

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

| | | |
|-----------------------------|-----------|-------------|
| (51) Int. Cl. | (45) 공고일자 | 2006년08월03일 |
| <i>G06F 15/00</i> (2006.01) | (11) 등록번호 | 10-0608585 |
| | (24) 등록일자 | 2006년07월27일 |

| | | | |
|-----------|-----------------|-----------|-----------------|
| (21) 출원번호 | 10-2004-0072555 | (65) 공개번호 | 10-2006-0005284 |
| (22) 출원일자 | 2004년09월10일 | (43) 공개일자 | 2006년01월17일 |

(30) 우선권주장 60/586,724 2004년07월12일 미국(US)

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 권문상
서울특별시 관악구 봉천동 1708 두산아파트 104동 1403호

오윤상
서울특별시 강남구 도곡2동 타워팰리스아파트 C-2901

정경임
경기도 성남시 분당구 정자동 88번지 느티마을 주공3단지 310동 2402호

(74) 대리인 김동진
정상빈

(56) 선행기술조사문헌
JP03202936 A KR1020030091664 A
KR1020040039952 A US6105103 A
WO조사보고서
* 심사관에 의하여 인용된 문헌

심사관 : 이영수

(54) 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리객체를 검색하는 방법 및 장치

요약

본 발명은 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법 및 장치에 관한 것이다.

본 발명의 일 실시예에 따른 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법은 이동형 저장 장치에 접근하는 단계, 상기 이동형 저장 장치에 객체 식별자를 송신하는 단계, 상기 이동형 저장 장치로부터 상기 객체 식별자에 의하여 검색된 제 1 객체의 위치 정보를 수신하는 단계, 상기 제 1 객체의 위치 정보를 상기 객체 식별자와 함께 저장하는 단계 및 상기 제 1 객체의 위치 정보를 사용하여 상기 이동형 저장 장치에 상기 제 1 객체 위치 정보와 상기 제 1 객체에 대하여 수행되는 작업 정보를 송신하는 단계를 포함한다.

대표도

도 5

색인어

이동형 저장 장치, 보안 멀티미디어 카드, 객체 위치, 검색

명세서

도면의 간단한 설명

도 1은 본 발명의 일 실시예에 따른 상호 인증의 과정을 보여주는 도면이다.

도 2는 본 발명의 일 실시예에 따른 호스트 디바이스와 이동형 저장 장치의 구성과 상호작용을 보여주는 블록도이다.

도 3은 본 발명의 일 실시예에 따른 객체 테이블을 나타내는 블록도이다.

도 4는 본 발명의 일 실시예에 따른 암호학적 방식으로 식별자를 해쉬 함수를 취하여 저장한 테이블을 보여준다.

도 5는 본 발명의 일 실시예에 따른 호스트 디바이스가 이동형 저장 장치에 저장된 객체에 최초로 접근하는 단계를 보여주는 블록도이다.

도 6은 본 발명의 일 실시예에 따른 저장부에 객체 식별자와 객체 위치정보가 저장된 테이블이다.

도 7은 본 발명의 일 실시예에 따른 호스트 디바이스가 객체 식별자와 객체 위치 정보를 이용하여 이동형 저장 장치에 저장된 객체에 접근하는 과정을 보여주는 블록도이다.

<도면의 주요 부분에 대한 부호의 설명>

100 : 이동형 저장 장치 500 : 호스트 디바이스

130 : 객체 정보 저장부 540 : 저장부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법 및 장치에 관한 것이다.

최근에 디지털 저작권 관리(Digital Rights Management; 이하, "DRM"이라 함)에 관한 연구가 활발하며, DRM을 적용한 상용 서비스들이 도입되었거나 도입 중에 있다. DRM이 도입되어야 하는 이유는 디지털 콘텐츠가 갖는 여러가지 특성으로부터 도출할 수 있다. 디지털 콘텐츠는 아날로그 데이터와는 달리 손실이 없이 복제가 가능하다는 특성과, 재사용 및 가공, 배포가 용이한 것에 반해 그 제작에 많은 비용과 노력 및 시간을 필요로 한다는 특성을 가진다. 따라서 디지털 콘텐츠의 무단 복제 및 배포가 용인될 경우에, 이는 디지털 콘텐츠 제작자의 이익을 침해하고, 디지털 콘텐츠 제작자의 창작 의욕은 꺾이게 될 것이고 이는 디지털 콘텐츠 산업의 활성화에 큰 저해요소가 된다.

디지털 콘텐츠를 보호하고자 하는 노력은 과거에도 있었으나, 과거에는 주로 디지털 콘텐츠 무단접근 방지에 중점을 두어 디지털 콘텐츠에 대한 접근(access)은 대가를 지불한 일부 사람에게만 허용되었다. 그렇지만 대가를 지불한 사람이 고의적으로 디지털 콘텐츠를 제3자에게 배포할 경우에 제3자는 대가를 지불하지 않고도 디지털 콘텐츠를 사용할 수 있게 된

다. 이러한 문제점을 해결하고자 DRM이라는 개념이 도입되었다. DRM은 어떤 암호화된 디지털 콘텐츠에 대한 접근을 누구에게나 무제한으로 허용하지만, 암호화된 디지털 콘텐츠를 복호화하여 실행시키려면 권리 객체(Rights Object)라는 라이선스가 있어야 한다. 따라서, DRM을 적용하면 디지털 콘텐츠를 기존과는 달리 효과적으로 보호할 수 있게 된다.

휴대용 저장장치는 휴대폰, 컴퓨터, 디지털 카메라등 여러 디지털 기기의 자료를 저장하고 이동할 수 있도록 하는 탈, 부착이 가능한 장치로서, 데이터를 저장하는 저장공간과 연산 및 제어를 담당하는 부분으로 구성된 것이다. 이러한 휴대용 저장장치의 하나인 멀티미디어 카드라 불리는 MMC(MultiMedia Card)는 종래의 하드 디스크나 콤팩트 디스크가 가지는 한계를 벗어나, 다양한 종류의 디지털 기기에서 사용할 수 있도록 멀티미디어 데이터를 저장하는 역할을 하고 있다. 또한 이 카드는 기존의 저장 매체에는 없는 연산부를 가지고 있어서, 단순한 데이터 저장이 아닌, 제어 등이 가능하게 되어 대용량의, 다양한 멀티미디어 데이터를 수용하기에 적합하다. 최근 이 멀티미디어 카드에 보안성의 기능을 추가하여 디지털 콘텐츠의 저장 및 송수신에 있어서의 보안과 저작권 보호가 가능한 보안 멀티미디어 카드(SecureMMC)가 개발되면서, 디지털 콘텐츠에 대한 저작권 관리가 저장 장치와 디지털 기기에서 가능하게 되었다. 이하 디지털 카메라, 휴대폰, 컴퓨터, 디지털 캠코더 등의 디지털 기기를 호스트 디바이스로 통칭하기로 한다.

최근의 플래쉬 메모리를 비롯한 메모리 카드들은 이동형 저장 장치로 주목받고 있다. 이들 이동형 저장 장치들은 DRAM 또는 SRAM과 달리, 전원의 공급 없이도 데이터를 보존할 수 있다는 장점을 가지고 있다. 그러나, 데이터의 입출력 속도가 상기 DRAM 보다 느리다는 단점이 있다.

이동형 저장 장치에 저장된 권리 객체는 콘텐츠의 재생시 항상 참조하게 되는 정보로, 여러 번의 읽기, 쓰기, 또는 수정의 오퍼레이션을 필요로 한다. 따라서 이러한 잦은 오퍼레이션을 효율적으로 수행하기 위해서는 특정 권리 객체를 검색하는데 들이는 시간을 줄여야 한다.

종래에, 한국 공개특허(특2002-0020104)에서는 메모리 카드의 입출력 속도를 높이기 위해 SRAM을 통해 캐쉬기능을 제공하는 방법이 제시되었다. 이 출원에서 SRAM은 메모리 카드가 디지털 장치와 결합될 경우 초기화되어 이후 수행되는 읽기 및 쓰기 오퍼레이션에서 특정 데이터를 저장하는 캐쉬의 역할을 하게 하여, 입출력 속도를 증가시키고 있다.

