사용하여 각각 복호화되며, 디스크 내에 저장된 키(620)는 사용되지 않는다.

[0141] 상기 로컬 스토리지 내에 저장된 키는 다운로드 받은 키일 수도 있고 디스크로부터 독출한 키일 수도 있으며, 로컬 스토리지 내에 보안영역을 설정하고 상기 보안영역에 키를 저장할 수 있음은 전술한 도 8a에서와 같다.

[0142] 관련하여, 디스크 내에 기록된 데이터의 복호화를 디스크 내에 저장된 키가 아닌 로컬 스토리지 내에 별도로 저장된 키를 사용하여 디스크 내에 기록된 데이터의 복호화하는 경우, 상기 디스크 내에 기록된 데이터의 복호화에 사용되는 로컬 스토리지 내에 저장된 키가 상기 디스크 내에 저장된 키로부터 독출된 경우에만 허용되

는 것으로 할 수도 있다.

[0143] 예를 들면, 디스크 내에 기록된 데이터를 복호화할 키는 디스크 내에 저장된 키로부터 독출하여 다운로드 되는 데이터를 복호화할 키와 함께 하나의 유닛 키 파일(Unit Key file)로 구성하여 로컬 스토리지 내에 저장하고, 데이터의 재생명령이 내려지면 로컬 스토리지의 상기 유닛 키 파일에서 필요한 키를 모두 독출할 수 있도록 할 수도 있을 것이다.

[0144] 도 8b에서는 디스크 내에 기록된 타이틀(630a, 630b)을 위한 키(831)와 다운로드 된 타이틀(630c)을 위한 키(832)가 구분되어 로컬 스토리지 내에 저장된 예를 도시하였으나, 도 6에서 디스크 내에 기록된 데이터에 사용되는 키가 다운로드 되는 데이터에 사용될 수 있는 것과 마찬가지로, 디스크 내에 기록된 타이틀을 위한 키인지 다운로드 된 타이틀을 위한 키인지를 구분하지 않고 저장될 수도 있음은 자명하다 할 것이다.

[0145] 본 발명을 통해 데이터 암호화에 대응하는 키를 소유한 사용자만이 데이터를 복호화할 수 있게 함으로써 콘텐츠 제공자의 안전한 콘텐츠 제공이 가능하게 된다. 즉, 권한 없는 사용자가 상기 데이터를 다운로드 받는 경우, 상응하는 키를 소유하고 있지 않을 것이므로 데이터를 재생할 수 없게 되며 이를 통해 기록매체 및 로컬 스토리지에 다운로드 되는 콘텐츠를 보호할 수 있게 된다.

[0146] 데이터가 암호화되어 있고 상기 데이터를 복호화할 수 있는 키가 복수개 존재하는 경우, 상기 키 중 상기 암호화된 데이터를 복호화할 수 있는 적절한 키가 선택되어야 할 필요가 있다. 본 발명은 링크정보를 이용하여 암호화된 데이터를 복호화할 수 있는 키를 선택하는 것을 포함하여 이루어지는 것을 특징으로 한다.

[0147] 도 9a ~ 도 9c는 본 발명의 링크(link)정보를 이용하여 데이터를 복호화하는 실시예를 도시한 것이다.

[0148] 이하에서는 한 타이틀을 구성하는 데이터가 동일한 "Unit Key"로 암호화되고, 링크정보로 "CPS_unit_number'를 이용하는 경우를 예로 하여 설명한다. 본 발명에서 "CPS_unit_number"는 "CPS Unit"단위로 주어지고, 상기 "CPS Unit"이 동일한 "Unit Key"로 암호화된 데이터의 그룹을 의미함은 앞서 설명한 바 있다.

[0149] 도 9a ~ 9b는 다운로드 되는 데이터의 링크정보가 인덱스 테이블(Index Table) 등 다운로드 되는 데이터의 데이터베이스(database) 정보 내에 기록된 경우이고, 도 9c는 다운로드 되는 데이터와 디스크 내에 기록된 데이터의 링크정보가 로컬 스토리지에 별도의 파일로 구성된 경우이다.

[0150] 도 9a는 본 발명의 링크정보를 이용하여 데이터를 복호화하는 방법의 제 1 실시예로서, 다운로드 되는 데이터를 복호화할 수 있는 키를 알려주는 링크정보가 인덱스 테이블에 존재하고, 상기 키가 디스크 내에 기록된 데이터의 암호화에 사용된 키인 경우를 도시한 것이다.

[0151] 즉, 9a에서는 유닛 키 파일(Unit Key file : 910)에 디스크 내에 기록된 데이터의 암호화에 사용된 키(예를 들면, 910a, 910b)만이 기록되고, 다운로드 되는 타이틀의 암호화에 사용되는 키는 별도로 기록되어 있지 않은 경우의 실시예를 설명한다.

[0152] 디스크 내의 유닛 키 파일(Unit Key file : 910)은 디스크 내에 기록된 데이터가 어떤 "CPS Unit"에 포함되는지를 알려주는 정보인 "CPS_unit_number"와 상기 "CPS Unit"에 대한 "Unit Key"로 구성된다. 도 9a의 실시예는 한 타이틀을 구성하는 데이터가 동일한 "Unit Key"로 암호화된 경우로서, 타이틀별로 "CPS_unit_number"가 주어질 수 있다.

[0153] 관련하여, 상기 "CPS_unit_number"는 타이틀 하나당 개별적으로 주어지면 족하고 별개의 타이틀이 각각 다른 "CPS_unit_number"를 가질 필요는 없다. 즉, 복수의 타이틀이 동일한 "CPS_unit_number"를 가질 수도 있고 각각의 타이틀마다 다른 "CPS_unit_number"를 가질 수도 있다.

[0154] 또한, 유닛 키 파일 내에 기록된 "Unit Key"는 "CPS Unit"마다 정의되는 것이 바람직하다. 따라서, 본 발명에서는 "CPS_unit_number"이 다르면 다른 "Unit Key"로 암호화되어 다른 "CPS Unit"에 포함되는 데이터인 것을 의미하고, "CPS_unit_number"이 같으면 동일한"Unit Key"로 암호화되어 동일한 "CPS Unit"에 포함되는 데이터인 것을 의미한다.

[0155] 인덱스 테이블(630)의 타이틀 #1(630a)은 디스크 내에 기록된 타이틀 중 타이틀 #1에 해당하고 타이틀 #3(630b)은 디스크 내에 기록된 타이틀 중 타이틀 #2에 해당하는 타이틀이다. 즉 타이틀 #3(630b)를 재생하면, 디스크 내에 기록된 타이틀 #2가 재생되게 된다. 상기 인덱스 테이블의 타이틀 #2(630c)는 다운로드 된 타이틀이다. 관련하여, 상기 인덱스 테이블은 다운로드 된 타이틀을 재생할 수 있도록 새로이 구성된 것으로서 콘텐츠 제공자에 의해 별도로 제공된 것일 수도 있고, 로컬 스토리지에서 새로이 생성된 것일 수도

있다.

[0156] 결국, "CPS_unit_number for Title #1"(930a)은 인덱스 테이블(630)의 타이틀 #1(630a)의 링크정보가 되고, "CPS_unit_number for Title #2"(930b)는 인덱스 테이블의 타이틀 #3(630b)의 링크정보가 된다.

[0157] 인덱스 테이블(630)의 타이틀 #1(630a)의 재생명령이 내려지면, 플레이어는 디스크 내에 저장된 유닛 키 파일(910)로부터 "CPS_unit_number for Title #1"을 확인하여 상기 타이틀 #1(630a)이 포함되는"CPS Unit"을 알 수 있게 된다. 도 9a에서 상기 타이틀 #1은 "CPS Unit #1"에 포함된다. 상기 타이틀 #1이 "CPS Unit #1"에 포함되는 것이 확인되면 "Unit Key for CPS Unit #1"(910a)이 상기 타이틀 #1을 복호화하기 위해 독출되게 된다. 상기 인덱스 테이블의 타이틀 #3(630b)의 경우, 상기 타이틀 #3는 디스크 내에 기록된 타이틀 #2와 동일한 타이틀이므로 유닛 키 파일(910)의 "CPS_unit_number for Title #2"로부터 상기 타이틀 #3(630b)가 "CPS Unit #2"에 포함됨을 확인할 수 있다.

[0158] 인덱스 테이블(630)의 타이틀 #2(630c)를 재생하기 위해서도 상기 타이틀 #2를 복호화할 수 있는 키가 필요하므로 유닛 키 파일에서 적절한 키가 선택되어야 한다. 본 발명은 다운로드 되는 데이터의 복호화에 필요한 적절한 키를 독출하기 위해 데이터와 상기 데이터의 복호화에 필요한 키를 연결하는 링크정보를 두는 것을 특징으로 하며, 상기 링크정보는 데이터베이스(database) 정보에 주어질 수 있다.

