(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 1/14

(45) 공고일자 2005년11월15일
(11) 등록번호 10-0527836
(24) 등록일자 2005년11월03일

(21) 출원번호 10-2000-7003206
(22) 출원일자 2000년03월24일
번역문 제출일자 2000년03월24일
(86) 국제출원번호 PCT/IB1998/001510
국제출원일자 1998년09월22일

(65) 공개번호 10-2001-0030706
(43) 공개일자 2001년04월16일
(87) 국제공개번호 WO 1999/15970
국제공개일자 1999년04월01일

(81) 지정국

국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바르바도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 인도, 가나, 감비아, 짐바브웨, 세르비아 앤 몬테네그로,

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 가나, 감비아, 짐바브웨,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드, 사이프러스,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

(30) 우선권주장 97402237.8 1997년09월25일 유럽특허청(EPO)(EP)

(73) 특허권자
까날 + (쏘시에떼 아노님)
프랑스공화국 빠리 께 앙드레 씨뜨로엥 85/89

(72) 발명자
베나르듀,크리스티앙
프랑스,에프-77600비지세인트죠지,알르데푸이사티에르스,13

(74) 대리인
최홍순
조성욱
박세걸
특허법인세신

심사관 : 허영한

(54) 기록된 디지털 데이터의 보호를 위한 방법 및 장치

를 액세스할 경우에 볼륨 디스크립터(V)의 암호화된 요소를 해독하고 이 요소를 판독기(5)에 공급하여 지원매체(2)의 비암호화 데이터의 판독 및/또는 기록을 가능케하기 위하여 집적회로 해독키(Kf)를 사용하는 단계를 포함하는 것을 특징으로 한다.

대표도

도 2

색인어

디지털 데이터, 지원매체, 볼륨 디스크립터

명세서

기술분야

본 발명은 기록된 디지털 데이터의 보호, 예를 들면 컴팩트 디스크, 디지털 비디오 디스크 등의 지원물에 기록된 음성 및/또는 영상 데이터의 보호를 위한 방법 및 장치에 관한 것이다.

배경기술

시청각 분야에서의 디지털 기술의 도입은 아날로그 기술과 비교하여 특히 지원매체의 음성 및 이미지의 복사 품질 및 내구성과 관련하여 소비자에게 상당한 이점을 가져다 주었다. 컴팩트 디스크는 구식 비닐 레코드를 거의 대체하고 있으며 이러한 경향은 일반적으로 멀티미디어 및 가정용 엔터테인먼트 시장을 겨냥한 새로운 디지털 제품, 특히 디지털 비디오 디스크의 도입으로 기대된다.

디지털로 기록된 데이터와 관련된 특정한 문제점은 복사의 용이성과 이로 인한 저작권 침해의 가능성에 있다. 단 한개의 디지털 기록물은 음성 또는 이미지의 품질의 어떠한 저하도 없이 완벽하게 어떠한 수의 복사물도 만드는 데 사용될 수 있다. 이러한 문제는 특히 미니디스크 또는 DAT와 같은 기록가능한 디지털 제품의 출현으로 심각하며, 이 문제가 남아있는 동안은 엔터테인먼트 회사가 저작권을 얻기를 꺼려함으로써 새로운 미디어 제품이 시장으로 도입되는 것이 중단되고 있다.

현재, 허가되지 않은 저작권의 사용에 대하여 실제적으로 유일하게 사용가능한 해결책은 합법적인 것이었으며, 유럽의 여러 나라 등에서는 시장으로 인입되는 다수의 해적판 필름, CD 등을 제거하기 위하여 반해적판(anti-piracy) 법률을 도입하고 있다. 명백한 이유로, 합법적인 해결책은 예방적 관점에서 보다 비효율적이다.
기록물의 원형을 검증하기 위하여 예를 들어 판독기와 지원매체 사이의 소정 형태의 디지털《핸드셰이크(handshake)》에 의존하는, 시청각 행위에 대한 일자에 제시된 기술적인 반복사 해결책은 매우 기본적이었다. 그러나, 이러한 보호는, 핸드셰이크 신호가 모든 방식에서 보호되지 않으며 허가되지 않은 복사물을 명백하게 허가되고 판독가능한 복사물로 변환하기 위하여 용이하게 판독 및 복사될 수 있기 때문에, 단지 가장 낮은 레벨의 복사 행위에 대해서만 효과적이다.