이는 이미 검색한 데이터를 다시 찾을 경우의 입출력 속도를 증가시킬 수 있으나, 데이터 검색에서 일어나는 지연 시간을 줄일 수는 없다.

특히, 권리 객체를 저장하는 DRM 시스템하의 이동형 저장 장치는 특정 권리 객체에 대한 잦은 입출력 오퍼레이션과 함께, 각 권리 객체들을 여러 조건으로 검색하는 오퍼레이션도 자주 일어나기 때문에, 입출력 속도와 검색 속도를 높이는 방법이 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명의 기술적 과제는 이동형 저장 장치에 저장된 객체를 신속하게 검색하여 객체를 이용하는 속도를 증가시키는데 있다.

본 발명의 다른 기술적 과제는 동일 객체 식별자의 객체들을 반복적으로 사용하는 경우 객체를 검색하는 시간을 줄이는 데 있다.

본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 구성 및 작용

본 발명은 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법 및 장치에 관한 것이다.

본 발명의 일 실시예에 따른 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법은 이동형 저장 장치에 접근하는 단계, 상기 이동형 저장 장치에 객체 식별자를 송신하는 단계, 상기 이동형 저장 장치로부터 상기 객체 식별자에 의하여 검색된 제 1 객체의 위치 정보를 수신하는 단계, 상기 제 1 객체의 위치 정보를 상기 객체 식별자와 함께 저장하는 단계 및 상기 제 1 객체의 위치 정보를 사용하여 상기 이동형 저장 장치에 상기 제 1 객체 위치 정보와 상기 제 1 객체에 대하여 수행되는 작업 정보를 송신하는 단계를 포함한다.

본 발명의 다른 실시예에 따른 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법은 호스트 디바이스에 접근하는 단계, 상기 호스트 디바이스로부터 객체 식별자를 수신하는 단계, 객체와 상기 객체 식별자가 저장된 저장부에서 상기 객체 식별자를 가지는 객체의 위치 정보를 검색하여 상기 호스트 디바이스로 송신하는 단계, 상기 호스트 디바이스로부터 상기 객체의 위치 정보와 상기 객체에 대하여 수행되는 작업 정보를 수신하는 단계 및 상기 수신한 객체의 위치 정보를 이용하여 상기 저장부의 객체에 직접 접근하여 상기 작업 정보에 따라 작업을 수행하는 단계를 포함한다.

본 발명의 일 실시예에 따른 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치는 이동형 저장 장치에 객체 식별자를 송신하여 상기 객체 식별자의 제 1 객체의 위치 정보를 수신하는 어플리케이션부, 상기 객체 식별자와 상기 제 1 객체의 위치 정보를 저장하는 저장부를 포함하며, 상기 어플리케이션부는 상기 저장된 객체 식별자를 검색하여 상기 저장된 제 1 객체의 위치 정보와 상기 제 1 객체에 대하여 수행되는 작업 정보를 송신한다.

본 발명의 일 실시예에 따른 이동형 저장 장치는 객체와 객체 식별자를 저장하는 객체 정보 저장부 및 호스트 디바이스가 송신한 객체 식별자를 수신하는 어플리케이션부를 포함하며, 상기 어플리케이션부는 상기 객체 정보 저장부에서 상기 객체 식별자를 가지는 객체의 위치 정보를 검색하여 상기 호스트 디바이스로 송신하며, 상기 호스트 디바이스로부터 객체의 위치 정보와 객체에 대하여 수행되는 작업 정보를 수신하여 상기 위치 정보를 이용하여 상기 저장부의 객체에 직접 접근하여 상기 작업 정보에 따라 작업을 수행한다.

본 명세서에서 사용하게 되는 용어를 정의하면 다음과 같다.

- 호스트 디바이스

본 명세서에서 사용하는 호스트 디바이스는 이동형 저장 장치와 결합하여 이동형 저장 장치에 저장된 권리 객체를 이용하는 장치를 의미한다. 휴대폰, PDA 등의 휴대용 멀티미디어 기기가 될 수 있고, 휴대용이 아닌 컴퓨터, 디지털 TV와 같은 멀티미디어 기기도 포함한다. 디바이스 혹은 호스트로도 명명될 수 있다.

- 이동형 저장 장치

본 명세서에서 사용하는 이동형 저장 장치는 플래시 메모리와 같이 읽고 쓰고 지울 수 있는 성질을 갖는 비휘발성 메모리를 포함하고 있으며, 디바이스에 연결이 가능한 저장 장치를 의미한다. 이러한 저장 장치의 예로는 스마트 미디어, 메모리 스틱, CF카드, XD카드, 멀티미디어 카드, USB 저장 장치 등이 있으며, 이하 상세한 설명에서는 보안 멀티미디어 카드를 중심으로 설명한다.

- 권리 객체 (Rights Object), 객체

권리 객체는 디지털 저작물에 대한 권리 내용을 가지게 되며, 디지털 저작물에 대한 재생(Play), 디스플레이(Display), 실행(Execute), 인쇄(Print), 전송(Export: 복사, 이동) 혹은 열람 등의 권한을 설정하는 부분이다. 디바이스와 휴대용 멀티미디어 간에 DRM을 수행하기 위해서는 콘텐츠에 대한 권리 부여 여부의 정보를 가지는 권리 객체의 사용이 필요하다. 한편 본 명세서에서 사용하는 객체는 상기 권리 객체를 의미할 수도 있고, 상기 권리 객체를 다수로 나눈 하나를 의미할 수 있다. 이는 권리 객체의 크기가 클 경우, 특정 포맷으로 나누어 여러 개로 관리할 수 있는데, 본 명세서에서의 객체는 상기의 경우도 포함한다.

- 객체 정보 저장부

이동형 저장 장치내에서 객체를 저장한다. 이동형 저장 장치 내의 저장부 또는 저장 매체이거나 그 일부일 수 있다. 또한 객체를 찾기 위한 식별자 정보도 함께 저장하며, 객체가 저장된 위치를 포함할 수 있다. 객체 정보 저장부는 여러 형식으로 저장될 수 있으며, 본 명세서의 일 실시예로는 테이블 형식으로 표현하고자 한다. 이하, 본 명세서에서 언급하게 될 객체 테이블은 객체 정보 저장부의 일 실시예이며, 이에 한정되는 것은 아니다.

객체 테이블에는 각각의 권리 객체와 객체에 대한 정보인 위치 정보, 식별자 필드, 메타정보 등을 포함할 수 있다. 객체의 위치정보는 해당 객체가 보관되어 있는 위치를 의미하며, 이 위치를 가지고 이동형 저장 장치에 저장된 객체를 읽고 쓰는 등의 작업을 수행할 수 있다.

객체 메타정보는 객체를 보관할 때 필요한 상태 정보를 기록하며, 객체 사상 테이블은 객체 테이블에 저장되어진 객체들의 상태를 보관할 수 있다.

- 객체 식별자

객체 식별자는 객체를 검색하고 구별하는 기준이 된다. 하나의 객체를 식별하는 식별자는 다수 존재할 수 있다. 예를 들어 특정 콘텐츠의 권리를 저장하고 있는 객체의 경우 해당 콘텐츠 식별자(Content ID)가 객체를 식별하는 식별자가 될 수 있다. 또한 콘텐츠 제작자의 이름 또는 제작자의 식별자가 객체를 식별하는 식별자가 될 수 있다. 이외에도, 해당 객체가 해당 콘텐츠의 재생에 관한 권리를 제공하는지, 혹은 해당 콘텐츠의 복사 또는 이동에 대한 권리를 제공하는지를 식별하는 정보로 이루어질 수 있다. 또한 객체의 사용 기간에 대한 정보를 식별자로 하여 사용기간이 만료한 객체를 검색할 수 있다. 객체의 식별자는 객체를 살펴보기 않고도 해당 조건에 해당하는 객체를 검색하기 위한 것이며, 객체를 검색하기 위해 필요한 정보이므로, 다양하게 정의될 수 있다. 물론, 각각의 객체에 주어지는 권리 객체 식별자(Rights Object ID) 역시 객체의 식별자가 될 수 있다.