[0159] 예를 들어, 상기 타이틀 #2(630c)가 "CPS Unit #1"에 포함되는 경우, 즉 "Unit Key for CPS Unit #1"으로 암호화된 경우, 상기 타이틀 #2를 포함하여 구성되는 인덱스 테이블에 상기 타이틀 #2에 대해 "CPS_unit_number = 1"이라는 링크정보를 둘 수 있다. 이 경우 상기 타이틀 #2(630c)의 재생명령이 내려지면, 플레이어는 인덱스 테이블로부터 "CPS_unit_number"를 확인하여 "Unit Key for CPS Unit #1"(910a)을 독출할 수 있다.

[0160] 관련하여, 상기 타이틀 #2(630c)의 복호화에 사용되는 키는 디스크 내에 기록된 타이틀인 타이틀 #1(630a)의 암호화에 사용된 키이기도 하다. 즉, 도 9a의 실시예는 다운로드 된 타이틀과 디스크 내에 기록된 타이틀이 "Unit Key"를 공유하는 경우를 나타낸 것이다.

[0161] 본 발명에 따라 상기와 같이 암호화된 데이터와 상기 데이터를 암호화한 키 사이에 링크정보를 두면, 상기 링크정보를 이용하여 데이터를 암호화한 키를 손쉽게 독출할 수 있게 됨으로써 데이터를 원활하게 복호화할 수 있는 장점이 있다.

[0162] 도 9b는 본 발명의 링크정보를 이용하여 데이터를 복호화하는 방법의 제 2 실시예로서, 다운로드 되는 데이터의 링크정보가 인덱스 테이블에 존재하고 상기 링크정보에 의해 독출되는 키가 다운로드 되는 데이터를 위해 디스크 내에 별도로 저장된 키인 경우를 도시한 것이다.

[0163] 도 9b는 도 9a와 마찬가지로 다운로드 된 데이터와 상기 데이터를 복호화할 수 있는 키에 대한 링크정보가 데이터베이스(database) 정보 내에 존재하나, 다운로드 되는 데이터가 디스크 내에 기록된 데이터와 다른 키를 사용하여 복호화된다는 점에 차이가 있다.

[0164] 인덱스 테이블은 도 9a에서 설명한 바와 같이 다운로드 된 타이틀을 재생할 수 있는 새로운 인덱스 테이블(630)이며, 상기 인덱스 테이블의 타이틀 중 타이틀 #1(630a)과 타이틀 #3(630b)은 각각 디스크 내에 기록된 타이틀 #1과 타이틀 #2와 동일한 타이틀이고 타이틀 #2(630c)는 다운로드 된 타이틀이다.

[0165] 따라서, 상기 디스크 내에 기록된 타이틀의 재생명령이 내려지면, 유닛 키 파일의 타이틀별 "CPS_unit_number"을 이용하여 상기 타이틀을 복호화할 수 있는 키를 독출할 수 있다. 즉, 인덱스 테이블(630)의 타이틀 #1(630a)은 "CPS_Unit_number for Title #1"으로부터 상기 타이틀 #1(630a)이 "CPS Unit #1"에 포함된다는 정보를 확인할 수 있다. 상기 정보가 확인되면 상기 타이틀 #1(630a)은 디스크 내에 기록된 데이터의 암호화에 사용된 키(921) 중에서 "Unit key for CPS Unit #1"(921a)를 독출하여 복호화될 수 있다. 마찬가지로, 인덱스 테이블(630)의 타이틀 #3(630b)는 "CPS_Unit_number for Title #2"을 통해 디스크 내에 기록된 데이터의 암호화에 사용된 키(921) 중 "Unit Key for CPS Unit #2"(921a)에 의해 복호화된다.

[0166] 디스크 제작자는 다운로드 되는 데이터를 고려하여, 디스크 내에 기록된 데이터를 암호화한 키와 별도로 다운로드 되는 데이터를 위한 키를 디스크 내에 여분으로 저장할 수도 있다. 콘텐츠 제공자는 상기 디스크 내에 저장된 키 중에서 다운로드 되는 데이터를 위해 별도로 저장된 키로 데이터를 암호화하여 데이터를 제공함으로써 상기 키를 가진 사용자만이 상기 다운로드 되는 데이터를 재생할 수 있도록 할 수 있다.

[0167] 타이틀 #2(630b)는 다운로드 되는 데이터를 위해 여분으로 디스크 내에 저장된 키(922) 중에서 "Unit Key for CPS Unit #n"(922a)으로 암호화된 것이다. 본 발명에 따라 상기 타이틀 #2(630c)을 암호화한 키에 대한 링크

정보가 가 "CPS_unit_number = N"으로 데이터베이스(database) 정보인 인덱스 테이블(630)에 존재하게 된다. 타이틀 #2(630c)의 재생명령이 내려지면 플레이어는 인덱스 테이블(630)에서 "CPS_unit_number"가 "N"임을 확인하고, 상기 "CPS_unit_number"을 이용하여 "Unit Key for CPS Unit #n"을 독출한다. 상기 독출된 "Unit Key for CPS Unit #n"가 타이틀 #3(630)과 함께 콘텐츠 복호화 모듈(Content Decryption Module)에 제공되어 타이틀 #3(630)이 복호화된 후 디코더에 의해 재생되게 된다.

[0168] 도 9c는 본 발명의 링크정보를 이용하여 데이터를 복호화하는 방법의 제 3 실시예로서, 상기 링크정보가 로컬 스토리지 내에 별도의 파일로 구성되는 경우를 도시한 것이다.

[0169] 도 9c는 도 9a 및 도 9b와 마찬가지로 링크정보를 두어 대응하는 키를 독출할 수 있도록 하는 실시예이나, 링크정보가 데이터베이스 정보에 존재하는 것이 아니라 별도의 파일로 존재하고, 디스크 내에 기록된 타이틀과 다운로드 된 타이틀 모두 상기 파일을 이용하여 대응하는 키를 독출하는 점에 차이가 있다.

[0170] 디스크 내에 암호화된 데이터를 위한 유닛 키 파일(Unit Key file : 910)이 존재하며, 데이터가 다운로드 된 경우 상기 데이터를 재생할 수 있도록 하는 새로운 인덱스 테이블(630)이 존재한다.

[0171] 타이틀 #1(630a)은 "Unit Key for CPS Unit #1"(910a)으로 암호화된 타이틀이고, 타이틀 #3(630b)는 "Unit Key for CPS Unit #2"(910b)로 암호화된 타이틀이다. 타이틀 #2는 다운로드 된 타이틀로서 "Unit Key for CPS Unit #3"(910b)로 암호화된 것이다.

[0172] 인덱스 테이블(630)의 "First Paly", "Top Menu", "타이틀" 중 하나에 의해 데이터가 재생되기 위해서는 상기 데이터가 복호화될 필요가 있고, 상기 복호화에 필요한 적절한 키가 독출되어 콘텐츠 복호화 모듈에 제공되어야 한다. 암호화된 데이터와 상기 데이터를 암호화한 키를 연결하기 위해 로컬 스토리지 내에 링크정보를 별도의 파일로 구성할 수 있다. 상기 별도로 구성된 파일을 이하 링크정보파일이라 한다.

[0173] 인덱스 테이블(630) 상의 각 항목에 대한 "CPS_unit_number"를 포함하여 이루어진 링크정보파일(930)이 로컬 스토리지 내에 구성된다. 상기 인덱스 테이블의 타이틀 #1(630a)은 상기 링크정보파일에서는 타이틀 #1을 의미하고 타이틀 #2(630c)는 타이틀 #3를, 타이틀 #3(630b)는 타이틀 #2를 의미한다. 즉, "CPS_unit_number for Titel #1"(930a)은 인덱스 테이블(630)의 타이틀 #1(630a)의 "CPS_unit_number"을 나타내며, "CPS_unit_number for Title #2"(930b)는 인덱스 테이블의 타이틀 #3(630b)의 "CPS_unit_number"을 나타낸다. "CPS_unit_number for Title #3"는 인덱스 테이블의 타이틀 #2(630b)의 "CPS_unit_number"이다.

[0174] 타이틀 #1(630a)의 재생명령이 내려지면 로컬 스토리지 내에 구성된 링크정보파일로부터 상기 타이틀 #1(630a)의 "CPS Unit"을 알 수 있다. 도 9a에서 인덱스 테이블의 타이틀 #1(630a)의 "CPS_unit_number"는 "1"이고, 타이틀 #2(630c)의 "CPS_unit_number"는 "3", 타이틀 #3(630b)의 "CPS_unit_number"는 "2"이다. 결국, 타이틀 #1(630a)은 "CPS Unit #1"에 포함되므로, 유닛 키 파일(910)로부터 "Unit Key for CPS Unit #1"(910a)이 독출되게 되고, 인덱스 테이블의 타이틀 #3(630b)의 경우에는 "Unit Key for CPS Unit #2"(910b)가 독출되게 된다. 타이틀 #2(630c)는 "CPS_unit_number"가 "3"이고, "CPS Unit #3"에 포함되는 데이터이므로 "Unit Key for CPS Unit #3"(910c)가 독출된다.