삭제

암호화된 컴퓨터 디스크 데이터로의 액세스를 제어하기 위하여 스마트카드에 저장된 비밀키를 사용하는 컴퓨터 시스템은, 예를 들어 미국 특허 제 5 191 611호에 공지되어 있다. 이러한 시스템은, 기록된 암호화 데이터를 해독 및 저장하기 위하여 판독기에 상당한 처리 및 메모리 능력이 제공되어야 한다는 단점이 있다. 아는 바와 같이, 이러한 시스템은 컴퓨터 데이터를 보호하기 위하여 사용될 경우에 일반적으로 불편하며 판독기가 전형적으로 컴퓨터와 비교하여 데이터의 처리 및 저장 용량이 작음에도 불구하고 데이터의 실시간 흐름이 유지될 필요가 있는 시청각 영역에 적용하기가 부적절하다.

발명의 상세한 설명

본 발명의 목적은 종래기술과 관련된 단점을 극복하고 특히 시청각 행위와 관련하여 허가되지 않은 디지털 기록물의 복사에 대하여 효과적인 기술적 해결책을 제공하는 것이다.

본 발명에 따르면, 제 1 해독키를 포함하는 집적회로를 사용하여 디지털 지원매체에 기록된 디지털 데이터로의 액세스를 제한하는 방법이 제공된다. 이 방법은 지원매체의 하나 이상의 볼륨 디스크립터 요소를 대응하는 암호화 키로 암호화하는 단계와, 암호화된 볼륨 디스크립터 요소를 지원매체의 비암호화 데이터와 함께 기록하는 단계와, 지원매체를 액세스할 경우에 암호화된 볼륨 디스크립터의 요소를 해독하고 이 요소를 판독기에 제공하여 지원매체의 비암호화 데이터의 판독 및/또는 기록이 가능하도록 집적회로 해독키를 사용하는 단계를 포함하는 것을 특징으로 한다.

CD, CD ROM 등과 같은 디지털 지원 매체에 대하여, 각 기록물은 매체의 디지털 정보의 저장 배치 및 액세스점, 매체에 저장된 데이터의 양, 지원 매체의 작성일자 등에 관련된 기본 정보를 설명하는 볼륨 디스크립터의 형태로 머리말 또는 헤더와 관련되어 있다. 소정량의 메모리만을 사용하는 이러한 정보는 그럼에도 불구하고 기록물의 판독에 반드시 필요하기 때문에 판독기는 이러한 정보 없이 기록된 데이터를 액세스할 수 없다.
이 정보를 암호화하고 해독키를 지원매체와 관련된 집적회로에 저장함으로써, 판독기는 해독된 볼륨 디스크립터의 요소없이 저장된 데이터를 액세스할 수 없으며 그리고 이것을 행하는 데 필요한 키가 물론 복사물에 저항하는 집적회로에 의해 유지되기 때문에 본 발명은 허가되지 않은 기록물의 복사에 대하여 보호한다. 저장된 비암호화 데이터가 복사될지라도, 볼륨 디스크립터가 불완전하게 또는 전적으로 암화화된 형태로만 존재할 것이기 때문에 복사물은 판독될 수 없을 것이다. 볼륨 요소의 해독은 집적회로내에서 수행될 수 있기 때문에, 키는 결코 자유롭게 사용될 수 없다.

삭제

컴퓨터 데이터를 보호하기 위하여 사용되는 종래기술과 달리, 볼륨 디스크립터 또는 헤더 데이터만이 암호화/해독됨으로써 저장된 데이터의 전체 볼륨에서 암호 동작을 수행할 필요가 없다. 아는 바와 같이, 이것은 본 발명이 시청각 장치의 분야에 적용될 경우에 특히 유리하며, 판독기의 처리 및 메모리 용량은 비교적 적을 수 있다.

일실시예로, 집적회로는 지원 매체와 관련된 스마트카드에 내장되며, 이 스마트카드는 암호화된 볼륨 요소를 해독하고 이것을 판독기로 전송하여 기록된 비암호화 데이터의 판독 및/또는 기록이 가능하도록 작용한다.