- 객체 사상 정보 저장부

객체 정보 저장부에 저장된 객체의 상태를 보여준다. 객체 사상 정보 저장부의 일 실시예로 객체의 저장 여부만을 나타내기 위해 비트의 연속으로 구현할 수 있으며, 테이블로 구현하여 보다 많은 정보를 저장할 수도 있다. 본 명세서의 일 실시예로는 테이블 형식으로 구현하고자 하며, 이에 한정되는 것은 아니다. 이하 객체 사상 테이블이라 칭하고자 한다.

- 호스트 디바이스와 이동형 저장장치의 접근

본 명세서에서의 호스트 디바이스와 이동형 저장장치는 유선 또는 무선을 통해 결합된다. 따라서, 무선의 결합까지 포괄하여 호스트 디바이스와 이동형 저장장치가 접근한다고 볼 수 있다. 이는 호스트 디바이스와 이동형 저장장치가 유무선을 통해 데이터를 송수신하는 것을 의미하며, 물리적으로 부착되거나 결합되는 것만을 의미하지 않는다. 즉, 물리적인 부착 또는 결합을 포함하며, 물리적 접촉 없이 데이터를 송수신하는 상태도 포함한다. 최근 무선 기술의 발달과 함께, 무선을 통한 데이터 송수신이 다양하게 증가하고 있으며, 본 명세서에서의 호스트 디바이스와 이동형 저장장치간의 데이터 전송은 무선을 통한 이동형 저장장치와 호스트 디바이스간의 데이터 전송을 포함한다.

본 실시예에서 사용되는 '~부'라는 용어, 즉 '~모듈' 또는 '~테이블' 등은 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 기능들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 모듈은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 모듈들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다. 뿐만 아니라, 구성요소들 및 모듈들은 디바이스 또는 보안 멀티미디어카드 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.

도 1은 본 발명의 일 실시예에 따른 상호 인증의 과정을 보여주는 도면이다. 도 1에서는 이동형 저장 장치의 일 실시예로 보안 멀티미디어 카드(100)를 가지고 인증 과정을 설명한다. 상호 인증 과정은 호스트 디바이스(500)와 보안 멀티미디어 카드(100)가 서로가 정당한 장치임을 확인하고 양자간에 세션키 생성을 위한 랜덤번호를 교환하는 과정이고, 상호 인증 과정을 통해 얻은 랜덤번호를 이용하여 세션키를 생성할 수 있다. 도 1에서 화살표의 위에 있는 단계는 상대 장치에게 어떤 동작을 요구하는 명령을 의미하고 화살표 아래는 명령에 따른 파라미터나 이동되는 데이터를 의미한다. 일 실시예에서 상호 인증과정의 모든 명령은 디바이스(500)가 하도록 하고 보안 멀티미디어 카드(100)는 명령에 따른 동작을 수행하도록 한다. 예를 들면 상호 인증 응답(S50)이라는 명령은 디바이스(500)가 보안 멀티미디어 카드(100)로 보내면 보안 멀티미디어 카드(100)가 명령을 받고 디바이스에게 인증서M과 암호화된 랜덤번호M을 보낸다. 다른 실시예에서 명령은 디바이스(500)와 보안 멀티미디어 카드(100) 모두가 할 수 있다. 이 경우에 상호 인증 응답(S50)은 보안 멀티미디어 카드(100)가 디바이스(500)에게 보내면서 인증서M과 암호화된 랜덤번호M을 함께 보낼 수 있다. 자세한 상호 인증 과정을 설명한다.

디바이스(500)에서 보안 멀티미디어 카드(100)로 상호 인증을 요청한다(S10). 상호 인증 요청을 하면서 디바이스는 보안 멀티미디어 카드가 디바이스(500)가 갖고 있는 디바이스 공개키(PubKeyD)를 보낸다. 일 실시예에 있어서 S10 단계에서 디바이스 공개키(PubKeyD)는 디바이스(500)에 대하여 인증기관(Certification Authority)이 발행한 디바이스 인증서

(CertD)를 보낸다. 디바이스 인증서(CertD)는 디바이스 아이디와 디바이스 공개키(PubKeyD)가 포함되어 있고 인증기관의 전자서명이 있다. 디바이스 인증서(CertD)를 수신한 보안 멀티미디어 카드(100)는 디바이스(500)가 정당한 디바이스 인증서를 확인할 수 있고, 디바이스 공개키(PubKeyD)를 얻을 수 있다.

보안 멀티미디어 카드(100)는 인증서 폐기 목록(Certificate Revocation List; 이하, "CRL"이라 함)을 사용하여 디바이스 인증서(CertD)가 유효한 것인지를 확인한다(S20). CRL에 등록된 디바이스의 인증서일 경우라면 보안 멀티미디어 카드(100)는 디바이스(500)와의 상호 인증을 거부할 수 있다. CRL에 등록되지 않은 디바이스의 인증서일 경우에 보안 멀티미디어 카드(100)는 디바이스 인증서(CertD)를 통해 디바이스 공개키(PubKeyD)를 얻는다.

그리고 나서 보안 멀티미디어 카드(100)는 랜덤 번호M을 생성한다(S30). 생성된 랜덤번호M는 디바이스 공개키(PubKeyD)로 암호화한다(S40). 그리고 나서 디바이스(500)에 의한 상호 인증 응답명령을 수신하거나, 보안 멀티미디어 카드(100)가 디바이스(500)에 상호 인증 응답명령을 보내며 상호 인증 응답과정이 수행된다(S50). 상호 인증 응답과정에서 보안 멀티미디어 카드(100)는 디바이스에 보안 멀티미디어 카드 공개키(PubKeyM)와 암호화된 랜덤번호M을 보낸다. 일 실시예에 있어서, 보안 멀티미디어 카드 공개키(PubKeyM) 대신에 보안 멀티미디어 카드 인증서(CERTM)를 보낸다. 다른 실시예에 있어서, 멀티미디어카드(100)는 보안 멀티미디어 카드 인증서(CERTM)와 암호화된 랜덤번호M와 더불어 보안 멀티미디어 카드의 전자서명(SigM)을 더 포함하여 디바이스(500)에게 보낸다.

디바이스(500)는 보안 멀티미디어 카드 인증서(CERTM)와 암호화된 랜덤번호M를 수신하고, 인증서 확인을 통해 보안 멀티미디어 카드(100)가 정당하다는 것을 확인하고 보안 멀티미디어 카드 공개키(PubKeyM)를 얻고 암호화된 랜덤번호M를 디바이스 개인키(PrivKeyD)로 복호화하여 랜덤번호M를 얻는다(S60). 그리고 나서 디바이스(500)는 랜덤번호D를 생성한다(S70). 생성된 랜덤번호D는 보안 멀티미디어 카드 공개키(PubKeyM)로 암호화한다(S80). 그리고 나서 상호 인증 종결 과정(S90)이 수행되는데, 상호 인증 종결 과정(S90)에서 디바이스(500)는 보안 멀티미디어 카드(100)에 암호화된 랜덤번호D를 전송한다. 일 실시예에 있어서, 디바이스(500)는 암호화된 랜덤번호D와 더불어 디바이스의 전자서명(SigD)을 더 포함하여 보안 멀티미디어 카드(100)에게 보낸다.

보안 멀티미디어 카드(100)는 암호화된 랜덤번호D를 수신하여 복호화한다(S100). 이에 따라 디바이스(500)와 보안 멀티미디어 카드(100)간에는 서로가 생성한 랜덤번호를 알 수 있게 된다. 본 실시예에서 디바이스(500)와 보안 멀티미디어 카드(100) 양자 모두에서 랜덤번호를 생성하여 사용함으로써 랜덤성을 크게 높일 수 있게 되고 안전한 상호 인증이 가능하게 된다. 즉, 어느 한쪽에서 랜덤성이 약하더라도 다른 한쪽에서 랜덤성을 보충할 수 있기 때문이다.

도 2는 본 발명의 일 실시예에 따른 호스트 디바이스와 이동형 저장 장치의 구성과 상호작용을 보여주는 블록도이다.

호스트 디바이스(500)와 이동형 저장 장치(100)는 서로 결합된 상태이다. 이는 유선으로 결합되는 것만을 의미하는 것이 아니라, 무선으로도 결합될 수 있다.