[0175] 관련하여, 상기 링크정보파일(930)은 로컬 스토리지 내에 보안영역을 설정하고 상기 보안영역에 구성될 수도 있고, AV 데이터(AV data)가 저장되는 AV 데이터 기록영역에 구성될 수도 있다. 상기 링크정보파일(930)은 "CPS_unit_number"만으로 구성된 유닛 키 파일(Unit Key file)의 일종일 수 있다. 다만, 상기 링크정보파일은(930) 디스크 내에 저장된 유닛 키 파일(910)과는 달리 데이터를 암호화하는 실제 키를 포함하고 있지는 않다.

[0176] 또한, 상기 링크정보파일(930)은 다운로드 되는 데이터의 재생을 위해 콘텐츠 제공자로부터 별도로 제공될 수도 있으며, 디스크 내에 기록된 데이터와 다운로드 된 데이터가 가진 링크정보를 독출하여 구성된 것일 수도 있다.

[0177] 또한, 유닛 키 파일(Unit Key file)에서 "Unit key"는 디스크 내에 기록된 데이터와 다운로드 된 데이터가 공유하여 사용할 수도 있으나, 다운로드 되는 데이터를 위해 여분의 "Unit Key"가 저장되고, 데이터가 다운로드 되면 상기 여분의 "Unit Key"를 사용하여 복호화될 수 있음은 앞서 설명한 바 있다.

[0178] 또한, 도 9a ~ 9c에서는 유닛 키 파일이 디스크 내에 저장된 경우를 예로 하여 설명하였으나, 앞서 도 8a 및 도 8b에서 설명한 바와 같이 로컬 스토리지 내에 별도의 유닛 키 파일이 저장되는 것도 가능하다.

[0179] 도 6 ~ 도 9c의 새로운 인덱스 테이블(630)은 외부로부터 인덱스 파일("index") 형태로 다운로드 된 것일 수

도 있고 로컬 스토리지 내에서 새로이 생성된 것일 수도 있는 것으로서 다운로드 된 데이터를 재생할 수 있도록 사용자에게 제공될 수 있으면 족함을 밝혀둔다.

[0180] 도 10은 본 발명에 따른 데이터 복호방법을 도시한 것이다.

[0181] 암호화된 데이터의 재생명령이 내려지면(S10), 플레이어는 상기 데이터의 링크 정보를 확인한다(S20). 상기 링크정보는 데이터베이스(database)에 존재할 수도 있고, 링크정보파일로 로컬 스토리지 내에 존재할 수도 있음은 도 9a~ 도 9c에서 설명한 바 있다.

[0182] 상기 링크정보를 이용하여 기록매체 또는 로컬 스토리지 내에 존재하는 유닛 키 파일(Unit Key file)로부터 데이터를 암호화한 키를 독출(S30)한다. 상기 유닛 키 파일은 기록매체 내에 기록된 데이터를 암호화한 키로만 구성된 것일 수도 있고 상기 기록매체 내에 기록된 데이터를 암호화한 키 외에 다운로드 되는 데이터를 위한 키를 여분으로 포함하여 구성된 것일 수도 있다.

[0183] 키가 독출(S30)되면, 상기 암호화된 데이터는 상기 키와 함께 콘텐츠 복호화 모듈(Contents Decryption Module)에 제공(S40)된다. 콘텐츠 복호화 모듈에서는 상기 제공된 키를 사용하여 상기 데이터가 복호화(S50)되고, 데이터가 복호화되면 상기 데이터는 암호화 이전 형태로 복원되어 디코더(17)에 의해 재생될 수 있게 된다.

[0184] 도 11은 재생되는 데이터가 공유되는 경우 본 발명의 실시예를 도시한 것이다.

[0185] 디스크 내에 복수의 타이틀이 존재하고, 상기 타이틀이 다른 타이틀을 구성하는 클립(Clip)의 일부 또는 전부를 공유할 수도 있다. 디스크 제작자는 복수의 타이틀이 클립을 공유하는 경우, 동일한 "Unit Key"에 의해 암호화된 같은 "CPS Unit"에 포함되는 데이터를 사용하여 타이틀을 구성하는 것이 바람직하며, 다른 "CPS Unit"에 속하는 데이터는 공유하지 않는 것이 좋다. 왜냐하면, 다른 "CPS Unit"에 포함되는 데이터로 구성된 타이틀의 경우 하나의 "Unit Key"로 복호화될 수 없고 다른 "Unit Key"가 사용되어야 하므로, 상기 타이틀이 재생되어야 할 때 오류가 발생할 수 있기 때문이다.

[0186] 타이틀 #3(Title #3)은 플레이리스 #3(PlayList #3)에 의해 재생되고, 상기 플레이리스트 #3은 두 개의 플레이아이템으로 구성된다. 상기 타이틀 #3은 타이틀 #1에 의해 재생되는 클립(1110)의 일부(1110a)와 타이틀 #2에 의해 재생되는 클립(1120)의 일부(1120a)를 공유하여 구성된다. 타이틀 #3가 타이틀 #1과 클립을 공유하기 위해서는 상기 타이틀 #3에는 타이틀 #1과 동일한 "Unit Key"가 할당되어야 한다. 마찬가지로 타이틀 #3가 타이틀 #2와 클립을 공유하기 위해서는 상기 타이틀 #2와 동일한 "Unit key"가 상기 타이틀 #3에 할당되어야 된다. 결국, 타이틀 #1과 타이틀 #2은 직접적으로 클립을 공유하지는 않으나, 같은 "Unit Key"에 의해 암호화되어야 할 것이다. 따라서, 클립을 직접적 또는 간접적으로 공유하여 서로 관계되는 타이틀 #1, 2, 3는 모두 동일한 "Unit Key"인 "Key #1"을 갖는다.

[0187] 타이틀 #3가 디스크 내에 기록된 타이틀인 경우를 예로 하여 상술하였으나, 상기 타이틀 #3가 디스크 외부로부터 다운로드 되는 타이틀인 경우에도 상술한 논리가 적용될 수 있다. 콘텐츠 제공자는 다운로드 받는 타이틀을 제공함에 있어서, 디스크 내에 기록된 클립을 포함하여 상기 타이틀을 구성하고자 하는 경우, 같은 "CPS Unit"에 포함되는 클립을 사용하는 것이 바람직하다. 디스크 제작자는 클립을 다운로드 되는 타이틀에 사용하고자 하는 경우, 상기 클립은 동일한 "Unit Key"로 암호화하여 디스크에 기록할 수 있을 것이다.

[0188] 상기에서는 기록매체에 데이터가 기록되어 있고 상기 기록되어 있는 데이터를 재생만 할 수 있는 BD-ROM을 예로 설명한 것이다. 기록매체에 따라 재생뿐만 아니라 상기 기록매체에 데이터를 기록할 수 있는바, 이하 기록가능한 기록매체 중 BD-RE(BD Rewritable)를 예로 하여, 키로 암호화된 데이터를 기록하는 방법에 대해 설명한다.

[0189] BD-RE에서는 데이터를 디스크에 기록하는 과정에서, 상기 기록되어야 할 데이터를 재생할 수 있는 플레이리스트를 가상적으로 생성하게 된다. 상기 가상적으로 생성되는 플레이리스트를 가상 플레이리스트(Virtual PlayList)라 하고, 상기 가상 플레이리스트에 의해 디스크에 기록되는 데이터의 편집, 기록 등이 이루어지게 된다.

[0190] 상기 가상 플레이리스트는 하나 이상의 플레이아이템(PI)으로 이루어지며 상기 플레이아이템은 상기 가상 플레이리스트에 의해 재생되어야 할 클립을 지정한다. 상기 클립은 기록매체 또는 로컬 스토리지 내에 존재하고, 리얼 플레이리스트(Real PlayList)에 의해 재생될 수 있는 실제 데이터이다. 상기 가상 플레이리스트는 하나의 리얼 플레이리스트에 의해 재생되는 데이터로만 생성될 수도 있으나 복수의 리얼 플레이리스트에

의해 재생되는 데이터의 일부 또는 전부를 조합하여 생성될 수도 있다.

[0191] 이하, 도 11의 플레이리스트 #1(PlayList #1)을 리얼 플레이리스트 #1, 플레이리스트 #2(PlayList #2)를 리얼 플레이리스트 #2라 하고, 플레이리스트 #3(PlayList #3)를 상기 플레이리스트 #1, 2에 의해 재생되는 데이터를 기록할 수 있는 플레이리스트로서 가상 플레이리스트 #3라 하여 설명하기로 한다.

[0192] 본 발명은 가상 플레이리스트를 생성함에 있어서, 상기 가상 플레이리스트의 생성에 사용되는 클립이 암호화된 경우, 상기 클립이 같은 "CPS Unit"에 포함되는 것을 특징으로 한다. 즉, 다른 "CPS Unit"에 포함되는 데이터에 의해서는 상기 가상 플레이리스트를 생성하지 않는 것이 바람직하다.