이러한 정황으로, 스마트카드는 볼륨 디스크립터 요소의 해독에 필요한 키를 저장하는 보안 및 내구성 수단을 제공한다. 그럼에도 불구하고, 이러한 카드의 제조 비용은 예를 들어 그 자체를 기록하는 비용과 비교하여 비교적 저렴하다.

이 출원서에서, 용어 <<스마트 카드>>는 예를 들어 마이크로프로세서 또는 키를 저장하는 EEPROM 메모리를 포함하는 종래의 모든 칩 기반 카드 디바이스를 의미하는 데 사용된다. 또한, TV 디코더 시스템에 종종 사용되는 키 형상(key-shaped) 디바이스와 같은 다른 물리적인 형태를 갖는 PCMCIA 카드 등의 휴대용 칩 적재 카드 또는 디바이스도 이 용어에 포함된다.

본 발명에서 사용되는 집적회로 또는 《칩》을 하우징하는 특별히 편리한 방식이 제공되지만, 스마트카드는 오로지 사용가능한 해결책이 아니다. 예를 들면, 하나의 구현으로, 키는 디지털 지원매체의 하우징에 내장된 집적회로에 저장된다.

지원매체의 하우징내에 마이크로프로세서를 결합하는 기술은 공지되어 있는 기술이며 예를 들어 DVHS 카세트의 경우에 하우징의 내부에 집적회로 또는 칩으로 안내하는 일련의 금속접점이 카세트 하우징의 외부면에 설치될 수 있는 것이 제안되었다. 이러한 접점은 집적회로와 비디오 레코더 사이의 통신을 가능케하기 위하여 레코더 리셉터클의 대응하는 일련의 접점에 의해 결합될 수 있다.

이러한 해결책은 기록물과 관련하여 스마트카드 등의 준비에 대한 필요성을 없앨 수 있으며, 따라서 소비자 관점에서는 보다 용이하다. 지원물을 판독하는 데 사용되는 판독기의 비용과 같이, 기록 매체의 제조비용이 물론 하우징내에 집적회로를 결합하기 위하여 증가할지라도, 예를 들어 디지털 판독기의 스마트카드 슬롯을 포함할 필요성도 없앨 수 있다.

일실시예로, 볼륨 디스크립터 요소를 암호화 및/또는 해독하는 키는 지원매체의 식별과 관련된 값 또는 기록된 데이터를 나타내는 상수, 예를 들어 일련번호 또는 일괄처리 번호를 제작함으로써 다양화된 키를 포함한다. 이 방식에서, 제작된 상수에 의해 다양화된 간단한 암호화 알고리즘이 사용되어 《유일한》 키 및 유일한 암호화된 볼륨 디스크립터를 제공할 수 있다. 사실, 가장 실용적인 목적을 위하여, 소정의 기록 지원물의 일괄처리번호 또는 하나의 특별하게 기록된 성능을 위하여 동일한 키가 생성될 수 있다.

가장 단순한 형태로, 본 발명에서 사용되는 키 알로리즘은 DES 또는 RC2 등과 같은 다수의 공지된 대칭 알로리즘 중 어느 하나일 수 있다. 이러한 경우에, 암호화/해독 키는 이상적인 것으로 생각될 수 있다. 예를 들면 공개키/비밀키쌍을 사용하는 다른 실시예가 가능하다.

삭제

본 발명의 방법의 하나의 구현으로, 볼륨 요소는 집적회로에 생성 및 저장된 새로운 키에 따른 집적회로에 의해 재암호화(re-encrypted)되며, 이전에 암호화된 값을 대체하는 재암호화된 볼륨 요소는 이후에 판독기에 의해 매체에 기록된다. 이 방식에서, 시스템의 보안은 강해지며 본 기록물로 집적회로의 식별이 확보된다.

새로운 키는 예를 들어 랜덤 또는 수도-랜덤 넘버 생성기를 사용하여 집적회로에 의해 생성될 수 있다. 따라서, 동일한 키로 초기에 인코딩된 기록의 일괄처리의 경우라도, 암호화된 볼륨 디스크립터는 각 기록물의 실행으로 빠르게 변화시키기 때문에 2개의 기록물이 동일한 키로 개방되지 않을 것이다.

일실시예로, 집적회로에 의해 생성된 새로운 키는 판독기로부터 집적회로에 의해 판독되는 판독기의 식별과 관련된 값, 예를 들어 일련번호에 의해 다양화된다. 이것에 의해 기록물은 특별한 판독기에 의해서만 판독될 수 있다.