호스트 디바이스(500)는 사용자와의 입출력을 위한 인터페이스(User Interface)(510)를 가지고 있다. 사용자 인터페이스(510)을 통해 사용자는 특정 콘텐츠의 재생, 복사, 이동 등을 요구할 수 있으며, 이에 따른 권리 객체의 재생, 복사, 이동에 대한 정보를 필요로 할 수 있다. 그리고, 객체를 저장하는 저장부(540)가 존재한다. 호스트 어플리케이션(550)은 이동형 저장 장치(100)에 권리 객체에 대한 정보를 요구하는 작업을 수행한다. 송수신부(590)는 이동형 저장 장치(100)와 데이터를 송수신하며, 인증부(580)는 도 1에서 살펴본 인증 과정 및 상기 데이터를 암호화 또는 복호화 하는 작업을 한다.

이동형 저장 장치(100)는 저장매체 어플리케이션(150)과 객체 사상 테이블(140), 그리고 객체 테이블(130)로 구성되어 있다. 저장매체 어플리케이션(150)은 호스트 디바이스(500)의 요청에 따라 객체를 읽거나 쓰는 등의 작업을 수행한다. 송수신부(190)는 호스트 디바이스(500)와 데이터를 송수신하며, 인증부(180)는 도 1에서 살펴본 인증 과정 및 상기 데이터를 암호화 또는 복호화 하는 작업을 한다.

도 2에서 호스트 디바이스(500)와 이동형 저장 장치(100)의 동작은 다음과 같다.

호스트 디바이스와 이동형 저장 장치가 결합시 도 1에서 살펴본 바와 같이 인증 과정을 거친다. 이는 각 장치내에 존재하는 인증부(180, 580)을 통해 이루어진다.

상기 인증이 완료하면 호스트 디바이스와 이동형 저장 장치는 상기 인증 절차에서 생성된 세션키를 이용하여 송수신 하는 데이터를 암호화 하거나 복호화 한다(12, 14). 그리고 호스트 어플리케이션과 저장 매체 어플리케이션은 송수신부를 통해 데이터를 주고받는다(11, 13).

사용자 인터페이스(510)가 호스트 어플리케이션(550)에 특정 작업을 수행할 것을 요청한다(1).

이에 따라, 호스트 어플리케이션(550)은 객체에 대한 검색, 또는 읽기, 쓰기 등의 작업을 수행한다. 호스트 어플리케이션(550)이 객체를 검색하기 위해서 호스트 디바이스 내에 객체가 있는지, 혹은 이동형 저장 장치에 있는지를 검색하여야 한다.

호스트 어플리케이션(550)이 객체를 사용하거나 객체의 정보를 이용하기 위해서는 이동형 저장 장치에 객체에 대한 정보를 요구하거나 정보를 읽어올 수 있다(2, 3). 호스트 어플리케이션(550)은 호스트 디바이스에서 동작하는 어플리케이션으로, 하나 이상이 동시에 또는 순차적으로 이동형 저장 장치(100)에 저장된 객체를 필요로 할 수 있다.

또한 저장부(540)에 객체를 저장하여 콘텐츠를 이용할 수 있다(8, 9). 그리고 상기 객체를 이동형 저장 장치에 저장할 수 있다.

호스트 어플리케이션(550)으로부터 요청받은 정보를 찾거나 작업을 수행하기 위해, 저장 매체 어플리케이션(150)은 객체 사상 테이블(140)을 통해 객체의 상태에 대한 정보를 얻거나, 또는 정보를 쓰거나 변경할 수 있다(4, 5). 또한 객체 테이블에 저장된 객체 또는 객체 식별자를 읽거나 쓰고, 변경하거나, 삭제하는 등의 작업을 수행할 수 있다(6, 7). 또한 이동형 저장 장치에서 읽어온 객체와 객체의 식별자 정보들을 저장할 수 있고, 추후 저장된 정보를 다시 사용할 수 있다(8, 9).

도 2의 호스트 어플리케이션과 저장매체 어플리케이션 사이에 송수신되는 정보는 도 1의 인증 과정에서 생성된 세션키를 통해 암호화 하여 전송될 수 있다.

도 3은 본 발명의 일 실시예에 따른 객체 테이블을 나타내는 블록도이다. 객체 테이블은 객체와 객체를 검색하기 위해 필요한 식별자 등을 가지고 있다. 그리고 선택적으로 객체의 위치 정보도 함께 가질 수 있다. 객체 테이블의 객체 식별자들은 객체를 검색하기 위한 일종의 키가 될 수 있다. 예를 들어, 해당 객체와 관련된 콘텐츠가 어떤 콘텐츠인지를 알려주는 콘텐츠 식별자(Content ID), 해당 객체와 관련된 콘텐츠의 제공자가 누구인지 알려주는 콘텐츠 제공자 식별자(Content Provider ID), 해당 객체의 객체 식별자(Rights Object ID) 등이 될 수 있다. 이 외에도 객체 식별자에는 객체에 대한 많은 정보를 가질 수 있으며, 이를 통해 객체를 검색할 수 있다.

예를 들어, 객체가 어떤 권한을 가진 객체인지 알기 위해, 재생 권한이 있음을 알려주는 식별자도 존재할 수 있으며, 복사 권한이 있음을 알려주는 식별자도 존재할 수 있다. 또한 해당 객체를 사용할 수 있는 기한을 식별자로 할 수 있다. 이러한 식별자 정보가 많을 때에, 호스트 어플리케이션(500)은 객체의 정보에 대해 접근할 필요없이 식별자 정보를 통해 검색 가능하다.

메타정보 필드(139)는 해당 객체에 데이터가 저장되었는지 혹은 수정되었는지, 삭제되었는지 등에 대한 정보를 가진다.

이외에도 이동형 저장 장치는 객체 테이블의 정보의 수정 여부를 알기 위한 객체 사상 테이블을 가질 수 있다.

객체 테이블은 객체와 객체에 대한 식별자를 가지고 있지만, 이들 객체들이 반드시 연속적으로 저장되는 것은 아니다. 또한 객체가 삭제될 수도 있다. 이 경우, 실제 객체를 삭제하는 것 보다는 사상 테이블(140)을 이용하여 객체가 삭제된 것으로 하여, 이후 해당 객체가 저장된 위치에 새로운 객체를 저장하는 방식도 가능하다. 객체는 객체 테이블의 객체 필드(132)에 저장된다. 예를 들어, 도 3에서 제 5행의 위치에 저장된 객체가 사용 만료등의 이유로 삭제될 경우, 실제 제 5행의 테이블 내의 객체를 지울 수도 있지만, 객체 사상 테이블을 이용하여 삭제되었음을 알릴 경우, 전체 객체와 그 식별자들을 지우는 데 소요되는 시간을 줄일 수 있다. 또한 객체 검색시 객체 사상 테이블을 통해 객체가 존재하는지 여부를 검토하여, 삭제된 객체를 검색할 가능성을 줄일 수 있다.

객체 위치 정보(131)는 해당 객체가 저장된 위치, 즉 주소를 의미한다. 객체 위치 정보는 생략될 수 있다. 객체가 정해진 길이를 가지고, 객체를 식별하는 식별자들 각각의 길이가 해쉬등을 통해 동일한 길이를 가진다면, 객체의 위치는 쉽게 계산할 수 있기 때문에, 객체 위치 정보는 필요하지 않다. 객체 식별자들은 각각 동일한 길이를 가지도록 해쉬를 통해 저장될 수 있다. 예를 들어, 도 3의 첫번째 필드(133)의 객체 식별자가 8byte를 가지며, 두 번째 필드(134)의 객체 식별자가 7byte를 가지도록 해쉬 함수를 사용할 수 있다. 특히 암호학적 해쉬를 사용할 수 있는데, 암호학적 해쉬는 임의의 정보 A를 특정한 길이를 가지는 해쉬값 B로 변환한다. 이때 해쉬값 B만을 가지고 임의의 정보 A를 유추할 수 없으며, 또한 A와 B만 가지고, A와 다르지만 동일한 해쉬값 B로 변환되는 또다른 C를 얻어 내는 것은 불가능하다. 이러한 암호학적 해쉬의 방법으로는 SHA1, MD4, MD5 등이 사용될 수 있다.