[0193] 가상 플레이리스트 #3은 리얼 플레이리스트 #1에 의해 재생되는 클립(1110) 일부(1110a)와 리얼 플레이리스트 #2에 의해 재생되는 클립(1120)의 일부(1120a)를 조합하여 생성될 수 있다. 리얼 플레이리스트 #1에 의해 재생되는 클립(1110)과 리얼 플레이리스트 #2에 의해 재생되는 클립(1120)은 "Unit Key"가 "Key #1"로 동일하다. 동일한 "Unit Key"를 사용하여 암호화된 경우 같은 "CPS Unit"에 포함되는바, 상기 클립(1110, 1120)은 같은 "CPS Unit"에 포함되는 클립이고, 상기 클립의 일부(1110a, 1120a)를 조합하여 가상 플레이리스트 #3를 생성할 수 있다. 상기 가상 플레이리스트 #3에 의해 데이터가 디스크에 기록된 경우, 상기 디스크에 기록된 데이터는 "Key #1"을 사용하여 복호화될 수 있다.

[0194] 본 발명은 리얼 플레이리스트 #1에 의해 재생되는 클립(1110)과 리얼 플레이리스트 #2에 의해 재생되는 클립(1120)이 다른 "CPS Unit"에 포함되는 경우 즉, 다른 "Unit Key"에 의해 암호화된 경우에는 가상 플레이리스트를 생성할 수 없도록 함으로써, 콘텐츠 제공자가 허용하지 않는 콘텐츠의 복사, 편집, 기록을 방지할 수 있으며, 이를 통해 콘텐츠를 보호할 수 있게 된다.

[0195] 도 12은 타이틀(Title)이 메인패스(main path)와 서브패스(sub path)로 이루어진 경우 본 발명의 실시예를 도시한 것이다.

[0196] 플레이리스트는 메인패스만으로 구성될 수 있으나 하나의 메인패스와 하나 이상의 서브패스로 구성될 수 있다. 플레이리스트가 서브패스를 포함하는 경우 메인패스와 상기 서브패스을 구성하는 데이터는 같은 "CPS Unit"에 포함되는 것이 바람직하며 이 경우 상기 메인패스와 서브패스는 동일한 "Unit Key"에 의해 복호화될 수 있다.

[0197] 도 12는 메인패스를 구성하는 데이터는 디스크 내에 기록된 데이터이고 서브패스를 구성하는 데이터가 로컬 스토리지에 다운로드 된 경우이다. 상기 다운로드 된 데이터를 재생할 수 있는 로컬 스토리지의 플레이리스트는 메인패스 하나와 서브패스 둘(sub path #2, sub path #3)로 이루어진다.

[0198] 상기 메인패스는 플레이아이템 #1, 2(PI #1, 2)로 구성되며, 상기 플레이아이템 #1은 디스크 내에 기록된 클립 #1(1210a)을 지정하고 상기 플레이아이템 #2는 디스크 내에 기록된 클립 #2(1210b)을 지정한다. 상기 클립 #1과 클립 #2는 비디오(Video), 오디오(Audio), 프레젠테이션 그래픽(PG), 인터액티프 그래픽(IG)이 멀티 플렉싱된 클립이다.

[0199] 서브패스 #2와 서브패스 #3은 각각 하나의 서브플레이아이템(SPI)으로 이루어지고, 상기 서브패스 #2을 이루는 서브플레이아이템은 로컬 스토리지 내에 저장된 클립 #1(1220a)을 지정하고 서브패스 #3을 이루는 서브플레이아이템은 로컬 스토리지 내에 저장된 클립 #2(1220b)를 지정한다. 로컬 스토리지 내에 저장된 상기 클립 #1, 2(1220a, 1220b)는 디스크 외부로부터 다운로드 된 클립으로서 상기 클립 #1(1220a)은 동기된 오디오 스트림(Sync type Audio stream)이고 클립 #2(1220b)는 프리젠테이션 그래픽만을 위한 스트림(PG-only stream)이다.

[0200] 상기 메인패스를 이루는 디스크 내에 기록된 클립 #1(1210a)과 클립 #2(1210b)는 "Key for Title #2"에 의해 암호화된 클립이며, 상기 클립이 재생되기 위해서는 "Key for Title #2"로 복호화가 이루어져야 한다. 상기 메인패스와 서브패스 #2 및/또는 서브패스 #3를 함께 재생하는 경우, 상기 서브패스 #2와 서브패스 #3를 이루는 로컬 스토리지에 저장된 클립 #1(1220a)과 클립 #2(1220b)는 상기 "Key for Title #2"에 복호화될 수 있다.

[0201] 콘텐츠 제공자는 서브패스 #2와 서브패스 #3를 이루는 클립 #1(1220a)과 클립 #2(1220b)를 암호화하는 경우, 상기 서브패스와 함께 재생될 메인패스를 이루는 클립 #1(1210a)과 클립 #2(1210b)을 암호화하는데 사용된 키와 동일한 "Key for Title #2"를 사용하여야 할 것이다. 상기 암호화된 클립을 다운로드 받은 사용자 중에서, 상기 "Key for Title #2"를 가진 사용자는 상기 "Key for Title #2"를 사용하여 메인패스와 상기 서브패스를

동시에 재생할 수 있게 된다.

[0202] 도 12에서는 서브패스를 구성하는 데이터를 다운로드 받는 경우를 예로 하였으나, 플레이리스트에 의해 재생되는 데이터가 모두 디스크 내에 기록된 데이터일 수도 있고 메인패스를 구성하는 데이터가 다운로드 될 수도 있다. 메인패스 또는 서브패스를 이루는 데이터 중 일부를 다운로드 받아 디스크 내에 기록된 데이터와 함께 재생할 수도 있을 것이다.

[0203] 이하, 전술한 도 4의 구성을 참조하여, 본 발명에 따른 데이터 복호장치에 대해 설명한다.

[0204] 본 발명에 따른 데이터 복호장치는 기록매체로부터 기록매체의 정보를 독출하는 픽업(11)과 상기 기록매체와 관련되어 다운로드 되는 암호화된 데이터가 저장되는 로컬 스토리지(15)와 상기 암호화된 데이터를 복호화하는 제어부(12)를 포함하여 이루어진다. 상기 제어부(12)는 상기 기록매체 내에 저장된 키(Key)를 독출하여 콘텐츠 복호화 모듈에 제공하고, 상기 콘텐츠 모듈에서 상기 독출된 키를 사용하여 상기 암호화된 데이터를 복호화(decryption)하도록 제어하는 것을 특징으로 한다.

[0205] 관련하여, 상기 제어부(12)에 의해 독출되는 키는 상기 기록매체 내에 기록된 데이터의 암호화에 사용된 키일 수 있다.

[0206] 또한, 상기 제어부(12)에 의해 독출되는 키는 다운로드 되는 데이터의 복호화를 위해 상기 기록매체 내에 별도로 저장된 키일 수도 있다.

[0207] 본 발명에 따른 데이터 복호장치는 기록매체로부터 기록매체의 정보를 독출하는 픽업(11)과, 데이터 복호화에 사용되는 키(Key)와 상기 기록매체와 관련되어 다운로드 되는 암호화(encryption)된 데이터가 저장되는 로컬 스토리지(15)와, 상기 로컬 스토리지 내에 저장된 키를 사용하여 상기 암호화된 데이터를 복호화(decryption)하는 제어부(12)를 포함하여 이루어진다. 상기 로컬 스토리지 내에 저장된 키는 기록매체 내에 저장된 키와는 별도로 존재하는 키이며, 상기 제어부(12)는 다운로드 되는 데이터를 복호화하는 경우, 상기 기록매체 내에 저장된 키가 아닌 상기 로컬 스토리지 내에 저장된 키를 사용한다.

[0208] 관련하여, 상기 제어부(12)는 기록매체 내에 기록된 데이터를 복호화하는 경우에는 상기 기록매체 내에 저장된 키를 독출하고, 상기 독출된 키를 콘텐츠 복호화 모듈에 제공하여 상기 데이터를 복호화할 수 있다.

[0209] 또한, 상기 제어부(12)는 기록매체 내에 기록된 데이터를 복호화하는 경우, 상기 기록매체 내에 저장된 키가 아닌 상기 로컬 스토리지(15) 내에 저장된 키를 독출하여 상기 데이터를 복호화할 수도 있다.

[0210] 관련하여, 상기 로컬 스토리지(15) 내에 저장된 키는 상기 로컬 스토리지(15)에 권한없는 사용자의 접근이 제한되는 보안영역(secure area)를 설정된 경우, 상기 보안영역(secure area)에 위치하는 것이 바람직하다.