일실시예로, 판독기의 식별과 관련된 값은 지원매체에 저장되고 후속 판독시 판독기로부터 직접 판독되는 값과 집적회로에 의해 비교된다. 하나의 구현으로, 집적회로는 판독기로부터 판독된 값이 매체에 저장된 것과 매칭되지 않으면 단지 그 값을 거부할 수 있다.
그러나, 다른 구현으로, 이 시스템은 예를 들어 판독기가 대체되거나 고장날 가능성에 대하여 이 값의 업데이트를 가능케 하도록 프로그램될 수 있다. 이러한 실시예에서, 집적회로는 지원매체로부터 판독된 식별값과 판독기로부터 판독된 것을 비교하여 둘 사이에 미스매치 또는 차이가 있는 경우에는 기록매체로부터의 이전의 판독기 식별값을 사용하여 볼륨 요소를 해독하고 그리고 나서 판독기로부터 새로운 판독기 식별값을 사용하여 볼륨 요소를 재암호화하도록 기능한다.

삭제

새로운 판독기 식별은 이전의 판독기 식별로 대체되거나 또는 이전의 판독기 식별과 함께 저장될 수 있다. 전자의 경우에, 무한한 수의 판독기가 디스크를 액세스하지 않도록 집적회로는 소정 시간만 이 동작을 수행하도록 프로그램될 수 있다. 후자의 경우에, 소정 개수의 허가된 판독기 식별이 저장될 수 있도록 집적회로가 프로그램되어 기록물이 예를 들어 사용자가 소유한 다수의 판독기에서 실행될 수 있다. 제한된 수의 판독기 식별로, 집적회로는 허가된 판독기 사이의 무한한 수의 변화를 안전하게 허용할 수 있다.

본 발명이 미리기록된 CD, CD ROM 등과 같은 미리기록된 기록물의 보호와 관련하여 대부분 설명하였다. 그러나, 아는 바와 같이, 동일한 기술이 기록가능한 장치를 차단하기 위하여 적용될 수 있으며 하나의 구현으로 지원 매체는 판독기의 첫번째 삽입에 앞서 차단되며, 상기 관련된 집적회로의 존재는 판독기가 블랭크 매체에 어떠한 데이터라도 기록할 수 있도록 하기 이전에 볼륨 요소를 해독하는 데 필요하다.

이러한 블랭크 장치는 일련의 볼륨 디스크립터 요소를 포함하며, 그 일부 또는 모두는 저장된 키에서 그리고 원한다면 하나 또는 선택된 수의 판독기에서 상기 장치가 판독/기록될수 있다는 것을 확보하기 위하여 상술한 바와 같이 암호화될 수 있다. 이 방식에서, 기록 매체의 비암호화 형태로 저장된 궁극적으로 기록된 작업의 허가되지 않은 복사물에 대한 보호를 행할 수 있다.

따라서, 이 명세서에서 용어《판독기》는 일반적으로 미리기록된 디지털 데이터를 판독할 수 있는 장치를 언급하기 위하여 사용되었지만, 이러한 데이터의 기록이 행해지는 실시예에서 지원매체에 디지털 데이터를 기록할 수 있는 장치도 포함한다는 것이 이해되어야 한다.

일실시예로, 본 발명은 데이터가 음성 및/또는 영상 데이터인 기록된 디지털 데이터로의 액세스를 제한하는 방법으로 확장된다. 그러나, 아는 바와 같이, 본 발명은 컴퓨터 처리 데이터의 보호에도 동등하게 적용될 수 있다.

본 발명은 본 발명의 방법에 사용하기 위한, 예를 들어 스마트카드에 결합된 디지털 지원매체 및 집적회로를 제조하는 방법에도 동일하게 확장된다.
본 발명의 바람직한 실시예가 첨부한 도면을 참조하여 예시로서만 기술될 것이다.

도면의 간단한 설명

삭제

도 1은 CD ROM의 경우에 적어도 부분적으로 암호화된 볼륨 디스크립터 및 해독키를 포함하는 스마트카드를 포함하는 디지털 지원 매체의 작성시의 단계를 나타낸 도면.
도 2는 도 1에 따라 암호화된 디지털 지원매체의 판독시에 수행되는 단계를 나타낸 도면.