도 3에서 저장되는 객체는 하나의 권리 객체를 의미할 수 있으며, 또는 여러 개의 자산(Asset)과 같은 단위로 나뉘어진 것을 의미할 수도 있다. 권리 객체가 다수의 자산(Asset)으로 나뉘어 진 경우, 객체 테이블에는 이들 자산이 객체로 들어갈 수 있고, 객체 식별자 필드에는 권리 객체 식별자와 자산 식별자도 들어갈 수 있다.

또한 이 식별자는 권리 객체를 동일한 장치나 다른 장치에 저장되어 있는 타 권리 객체, 그리고 앞으로 발급될 권리객체와 구분할 수 있는 유일한 값이 될 수 있으며, 식별자의 길이는 가변적일 수 있다. 이때, 제한된 저장공간을 가진 이동형 저장 장치에 이러한 가변적인 길이를 가진 권리객체 식별자를 저장하기 위해서는 암호학적 해쉬를 사용하여 일정한 길이를 가지며 길이를 줄이는 것이 제한된 메모리 공간에서 필요하다. 또한, 객체 외에도 객체 식별자를 암호화 해쉬를 통해 저장함으로써, 데이터의 보안성을 높일 수 있다. 해쉬화된 객체의 식별자를 사용하기 위해서는 이동형 저장 장치와 호스트 디바이스에 해쉬를 수행하는 해쉬부가 존재하여야 한다. 호스트 디바이스에서 특정 값을 검색하고자 할 때, 이를 해쉬로 변환하여 객체 식별자 테이블을 검색할 수 있기 때문이다.

또한 이동형 저장 장치는 도 3에서 살펴본 객체 사상 테이블을 가지고 있어서, 해당 객체가 삭제되거나 수정된 정보를 유지하여, 굳이 해당 객체를 검색하기 전이라도 객체가 삭제된 것을 안다. 그 결과 검색의 속도를 빨리할 수 있다.

도 4는 본 발명의 일 실시예에 따른 암호학적 방식으로 식별자를 해쉬 함수를 취하여 저장한 테이블을 보여준다.

도 4는 객체 테이블에 저장된 객체와 객체 식별자들의 일실시예를 보여주는 테이블이다.

객체 테이블에는 객체가 저장되어 있다. 이 객체는 하나의 권리 객체일 수 있고, 하나의 권리 객체를 분할한 권리객체의 일부일 수 있다. 상기 객체 테이블에 저장하기 위해서는 고정된 길이를 요할 수 있는데, 만약 권리 객체가 고정된 길이보다 더 긴 경우, 권리 객체를 나누어서 저장할 수 있다. 상기 테이블은 저장 매체 내에서 연속적으로 저장될 수 있음을 의미한다.

객체를 검색하기 위한 식별자는 다양하게 존재할 수 있다. 도 5의 객체 테이블에는 콘텐츠 식별자, 권리 객체 식별자, 콘텐츠 제공자 등이 객체 식별자의 기능을 하고 있다. 권리 객체를 찾기 위해서는 호스트 디바이스에 저장된 콘텐츠의 식별자를 가지고 검색할 수 있고, 또는 권리 객체 식별자를 가지고 검색할 수 있다. 또는 작곡가 또는 가수 명으로도 찾을 수 있다. 이러한 검색을 위해 저장하는 객체 식별자는 다양한 길이를 가질 수 있다. 그러나 객체의 빠른 검색을 위해서는 식별자의 길이가 다양할 경우, 객체가 저장된 위치를 정확히 예측하기 어렵다. 따라서 본 발명의 일 실시예에서는 객체 식별자를 암호학적 해쉬를 통해 저장한다. 암호학적 해쉬는 임의의 정보 A를 특정한 길이를 가지는 해쉬값 B로 변환한다. 이때 해쉬값 B만을 가지고 임의의 정보 A를 유추할 수 없으며, 또한 A와 B만 가지고, A와 다르지만 동일한 해쉬값 B로 변환되는 또다른 C를 얻어 내는 것은 불가능하다. 이러한 암호학적 해쉬의 방법으로는 SHA1, MD4, MD5 등이 사용될 수 있다.

예를 들어 콘텐츠 식별자를 살펴보면, 실제 콘텐츠 식별자는 각 객체 1, 2, 3등에 대해 1058, 132, 7985214 등과 같이 각기 다른 길이로 구성된다. 그러나 이들을 해쉬 함수를 통해 동일한 길이의 해쉬값으로 저장할 경우, 길이는 고정된다. 이는 권리 객체 식별자와 콘텐츠 제공자의 경우에도 마찬가지다.

이렇게 해쉬를 통해 저장하면, 호스트 디바이스와 이동형 저장 장치는 동일한 해쉬부를 가진다면, 호스트 디바이스에서 찾고자하는 식별자를 해쉬부를 통해 해쉬값을 얻어서 호스트 디바이스에 저장된 객체 식별자 테이블을 검색하여 객체의 위치 정보를 얻을 수 있다.

또한 객체 테이블의 객체 식별자 부분은 일부분의 객체 식별자 필드를 공란으로 두어, 호스트 디바이스가 상기 객체 테이블을 유용하게 사용할 수 있게 객체 식별자를 생성할 수 있도록 한다. 예를 들어, 식별자 4의 경우, 어떤 식별자를 사용할지를 정하지 않고 공란으로 둔 후에, 호스트 디바이스의 어플리케이션에서 이 식별자를 새로이 설정하여 객체 테이블에 저장할 수 있다.

이하 설명의 편의를 위해 호스트 디바이스와 이동형 저장 장치의 송수신부와 인증부를 제외하고자 한다. 호스트 디바이스와 이동형 저장 장치에서 송수신되는 데이터는 모두 상기 송수신부를 통해 이루어지며, 상기 데이터는 상기 인증부를 통해 암호화 또는 복호화 된다.

도 5는 본 발명의 일 실시예에 따른 호스트 디바이스가 이동형 저장 장치에 저장된 객체에 최초로 접근하는 단계를 보여주는 블록도이다.

호스트 어플리케이션(550)은 찾고자 하는 객체의 식별자 정보와 객체 위치 정보를 송신한다(S101). 객체의 식별자 정보라면, 도 3, 4에서 살펴본 바와 같이 특정 콘텐츠 식별자가 될 수 있고, 또는 특정 콘텐츠 제작자도 될 수 있다. 또한, 권리 객체가 다수로 나뉘어져 저장된 경우, 해당 권리 객체 식별자가 될 수도 있다. 지금 해당 식별자에 따른 객체 정보가 없으므로, 처음부터 순차적으로 찾기 위해 0을 보낸다. 또한 다른 실시예에 의할 때, 객체 식별자만 보낼 수도 있다. 객체 식별자만 보내는 경우, 저장매체 어플리케이션은 내부에 정해진 기준, 예를 들어 0번지라든지, 1번지, 혹은 객체가 저장되어 있는 첫번지 등에서 시작할 수 있다.

이를 수신한 저장매체 어플리케이션(150)은 0번지부터 순차적으로 객체를 검색한다(S111). 객체 테이블의 객체가 가지는 식별자를 비교하여 객체를 검색할 수 있다. 검색 과정을 통해 객체를 찾은 경우 객체와 객체의 위치 정보(K) 및 객체의 식별자 정보 등을 읽어온다(S112). 이렇게 읽어온 정보는 다시 호스트 어플리케이션으로 송신한다(S121). 이 정보들은 저장부(540)에 저장될 수 있다(S131). 또한 객체는 저장하지 않고, 객체의 식별자와 객체의 위치 정보만을 저장할 수 있다.

한편 객체의 식별자에 의한 객체는 하나 이상이 될 수 있다. 따라서, 다른 객체를 찾기 위해 다시 해당 객체 식별자 정보를 보낼 수 있다. 이때에는, 객체의 위치 정보로 0이 아닌 K+1을 보낼 수 있다(S151). 이는 이전에 0번지부터 K번지까지 검색한 결과 객체 정보를 얻게 되었으므로, 같은 객체 식별자를 통해 객체 또는 객체의 정보를 얻고자 할 경우에는 K+1번지부터 검색하면 검색 시간을 줄일 수 있다. K+1번지를 넘겨주는 것은 본 발명의 일 실시예이며, 이전 검색 결과를 이용한 위치 정보들 모두 가능하다. 따라서 K를 넘겨줘서 저장매체 어플리케이션(150)이 K+1번지부터 검색할 수 있다. S151 단계에서 검색을 시작할 위치를 수신한 저장매체 어플리케이션(150)은 S111, S112 단계를 다시 수행하여 해당 객체 식별자를 가지는 또다른 객체와 상기 객체의 식별자 정보 및 위치 정보(L)을 S121의 방식으로 전송할 수 있다. 이와 같은 과정은 저장 매체에 검색하고자 하는 객체 식별자를 가지는 객체를 모두 검색할 때까지 진행할 수 있다.