[0211] 본 발명에 따른 데이터 복호장치는 기록매체로부터 기록매체의 정보를 독출하는 픽업(11)과, 데이터 복호화에 사용되는 키(Key)와 상기 기록매체와 관련되어 다운로드 되는 암호화(encryption)된 데이터가 저장되는 로컬 스토리지(15)와, 상기 암호화된 데이터와 키 사이의 링크(link)정보를 확인하고, 상기 링크정보를 사용하여 상기 데이터의 암호화에 사용된 키를 독출하는 제어부(12)를 포함하여 이루어진다. 상기 제어부는 상기 독출된 키를 사용하여 상기 암호화된 데이터를 복호화(decryption)하게 된다.

[0212] 관련하여, 상기 제어부(12)는 상기 링크정보를 상기 다운로드 되는 데이터의 데이터베이스(database)정보에서 확인하여, 상기 확인된 링크정보를 이용하여 상기 데이터를 암호화한 키를 독출하는 것이 가능하다.

[0213] 또한, 상기 제어부(12)는 상기 링크정보를 로컬 스토리지(15)에 구성되는 링크정보파일에서 확인하는 것도 가능하다.

[0214] 또한, 상기 제어부(12)는 상기 로컬 스토리지(15)에 다운로드 되는 데이터가 기록매체 내에 기록된 메인패스(main path)와 관련되어 다운로드 되는 서브패스(sub path) 데이터인 경우, 상기 서브패스 데이터를 상기 메인패스 데이터와 동일한 키를 사용하여 복호화할 수도 있다.

[0215] 본 발명은 상술한 실시예에 한정되지 않으며, 첨부된 청구범위에서 알 수 있는 바와 같이 본 발명이 속한 분야의 통상의 지식을 가진 자에 의해 변형이 가능하고 이러한 변형은 본 발명의 범위에 속한다.

발명의 효과

[0216] 상기 본 발명에 따른 데이터 복호방법 및 복호장치, 기록매체 등을 통해 콘텐츠의 무단 복제, 배포 등을 방지할 수 있고, 따라서 안전한 콘텐츠의 제공과 데이터의 효율적 재생이 가능하게 되어 사용자에게 더욱 편리한

기능을 제공하게 되는 장점이 있다.

도면의 간단한 설명

[0001] 도 1은 본 발명의 개념적 이해를 돕기 위해 나타낸 위해 도시한 것이다.

[0002] 도 2는 본 발명의 기록매체로서 광 디스크에 기록되는 파일구조 및 이를 활용하여 특정 타이틀이 재생되는 관계를 도시한 것이다.

[0003] 도 3은 본 발명의 기록매체로서 광 디스크의 기록구조를 도시한 것이다.

[0004] 도 4는 본 발명의 광 기록재생장치의 전체 구성을 도시한 것이다.

[0005] 도 5는 본 발명의 데이터의 암호화 및 복호화에 대한 개념적 이해를 돕기 위해 도시한 것이다.

[0006] 도 6은 본 발명의 데이터 복호방법의 제 1 실시예를 도시한 것이다.

[0007] 도 7은 본 발명의 데이터 복호방법의 제 2 실시예를 도시한 것이다.

[0008] 도 8a은 본 발명의 데이터 복호방법의 제 3 실시예를 도시한 것이다.

[0009] 도 8b은 본 발명의 데이터 복호방법의 제 4 실시예를 도시한 것이다.

[0010] 도 9a는 본 발명의 링크(link)정보를 이용하여 데이터를 복호화하는 방법의 제 1 실시예를 도시한 것이다.

[0011] 도 9b는 본 발명의 링크(link)정보를 이용하여 데이터를 복호화하는 방법의제 2 실시예를 도시한 것이다.

[0012] 도 9c는 본 발명의 링크(link)정보를 이용하여 데이터를 복호화하는 방법의제 3 실시예를 도시한 것이다.

[0013] 도 10은 본 발명에 따른 데이터 복호방법을 도시한 것이다.

[0014] 도 11은 재생되는 데이터가 공유되는 경우 본 발명의 실시예를 도시한 것이다.

[0015] 도 12는 타이틀이 메인패스와 서브패스로 이루어진 경우 본 발명의 실시예를 도시한 것이다.

[0016] ※ 도면의 주요부분에 대한 부호의 설명

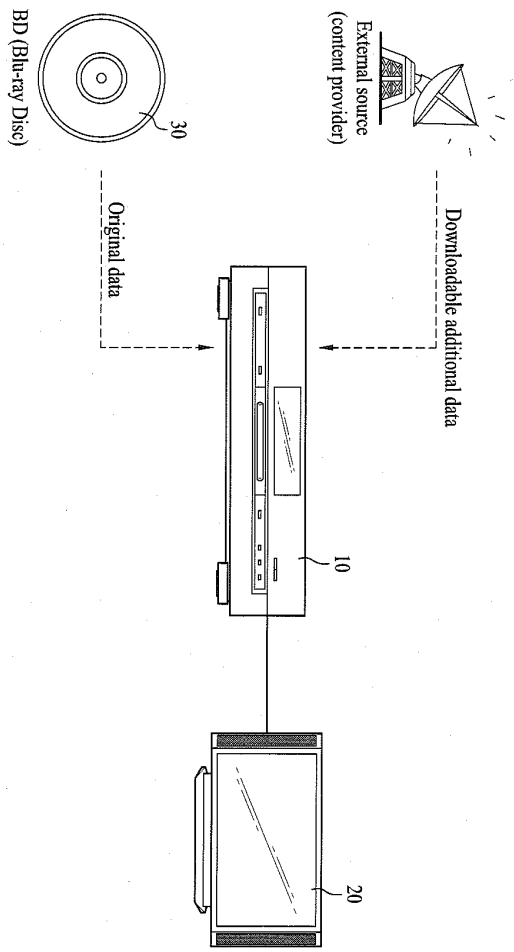
[0017] 11 : 픽업 12 : 제어부

[0018] 13 : 신호처리부 15 : 로컬 스토리지

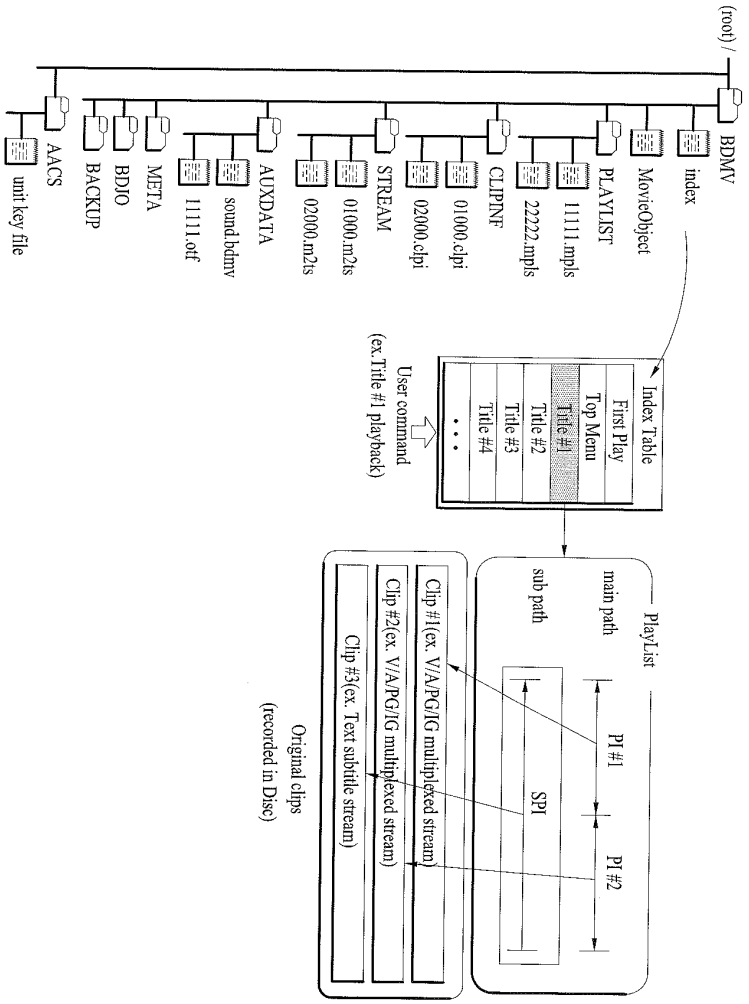
[0019] 17 : 디코더 (Decoder)

도면

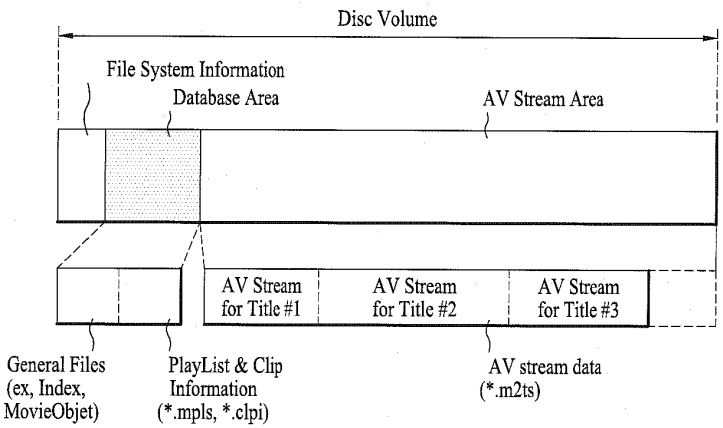
도면1


BD (Blu-ray Disc)
30
External source
(content provider)
Original data
Downloadable additional data
10
20