삭제

실시예

도 1을 참조하면, 암호화된 볼륨 디스크립터를 포함하는 디지털 기록물의 제작 단계가 도시되어 있다. 제 1 암호화 키(Kf)는 본 기록물과 관련된 《유일한》 키를 유도하기 위하여 제작상수(Cf)에 의해 단계 1에서 얻어지고 다양화된다. 암호화 키(Kf)는 예를 들어 DES와 같은 기술분야에서 당업자에게 알려진 어떠한 표준 대칭 암호화 알고리즘으로도 얻을 수 있다.

제작 상수(Cf)는 예를 들어 기록매체의 일련번호를 포함하는, 본 기록물과 관련된 다수의 값에서 선택될 수 있다. 그러나, 간략화된 실시예로, 제작상수(Cf)는 CD-ROM의 일괄처리의 생산과 관련된 일괄처리번호, 또는 CD-ROM에 기록된 필름, 음악공연 등의 카달로그 번호에 해당하는 일련번호도 나타낼 수 있다.

후자의 경우에, 동일한 디지털 키는 예를 들어 동일한 성능 또는 동일한 필름의 모든 기록 버젼에 대하여 생성될 것이다. 기록 매체를 기반으로 한 작성상수(예를 들면 CD ROM 일련번호 또는 일괄처리번호)가 사용되는 구현보다 덜 안전하더라도, 이 실시예에 의해 제공되는 보안 레벨은 상업적인 목적으로는 충분할 수 있다.

그리고, 제 1 키(Kf)의 다양화로부터 얻어진 《유일한》 암호화 키는 본 기록 매체와 관련된 볼륨 디스크립터 V의 하나 이상의 요소를 암호화하기 위하여 단계 3에서 사용된다. 도입부에서 언급한 바와 같이, 디지털 기록 분야에서 볼륨 디스크립터의 사용은 이 기술분야에서 공지된 개념이다. 이러한 디스크립터는 기록물이 실행되기 이전에 판독기에 의해 판독 및 동화되어야 하는 기록물의 특성(저장된 데이터의 양, 기록물의 디지털 정보의 레이아웃 등)을 서술하는 다수의 요소를 포함한다.

소정의 디지털 기록매체(CD,CD ROM,DVD 등)에 대한 볼륨 디스크립터의 포맷은 서로 다른 판독기 사이의 호환성을 확보하기 위하여 일반적으로 국제 표준 또는 기준에 의해 좌우된다. CD ROM의 경우에, 예를 들면, 볼륨 디스크립터의 포맷은 본 출원의 판독기가 언급된 국제 표준 ISO 9660에 의해 좌우된다.

원한다면, 모든 정보는 본 발명의 일실시예로 암호화될 수 있다. 그러나, 볼륨 디스크립터의 정보중 일부는 모든 표준화된 기록물에 대하여 사실상 불변일 수 있기 때문에, 보다 효과적인 해결책은 전반적인 볼륨 디스크립터의 소정의 요소만의 암호화에 기반을 둘 수 있다.

예를 들면, CD ROM의 경우에, 표준 ISO 9660의 표 4에 나타낸 것과 같이 볼륨 디스크립터의 옥텟 위치 129 내지 190에서 확인된 데이터가 암호화될 수 있다. 이 위치에서, 다음의 데이터가 확인된다:
129 내지 132 논리 블록의 크기

삭제

133 내지 140 경로 테이블의 크기

141 내지 144 형식 L의 경로 테이블의 발생 위치

145 내지 148 형식 L의 경로 테이블의 선택적 발생 위치

149 내지 152 형식 M의 경로 테이블의 발생 위치

153 내지 156 형식 M의 경로 테이블의 선택적 발생 위치

157 내지 190 소스 인덱스에 대한 인덱스의 기록

아는 바와 같이, 여기서 디스크립터는 CD ROM 디스크와 관련하여 기술되었지만, 본 발명은 디스크립터, 디지털 비디오 디스크 등을 포함하는 시청각 또는 멀티미디어 타입 데이터의 디지털 기록물의 다른 포맷에도 동등하게 적용될 수 있다.