도 6은 본 발명의 일 실시예에 따른 저장부에 객체 식별자와 객체 위치정보가 저장된 테이블이다. 도 5를 통해 읽어온 객체의 식별자 정보와 객체의 위치정보는 도 6의 실시예처럼 저장될 수 있다.

도 6에서는 객체 식별자 종류와 객체 식별자, 그리고 관련 객체들의 위치 정보를 함께 저장하고 있다. 객체 식별자 종류는 어떤 식별자 항목을 사용할 것인지를 보여준다. 콘텐츠 제작자 정보를 찾는 것인지, 권리 객체가 가지는 정보를 대상으로 찾는 것인지 등을 나타낸다. 도 6에서는 일 실시예로 콘텐츠 제작자, 권리 객체 식별자, 콘텐츠 식별자를 보여준다.

두번째 열은 객체 식별자의 값을 의미한다. 예를 들어 콘텐츠 제작자가 베토벤인 경우, 객체 식별자를 해쉬로 하여 저장한다. 그리고 도 5의 과정을 통해 취득한 객체 위치인 120, 140, 300을 함께 저장한다. 한편 다른 콘텐츠 제작자가 비틀즈인 경우, 150, 250 이라는 객체 위치와 함께 저장된다. 이후 검색한 식별자를 가지고 객체의 정보를 얻기 위해서는 상기 객체 위치를 사용할 수 있다. 통상의 이동형 저장 장치의 메모리는 NAND와 같은 기술을 사용하는데, 이때 임의의 자료의 검색은 첫번째 위치부터 순차적으로 검색할 수 있다. 혹은 특정 위치가 주어질 경우 해당 위치로 직접 접근이 가능하다. 따라서, 객체의 특정 정보를 바탕으로 반복적으로 객체에 접근하는 경우, 해당 객체의 특정 정보, 즉 객체 식별자와 이 객체 식별자를 가지는 객체 위치 정보를 유지하여, 검색 과정없이 직접 객체에 접근할 수 있다.

DRM에서는 특정 권리 객체를 사용함에 있어서 권리 객체를 변경하는 작업이 잦아질 수 있는데, 이러한 권리 객체의 위치 정보를 유지할 경우, 검색 없이 변경, 읽기 등의 작업을 할 수 있다는 점에서 이동형 저장 장치에 저장된 객체를 사용하는 시간을 줄일 수 있다. 또한, 권리 객체가 여러 객체로 나뉘어지거나, 특정 가수 혹은 특정 콘텐츠에 대한 권리 객체가 둘 이상 존재할 경우, 이들 권리 객체들의 위치를 체계적으로 관리하는 작업이 필요하다.

도 6은 객체 식별자로 해쉬 값을 취하여 저장하고 있다. 이는 해쉬 함수를 호스트 디바이스가 가지고 있는 경우에 가능하다. 또한, 해쉬 값이 아닌 원시 객체 식별자로 저장할 수 있다. 이 경우에는 이동형 저장 장치에 상기 원시 객체 식별자를 송신할 때, 이동형 저장 장치에서 원시 객체 식별자를 해쉬 함수를 취해 해쉬값으로 변환하여 검색하는 과정이 필요하다.

도 7은 본 발명의 일 실시예에 따른 호스트 디바이스가 객체 식별자와 객체 위치 정보를 이용하여 이동형 저장 장치에 저장된 객체에 접근하는 과정을 보여주는 블록도이다.

도 7의 저장부(540)는 도 5의 과정을 통해 도 6의 형식으로 객체 식별자와 객체 위치 정보를 저장하고 있다. 호스트 어플리케이션(550)은 검색하고자 하는 객체의 위치를 저장부(540)에서 취득하여(S201), 이 위치 정보와 이 객체에 대해 행해질 작업을 함께 이동형 저장 장치로 보낸다(S211). 객체에 대해 행해질 작업은 객체를 읽어오거나 수정하는 작업, 또는 해당 객체의 객체 식별자를 읽어오는 작업 등을 의미한다. 객체 위치 정보와 객체에 행해질 작업을 함께 이를 수신한 저장매

체 어플리케이션(150)은 객체 테이블에서 직접 객체를 찾아서, 상기 작업에 따라 객체 정보를 읽어오거나, 수정 또는 갱신 등의 작업을 수행한다(S222). 또한 선택적으로 객체 사상 테이블(140)에 상기 작업에 따른 객체 정보의 변화를 저장할 수 있다(S225). 저장매체 어플리케이션(150)은 호스트 디바이스(550)에 상기 작업 결과를 송신한다(S231).

본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구의 범위에 의하여 나타내어지며, 특허청구의 범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

발명의 효과

본 발명을 구현함으로써 이동형 저장 장치에 저장된 객체를 신속하게 검색하여 객체를 이용하는 속도를 증가시킬 수 있다.

본 발명을 구현함으로써 동일 객체 식별자의 객체들을 반복적으로 사용하는 경우 객체를 검색하는 시간을 줄일 수 있다.

(57) 청구의 범위

청구항 1.

이동형 저장 장치에 접근하는 단계;

상기 이동형 저장 장치에 객체 식별자를 송신하는 단계;

상기 이동형 저장 장치로부터 상기 객체 식별자에 의하여 검색된 제 1 객체의 위치 정보를 수신하는 단계;

상기 제 1 객체의 위치 정보를 상기 객체 식별자와 함께 저장하는 단계; 및

상기 제 1 객체의 위치 정보를 사용하여 상기 이동형 저장 장치에 상기 제 1 객체 위치 정보와 상기 제 1 객체에 대하여 수행되는 작업 정보를 송신하는 단계를 포함하는 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 2.

제 1항에 있어서,

상기 접근하는 단계 이후에,

상기 이동형 저장 장치와 상호 인증하여 세션키를 공유하는 단계를 더 포함하며,

상기 이동형 저장 장치와 송수신하는 데이터는 상기 세션키로 암호화하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 3.

제 1항에 있어서,

상기 제 1 객체의 위치 정보를 저장하는 단계 이후에,

상기 객체 식별자와 상기 제 1 객체 위치 정보를 송신하는 단계;

상기 이동형 저장 장치로부터 상기 객체 식별자에 의하여 검색된 제 2 객체의 위치 정보를 수신하는 단계; 및

상기 제 2 객체의 위치 정보를 저장하는 단계를 더 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 4.

제 1항에 있어서,

상기 객체 식별자를 송신하는 단계는 객체 식별자와 상기 이동형 저장 장치에서 객체를 검색하는 기준이 되는 위치 정보를 송신하는 단계를 더 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 5.

제 1항에 있어서,

상기 객체 식별자는 해쉬를 통해 얻은 값인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 6.

제 1항에 있어서,

상기 객체 식별자는 상기 객체와 관련된 컨텐츠에 관한 식별 정보, 객체의 사용과 관련된 식별 정보, 또는 상기 객체를 생성한 주체에 대한 식별 정보 중 어느 하나를 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 7.

제 1항에 있어서,

상기 객체는 컨텐츠에 대한 권리 정보를 포함하는 권리 객체 또는 상기 권리 객체의 일부분인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 8.

호스트 디바이스에 접근하는 단계;

상기 호스트 디바이스로부터 객체 식별자를 수신하는 단계;

객체와 상기 객체 식별자가 저장된 저장부에서 상기 객체 식별자를 가지는 객체의 위치 정보를 검색하여 상기 호스트 디바이스로 송신하는 단계;

상기 호스트 디바이스로부터 상기 객체의 위치 정보와 상기 객체에 대하여 수행되는 작업 정보를 수신하는 단계; 및

상기 수신한 객체의 위치 정보를 이용하여 상기 저장부의 객체에 직접 접근하여 상기 작업 정보에 따라 작업을 수행하는 단계를 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 9.