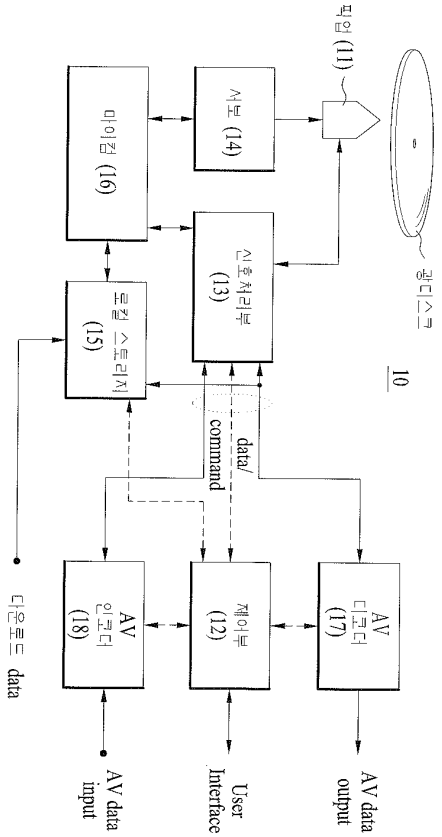
도면2


(root) /
BDMV
index
MovieObject
PLAYLIST
11111.mpls
22222.mpls
CLIPINF
01000.clpi
02000.clpi
STREAM
01000.m2ts
02000.m2ts
AUXDATA
sound.bdmv
11111.otf
META
BDJO
BACKUP
AACS
unit key file
Index Table
First Play
Top Menu
Title #1
Title #2
Title #3
Title #4
User command
(ex.Title #1 playback)
PlayList
main path
sub path
PI #1
PI #2
SPI
Clip #1(ex. V/A/PG/IG multiplexed stream)
Clip #2(ex. V/A/PG/IG multiplexed stream)
Clip #3(ex. Text subtitle stream)
Original clips
(recorded in Disc)

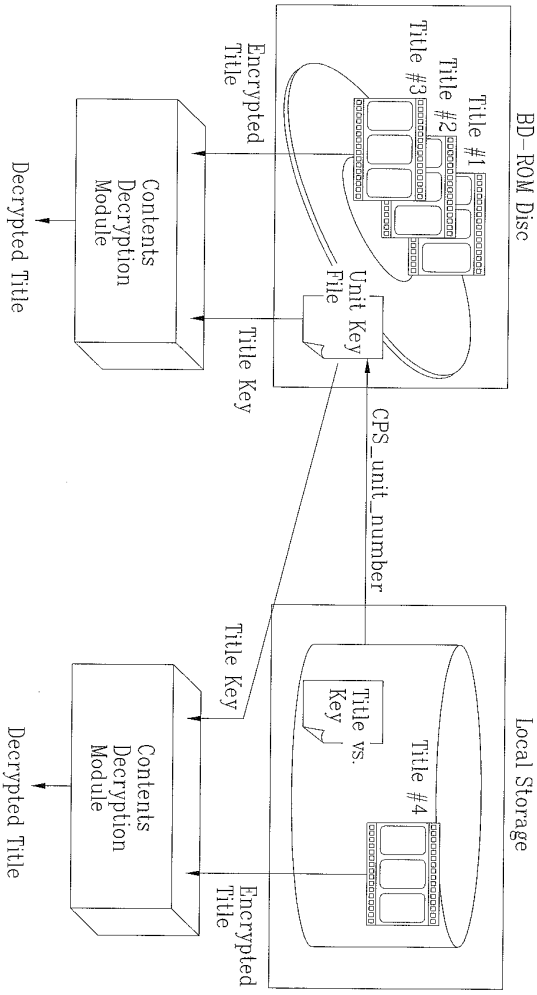
도면3


Disc Volume
File System Information
Database Area
AV Stream Area
AV Stream for Title #1
AV Stream for Title #2
AV Stream for Title #3
General Files (ex, Index, MovieObjet)
PlayList & Clip Information (*.mpls, *.clpi)
AV stream data (*.m2ts)

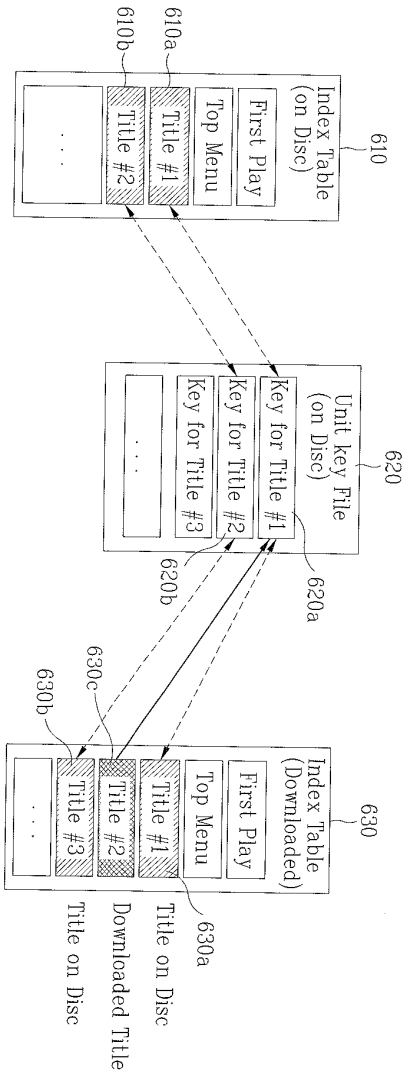
도면4


픽업 (11)
서보 (14)
마이컴 (16)
신호처리부 (13)
로컬 스토리지 (15)
광디스크
10
data/ command
AV 인코더 (18)
제어부 (12)
AV 디코더 (17)
다운로드 data
AV data input
User Interface
AV data output

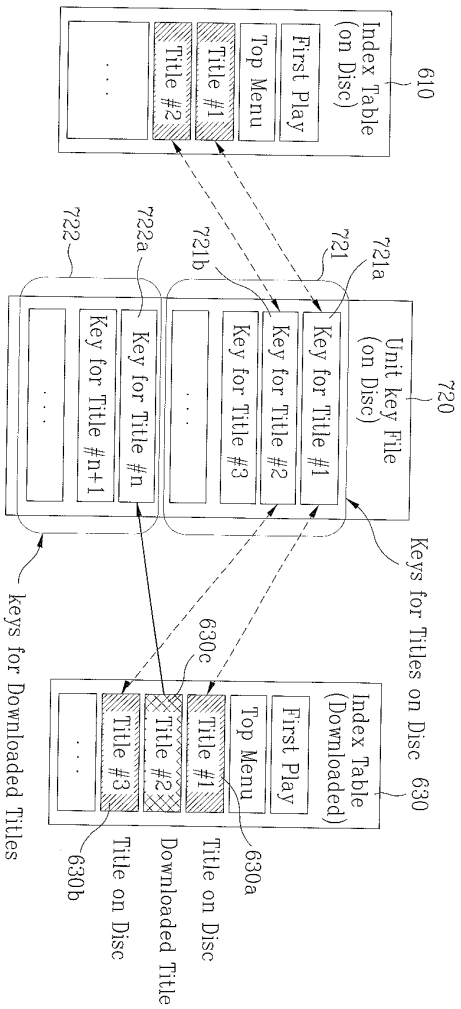
도면5


BD-ROM Disc
Title #1
Title #2
Title #3
Encrypted Title
Contents Decryption Module
Decrypted Title
Unit Key File
Title Key
CPS_unit_number
Local Storage
Title #4
Title vs. Key
Title Key
Contents Decryption Module
Decrypted Title
Encrypted Title