삭제

다시 도 1을 참조하면, 선택된 볼륨 스크립터(V)의 요소는 지원매체(2)로부터 판독되고 다양화된 키(kf)에 의해 단계 3에서 암호화된다. 여기서 E1(V)로 지칭한 암화화된 볼륨 디스크립터의 요소는 이후로는 지원(2)의 원래 요소(V)를 대체하는데 사용된다. 따라서, 형성된 지원매체는 부분적으로 또는 전체적으로 암호화된 볼륨 디스크립터와 함께 본 기록물의 벌크를 나타내는 암호화되지 않은 디지털 데이터를 포함한다. 아는 바와 같이, 동등한 해독키 없이 기록물은 판독될 수 없다.

허가된 사용자가 지원물의 데이터를 액세스할 수 있도록 하기 위해서는, 사용자에게 키 Kf와 다양화기 Cf를 제공할 필요가 있다. 본 실시예에서, 값 Kf,Cf는 스마트카드에 장착된 집적회로의 EEPROM에 저장된다. 이 스마트카드는 기록물로 판매되므로 정당한 사용자는 본 기록물을 청취 또는 시청할 수 있다. 해독 공정은 하기에 보다 상세히 기술되어 있다. 해독키 없이는, 기록물로 이루어진 어떠한 복사물도 판독될 수 없다. 아는 바와 같이, 스마트카드에 저장된 정보는 쉽게 복사될 수 없으며 스마트카드(은행, 전화 카드 등)가 사용되는 분야에서 공지된 어떠한 기술도 해독된 데이터로의 허가되지 않은 액세스를 방해하기 위하여 사용될 수 있다.

다른 실시예로, 키는 디지털 기록매체의 몸체 또는 하우징에 내장된 집적회로에 저장될 수 있다. 기록매체의 하우징내에 마이크로프로세서를 결합하는 기술은 공지된 기술이며 예를 들어 DVHS의 경우에 하우징 내부의 집적회로 또는 칩과 같은 전자회로를 유도하는 일련의 금속 접점이 카세트 하우징의 외부면에 설치될 수 있다. 이 접점은 접적회로와 비디오 레코더 사이의 통신이 가능하도록 레코더 리셉터클의 대응하는 일련의 접적에 의해 결합될 수 있다.

이러한 실시예는 사용자에게 판매되는 형태의 물리적인 기록물의 소유가 기록된 데이터의 실행에 필요한 조건이기 때문에 허가되지 않은 복사물을 동등하게 방지할 수 있다.

이하, 도 2를 참조하여 볼륨 요소 V의 해독 및 후속 재암호화에 포함된 단계를 설명한다. 상술한 바와 같이, 암호화 키 Kf와 다양화기 Cf의 값은 지원매체(2)와 관련된 스마트카드(4)에 장착된 집적회로에 저장된다. 기록물을 판독하기 위하여, 스마트카드(4)와 지원(2)은 판독기(5)의 적절한 슬롯에 삽입된다. 스마트카드는 공지되어 있으며 예를 들어 스마트카드 슬롯을 포함하기 위하여 CD ROM 또는 DVD 판독기의 변형은 제조공정의 견지에서 비교적 단순한 공정일 수 있다.

도 1의 암호화 방법에서와 같이, 키 Kf는 단계 6에서 스마트카드(4)에 저장된 제작상수 Cf 및 지원요소(2)로부터 판독된 암호화된 요소 E1(V)를 해독하기 위하여 단계 7에서 사용되는 다양화 키에 의해 다양화된다. 해독 공정은 스마트카드에서 수행되며 이후에 해독된 볼륨 요소 V는 기록물을 판독할 수 있도록 단계 8에서 판독기(5)로 제공된다.

간단한 실시예로, 암호화된 볼륨 요소 E1(V)는 지원(2)에 보유되며 카드(4)에 저장된 동일한 키 Kf와 상수 Cf는 이후의 모든 기록물의 판독에 사용될 수 있다. 그러나, 바람직한 실시예로, 해독된 볼륨 요소는 초기 값 E1(V)를 통해 지원 (2)에 기록된 새로운 암호화된 값 E2(V)를 형성하기 위하여 이후에 단계 9에서 재암호화된다.

볼륨요소 V는 스마트카드 자체의 집적회로내의 랜덤 또는 수도 랜덤 넘버 생성기(10)에 의해 생성된 랜덤 넘버 R을 기반으로 한 키를 사용하여 재암호화된다. 랜덤넘버 R는 기록물의 다음 판독시 볼륨 요소의 후속 해독이 가능하도록 스마트카드에 저장된다. 이 방식에서, 동일한 키 Kf와 다양화기 Cf를 사용하여 초기에 인코딩된 기록물의 일괄처리의 경우라도 본 실시예는 카드와 기록물의 급격한 차별화를 가능케한다.