제 8항에 있어서,

상기 호스트 디바이스에 접근하는 단계 이후에,

상기 호스트 디바이스와 상호 인증하여 세션키를 공유하는 단계를 더 포함하며,

상기 호스트 디바이스와 송수신하는 데이터는 상기 세션키로 암호화하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 10.

제 8항에 있어서,

상기 객체 식별자를 수신하는 단계에서 객체의 위치 정보를 더 수신하는 경우,

상기 객체의 위치 정보의 검색은 상기 저장부에서 상기 위치 정보를 기준으로 이루어지는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 11.

제 8항에 있어서,

상기 객체 식별자를 수신하는 단계에서 객체의 위치 정보를 수신하지 않는 경우,

상기 객체의 위치 정보의 검색은 상기 저장부의 특정 위치를 기준으로 이루어지는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 12.

제 8항에 있어서,

상기 저장부는 테이블인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 13.

제 8항에 있어서,

상기 작업을 수행하는 단계 이후에,

상기 객체의 상태의 변경 사항을 표시하는 단계를 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 14.

제 8항에 있어서,

상기 객체에 직접 접근하는 단계는 상기 객체에 대하여 수행되는 작업이 객체를 갱신하는 작업인 경우,

상기 객체의 갱신 여부를 상기 저장부에 표시하는 단계를 더 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 15.

제 8항에 있어서,

상기 객체 식별자는 해쉬를 통해 얻은 값인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 16.

제 8항에 있어서,

상기 객체의 식별자는 상기 객체와 관련된 콘텐츠에 관한 식별 정보, 객체의 사용과 관련된 식별 정보, 또는 상기 객체를 생성한 주체에 대한 식별 정보 중 어느 하나를 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 17.

제 8항에 있어서,

상기 객체는 콘텐츠에 대한 권리 정보를 포함하는 권리 객체 또는 상기 권리 객체의 일부분인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 방법.

청구항 18.

이동형 저장 장치에 객체 식별자를 송신하여 상기 객체 식별자의 제 1 객체의 위치 정보를 수신하는 어플리케이션부;

상기 객체 식별자와 상기 제 1 객체의 위치 정보를 저장하는 저장부를 포함하며,

상기 어플리케이션부는 상기 저장된 객체 식별자를 검색하여 상기 저장된 제 1 객체의 위치 정보와 상기 제 1 객체에 대하여 수행되는 작업 정보를 송신하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 19.

제 18항에 있어서,

상기 이동형 저장 장치와 상호 인증하여 세션키를 공유하는 인증부를 더 포함하며,

상기 이동형 저장 장치와 송수신하는 데이터는 상기 세션키로 암호화하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 20.

제 18항에 있어서,

상기 어플리케이션부는 상기 객체 식별자와 상기 제 1 객체 위치 정보를 송신하여, 상기 이동형 저장 장치로부터 상기 객체 식별자로 검색한 제 2 객체의 위치 정보를 수신하여 상기 제 2 객체의 위치 정보를 저장하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 21.

제 18항에 있어서,

상기 어플리케이션부는 상기 이동형 저장 장치에서 객체를 검색하는 기준이 되는 위치 정보를 더 송신하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 22.

제 18항에 있어서,

상기 어플리케이션부는 검색하고자 하는 객체의 식별 정보를 해쉬를 통해 얻은 값으로 검색하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 23.

제 18항에 있어서,

상기 객체 식별자는 해쉬를 통해 얻은 값인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 24.

제 18항에 있어서,

상기 객체 식별자는 상기 객체와 관련된 콘텐츠에 관한 식별 정보, 객체의 사용과 관련된 식별 정보, 또는 상기 객체를 생성한 주체에 대한 식별 정보 중 어느 하나를 포함하는, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 25.

제 18항에 있어서,

상기 객체는 콘텐츠에 대한 권리 정보를 포함하는 권리 객체 또는 상기 권리 객체의 일부분인, 이동형 저장 장치에서 객체의 위치 정보를 이용하여 권리 객체를 검색하는 장치.

청구항 26.

객체와 객체 식별자를 저장하는 객체 정보 저장부; 및

호스트 디바이스가 송신한 객체 식별자를 수신하는 어플리케이션부를 포함하며,

상기 어플리케이션부는 상기 객체 정보 저장부에서 상기 객체 식별자를 가지는 객체의 위치 정보를 검색하여 상기 호스트 디바이스로 송신하며, 상기 호스트 디바이스로부터 상기 객체의 위치 정보와 상기 객체에 대하여 수행되는 작업 정보를 수신하여 상기 위치 정보를 이용하여 상기 저장부의 객체에 직접 접근하여 상기 작업 정보에 따라 작업을 수행하는 이동형 저장 장치.

청구항 27.

제 26항에 있어서,

상기 호스트 디바이스와 상호 인증하여 세션키를 공유하는 인증부를 더 포함하며,

상기 호스트 디바이스와 송수신하는 데이터는 상기 세션키로 암호화하는 이동형 저장 장치.

청구항 28.

제 26항에 있어서,

상기 어플리케이션부가 객체의 위치 정보를 더 수신하는 경우, 상기 객체의 위치 정보의 검색은 상기 객체 정보 저장부에서 상기 위치 정보를 기준으로 객체를 검색하는 이동형 저장 장치.

청구항 29.

제 26항에 있어서,

상기 어플리케이션부가 객체의 위치 정보를 수신하지 않는 경우, 상기 객체의 위치 정보의 검색은 상기 객체 정보 저장부의 특정 위치를 기준으로 이루어지는 이동형 저장 장치.

청구항 30.

제 26항에 있어서,

상기 객체 정보 저장부는 테이블인 이동형 저장 장치.

청구항 31.

제 26항에 있어서,

상기 어플리케이션부는 상기 작업을 수행한 이후에,

상기 객체의 상태에 대한 정보가 포함된 객체 사상 저장부에 객체의 변경 사항을 표시하는 이동형 저장 장치.

청구항 32.

제 26항에 있어서,

상기 어플리케이션부는 상기 객체에 대해 수행한 작업이 객체를 갱신하는 작업인 경우,
상기 객체의 갱신 여부를 상기 객체 정보 저장부에 표시하는 이동형 저장 장치.

청구항 33.

제 26항에 있어서,

상기 객체 식별자는 해쉬를 통해 얻은 값인 이동형 저장 장치.

청구항 34.

제 26항에 있어서,

상기 객체의 식별자는 상기 객체와 관련된 콘텐츠에 관한 식별 정보, 객체의 사용과 관련된 식별 정보, 또는 상기 객체를 생성한 주체에 대한 식별 정보 중 어느 하나를 포함하는 이동형 저장 장치.

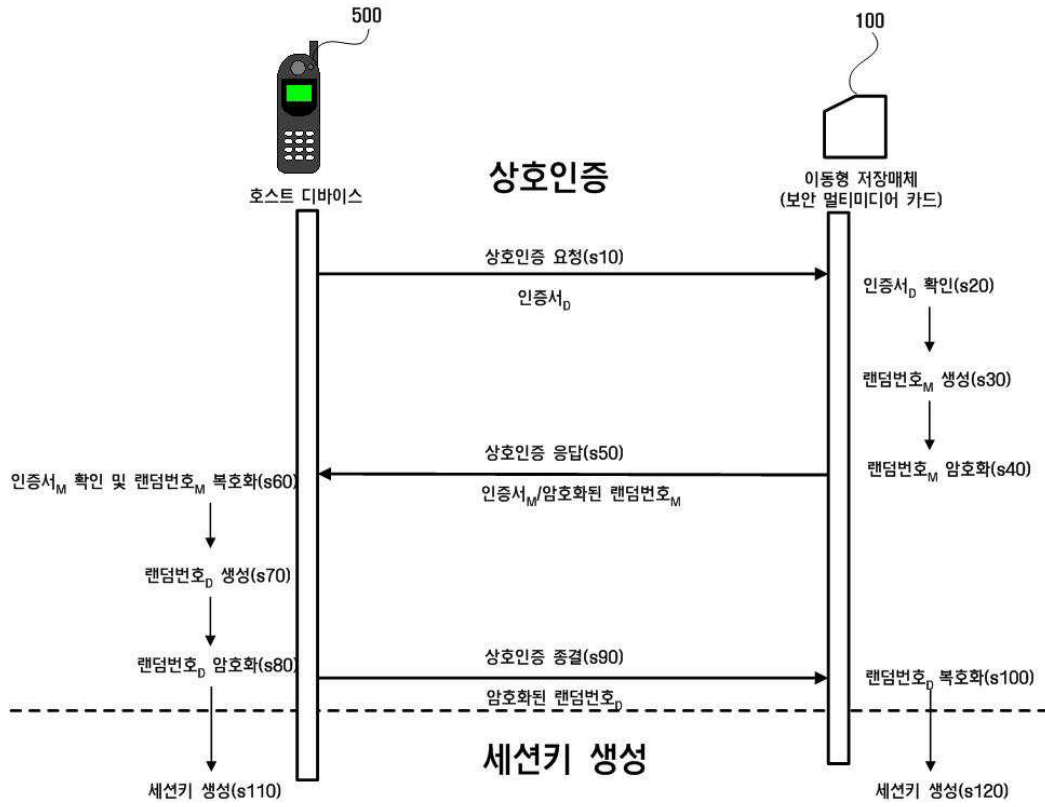
청구항 35.