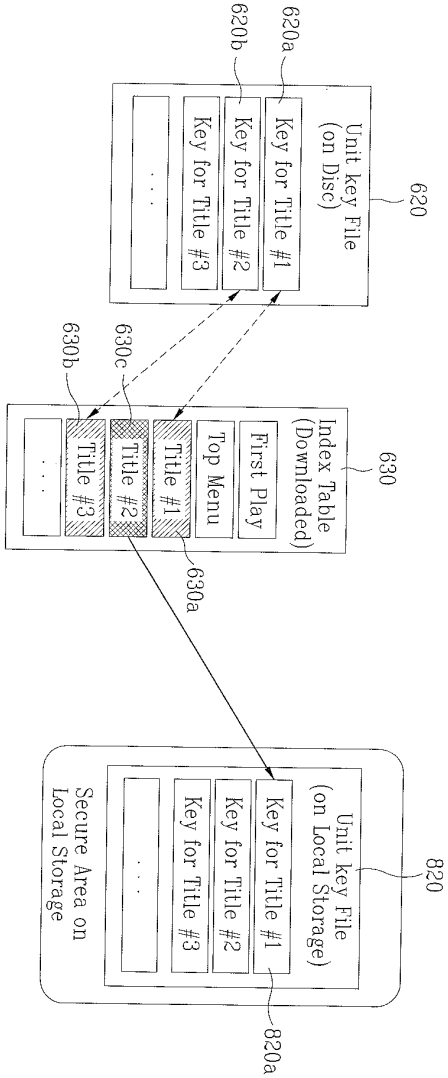
도면6


610b
610a
Index Table (on Disc)
610
Title #2
Title #1
Top Menu
First Play
Unit key File (on Disc)
620
Key for Title #3
Key for Title #2
Key for Title #1
620b
620a
630c
630b
Index Table (Downloaded)
630
Title #3
Title #2
Title #1
Top Menu
First Play
630a
Title on Disc
Downloaded Title
Title on Disc

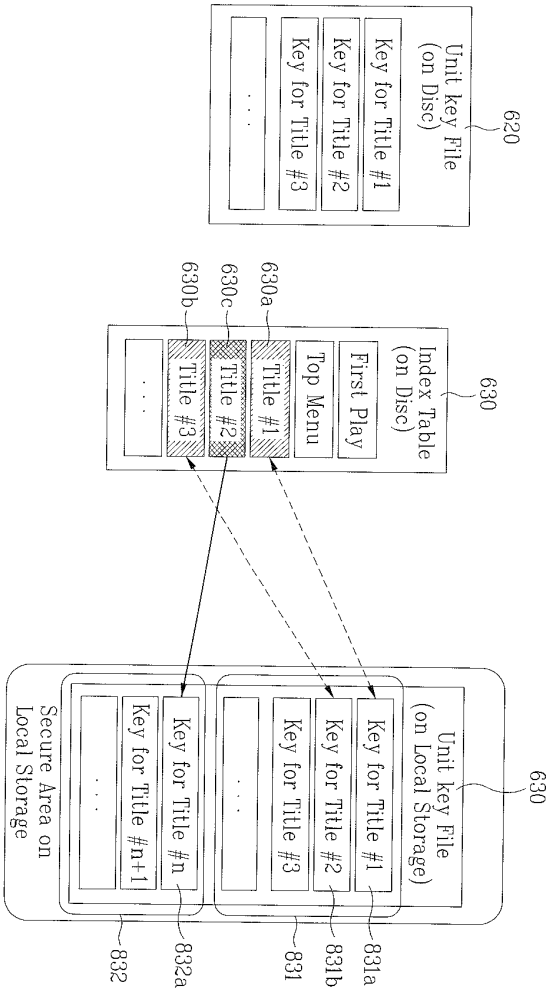
도면7


Index Table (on Disc)
610
First Play
Top Menu
Title #1
Title #2
. . .
Unit key File (on Disc)
720
721
721a
721b
722
722a
Key for Title #1
Key for Title #2
Key for Title #3
Key for Title #n
Key for Title #n+1
. . .
Keys for Titles on Disc
keys for Downloaded Titles
Index Table (Downloaded)
630
630a
630b
630c
First Play
Top Menu
Title #1
Title #2
Title #3
. . .
Title on Disc
Downloaded Title
Title on Disc

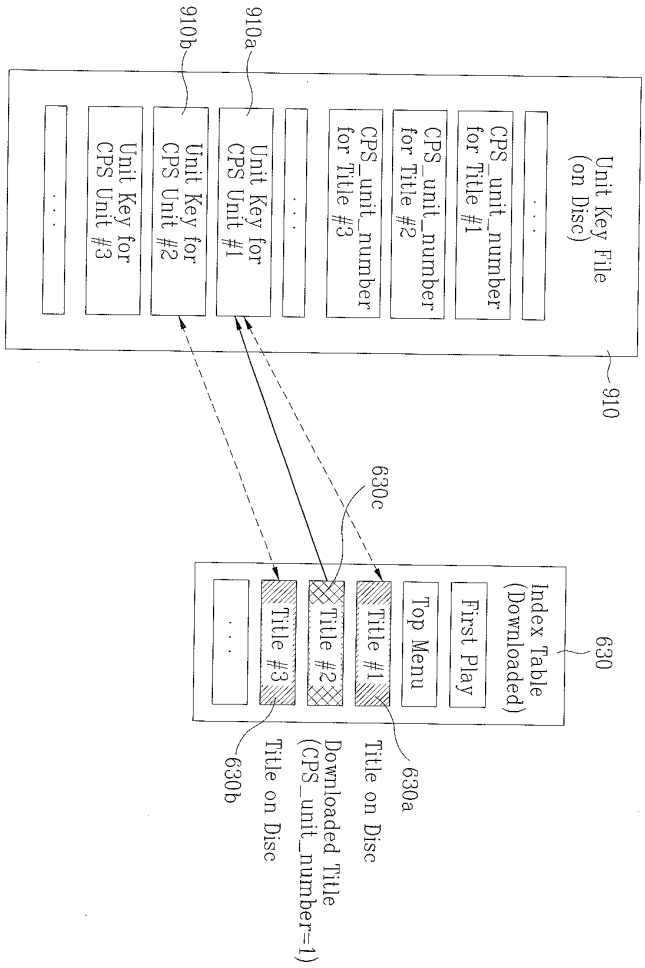
도면8a


620a
620b
Unit key File
(on Disc)
620
Key for Title #1
Key for Title #2
Key for Title #3
630b
630c
Index Table
(Downloaded)
630
First Play
Top Menu
Title #1
Title #2
Title #3
630a
820
Unit key File
(on Local Storage)
Key for Title #1
Key for Title #2
Key for Title #3
Secure Area on
Local Storage
820a

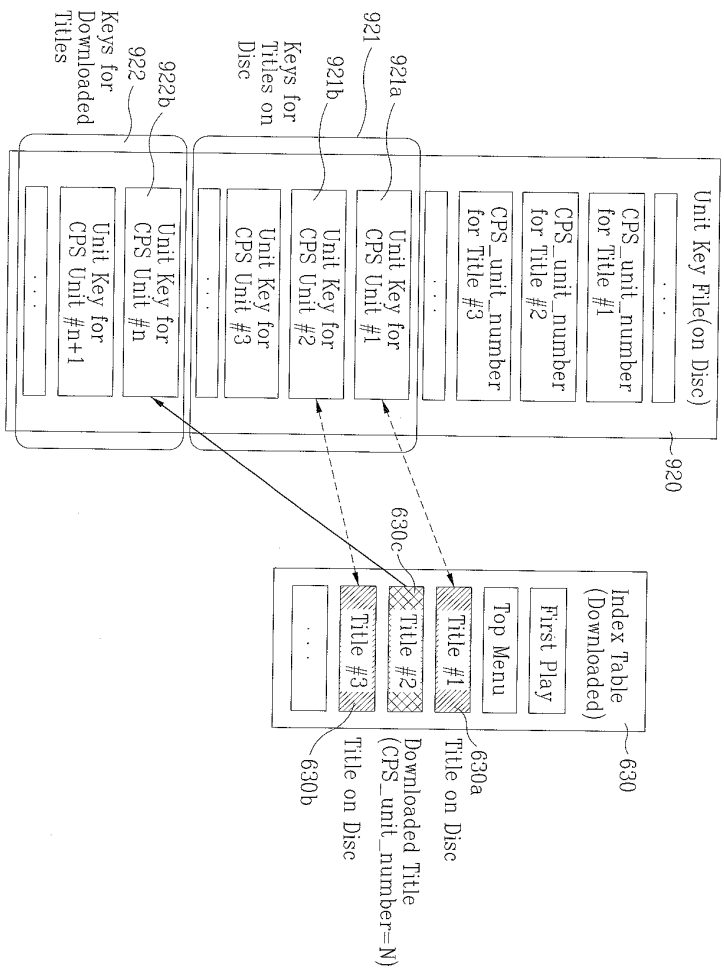
도면8b


Unit key File
(on Disc)
620
Key for Title #1
Key for Title #2
Key for Title #3
Index Table
(on Disc)
630
First Play
Top Menu
Title #1
Title #2
Title #3
630a
630c
630b
Unit key File
(on Local Storage)
630
Key for Title #1
Key for Title #2
Key for Title #3
831a
831b
831
Secure Area on
Local Storage
Key for Title #n
Key for Title #n+1
832a
832

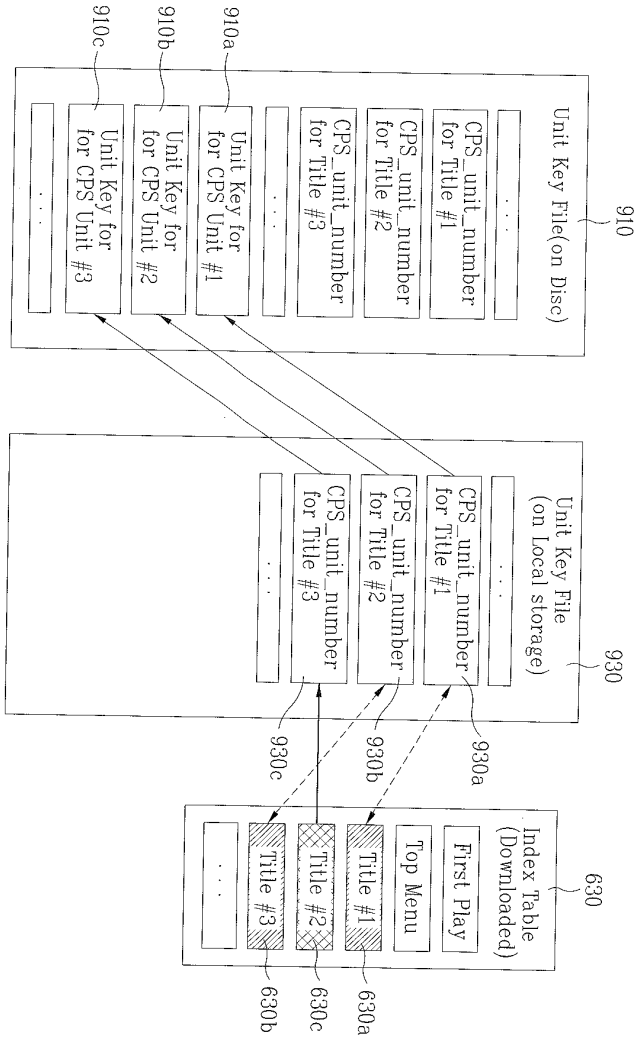
도면9a


Unit Key File
(on Disc)
CPS_unit_number
for Title #1
CPS_unit_number
for Title #2
CPS_unit_number
for Title #3
Unit Key for
CPS Unit #1
Unit Key for
CPS Unit #2
Unit Key for
CPS Unit #3
910
910a
910b
Index Table
(Downloaded)
First Play
Top Menu
Title #1
Title #2
Title #3
630
630a
630b
630c
Title on Disc
Downloaded Title
(CPS_unit_number=1)
Title on Disc

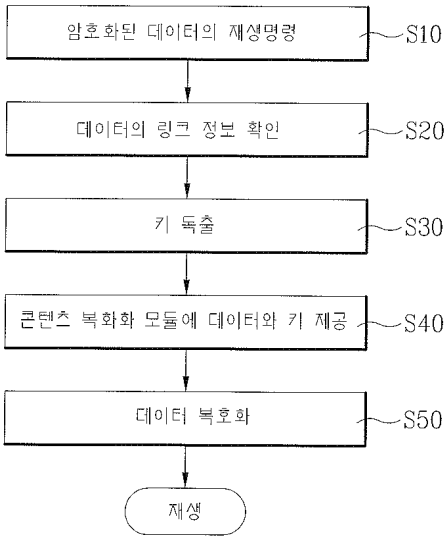
도면9b


Unit Key File(on Disc)
CPS_unit_number for Title #1
CPS_unit_number for Title #2
CPS_unit_number for Title #3
Unit Key for CPS Unit #1
Unit Key for CPS Unit #2
Unit Key for CPS Unit #3
Unit Key for CPS Unit #n
Unit Key for CPS Unit #n+1
920
921
921a
921b
Keys for Titles on Disc
922
922b
Keys for Downloaded Titles
Index Table (Downloaded)
First Play
Top Menu
Title #1
Title #2
Title #3
630
630a
Title on Disc
630b
Title on Disc
630c
Downloaded Title (CPS_unit_number=N)

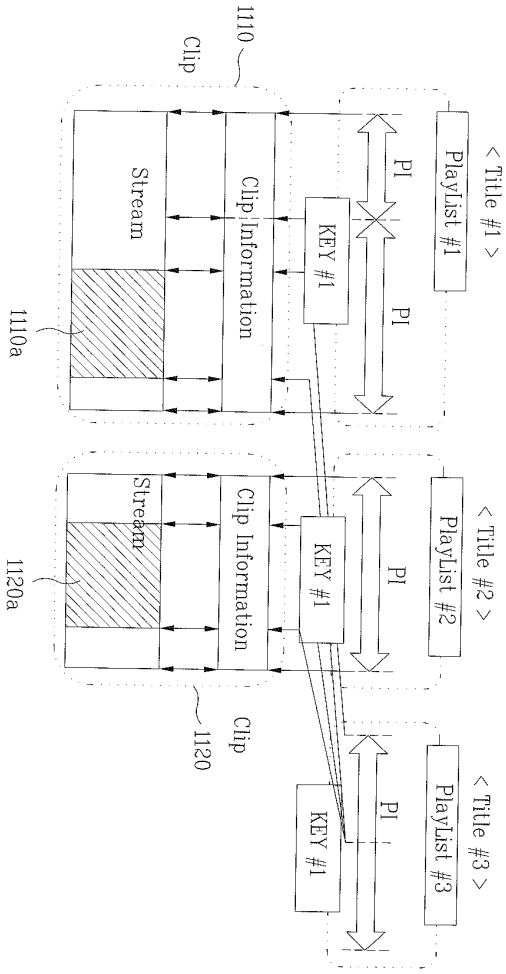
도면9c


Unit Key File(on Disc)
910
CPS_unit_number for Title #1
CPS_unit_number for Title #2
CPS_unit_number for Title #3
Unit Key for CPS Unit #1
Unit Key for CPS Unit #2
Unit Key for CPS Unit #3
910a
910b
910c
Unit Key File (on Local storage)
930
CPS_unit_number for Title #1
CPS_unit_number for Title #2
CPS_unit_number for Title #3
930a
930b
930c
Index Table (Downloaded)
630
First Play
Top Menu
Title #1
Title #2
Title #3
630a
630c
630b

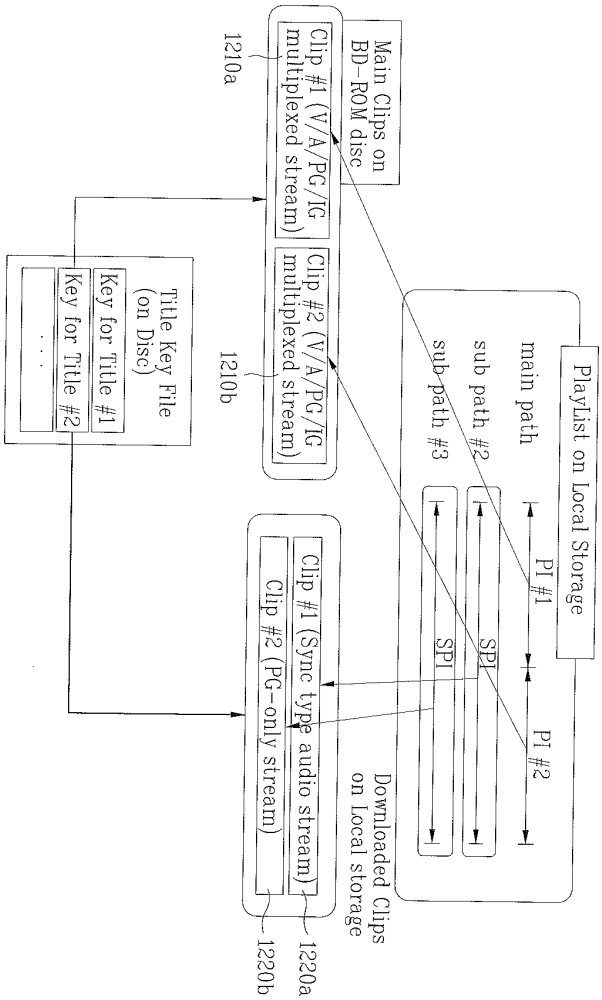
도면10


암호화된 데이터의 재생명령
S10
데이터의 링크 정보 확인
S20
키 독출
S30
콘텐츠 복화화 모듈에 데이터와 키 제공
S40
데이터 복호화
S50
재생

도면11


1110
Clip
Stream
Clip Information
1110a
PI
KEY #1
PI
< Title #1 >
PlayList #1
1120a
Stream
Clip Information
KEY #1
PI
< Title #2 >
PlayList #2
1120
Clip
KEY #1
PI
< Title #3 >
PlayList #3

도면12


PlayList on Local Storage
main path
sub path #2
sub path #3
PI #1
PI #2
SPI
SPI
SPI
Main Clips on BD-ROM disc
Clip #1 (V/A/PG/IG multiplexed stream)
Clip #2 (V/A/PG/IG multiplexed stream)
1210a
1210b
Title Key File (on Disc)
Key for Title #1
Key for Title #2
Downloaded Clips on Local storage
Clip #1 (Sync type audio stream)
Clip #2 (PG-only stream)
1220a
1220b