제 26항에 있어서,

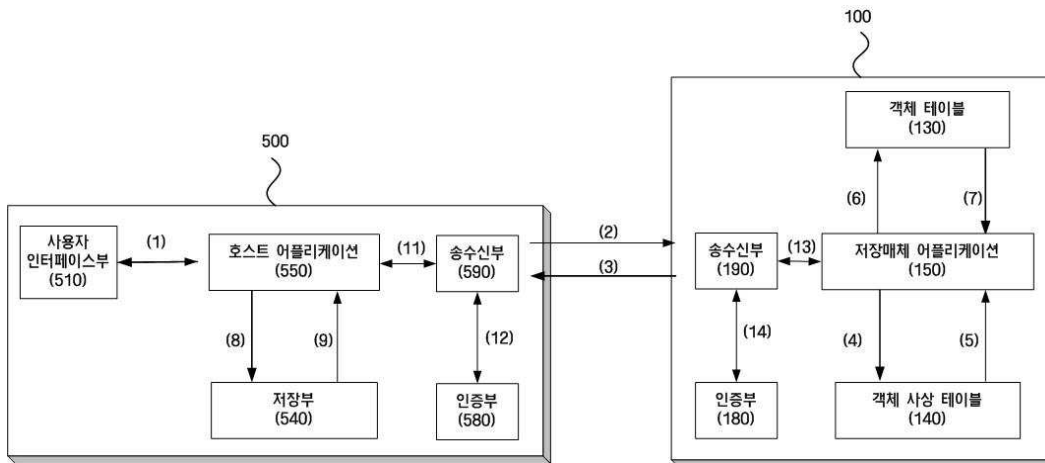
상기 객체는 콘텐츠에 대한 권리 정보를 포함하는 권리 객체 또는 상기 권리 객체의 일부분인 이동형 저장 장치.

도면

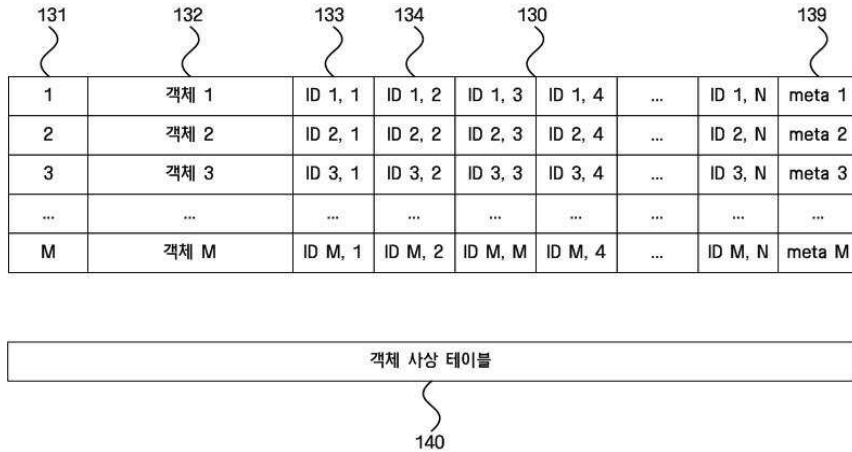
도면1



도면2



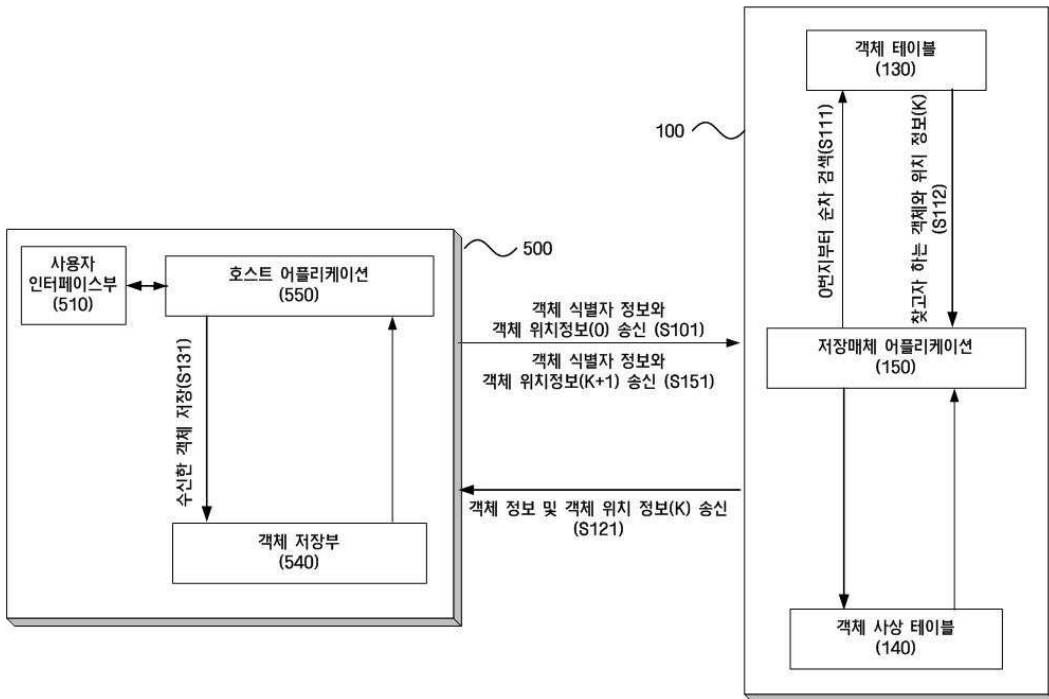
도면3



도면4

| 위치 | 저장된 권리 객체 | 컨텐츠 식별자 | 권리객체 식별자 | 컨텐츠 제공자 | 식별자 4 | ... | 식별자 N | 메타필드 |
|-----|-----------|---------------|-------------------|-----------|---------|-----|---------|------|
| 1 | 객체 1 | Hash(1058) | Hash(RID_837) | Hash(베토벤) | ID 1, 4 | ... | ID 1, N | 0 |
| 2 | 객체 2 | Hash(132) | Hash(RID_5396393) | Hash(스팅) | ID 2, 4 | ... | ID 2, N | 0 |
| 3 | 객체 3 | Hash(7985214) | Hash(RID_39741) | Hash(비틀즈) | ID 3, 4 | ... | ID 3, N | 0 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |

도면5



도면6

| 객체 식별자 종류 | 객체 식별자 | 객체위치 | 객체위치 | 객체위치 | 객체위치 |
|-----------|-----------------|------|------|------|------|
| 컨텐츠 제작자 | Hash(베토벤) | 120 | 140 | 300 | |
| 컨텐츠 제작자 | Hash(비틀즈) | 150 | 250 | | |
| 권리 객체 식별자 | Hash(RID_39741) | 123 | 231 | 345 | |
| 컨텐츠 식별자 | Hash(CID_536) | 39 | 62 | | |

도면7