바람직한 변형으로, 랜덤 넘버 키는 판독기(5)로부터 판독된 값, 예를 들어 그 일련번호 Ns를 사용하여 단계 11에서 다양화된다. 다양화기 값 Ns는 지원(2)의 재암호화된 볼륨요소 E2(V)와 함께 저장된다. 이 실시예에서, 값 Ns는 랜덤넘버 R와 함께 스마트카드(4)에 저장된다.

기록물의 다음 판독시에, 스마트카드(2)는 지원(2)에 저장된 값 E2(V)와 Ns와 함께 판독기(5)로부터 일련번호 Ns를 판독한다. 일련번호 Ns와 동일한 값이 판독기(5)와 지원(2)으로부터 판독되었다고 가정하면, 스마트카드는 기록물을 판독할 수 있도록 볼륨요소 V를 해독하기 위하여 저장된 랜덤넘버 값 R과 다양화기 Ns로부터 해독키를 생성한다. 이전과 같이, 새로운 랜덤 넘버가 생성되고 볼륨요소의 새로운 암호화 값이 지원(2)에서 생성되어 기록된다.

스마트카드(2)가 지원(2)과 판독기(5)로부터 일련번호 Ns와 동일한 값을 판독하지 않으면, 이것은 다른 판독기가 기록물을 판독하기 위하여 지금 사용되고 있다는 것을 나타낸다. 이것은 허가되지 않거나 또는 부당한 기록물의 사용을 나타낼 수 있더라도, 단지 사용자가 자신의 판독기를 대체하였거나 또는 판독기의 번호를 대체하였다는 것을 나타낼 수도 있다.

단지 판독기로부터 판독된 값 Ns를 거부하고 볼륨 요소를 해독하기 위하여 거부하도록 스마트카드가 프로그램되더라도, 다른 실시예는 제한된 수의 서로 다른 판독기가 데이터를 액세스할 수 있는 것이 바람직하다. 이러한 하나의 실시예로, 카드는, 일련번호 Ns의 값 사이에 미스매치하는 경우에 볼륨요소를 올바르게 해독하기 위하여 지원으로부터 판독된 일련번호가 랜덤 키를 다양화하는 데 사용되도록 프로그램된다.

그 후에, 판독기로부터 판독된 새로운 일련번호 Ns는 요소를 재암호화하기 위하여 사용되며 이 새로운 일련번호는 지원에 재암호화 볼륨요소와 함께 저장된다. 이 실시예에서, 새로운 일련번호는 이전의 일련번호를 대체한다. 카드는 지원의 일련번호의 제한된 수의 익스체인지(예를 들어 1 또는 2)만을 허용하도록 플래그 등에 의해 프로그램될 수 있다. 이 수가 전달될 후, 카드는 모든 후속 익스체인지를 거부하고, 부당한 기록물의 사용이 발생하였다고 판단한다.

다른 실시예로, 카드는 지원의 리스트에서 새로운 판독기의 일련번호를 저장하도록 프로그램될 수 있다. 각 판독시에, 카드는 판독기의 일련번호가 마지막에 사용된 판독기의 것과 대응하는지, 즉 마지막 기록시 볼륨 디스크립터를 암호화하기 위하여 사용되는 판독기 일련번호와 대응하는 지를 알기 위하여 체크한다. 대응하지 않다면, 마지막 판독시 볼륨 요소를 암호화하는 데 사용되는 일련번호가 볼륨 요소를 해독하는 데 사용하기 위한 지원으로부터 판독된다.

카드는 본 판독기의 일련번호가 지원에 이미 저장된 번호와 대응하는 지를 알기 위하여 체크한다. 대응하지 않다면, 새로운 《허가된》 일련번호가 리스트에 추가된다. 그리고, 이 새로운 일련번호는 다음 판독을 위한 볼륨 요소의 재암호화동안 랜덤 넘버를 다양화하는 데 사용된다.

리스트가 소정의 드레스홀드, 예를 들어 2 또는 3 허가된 판독기에 이르면, 카드는 리스트에 어떠한 다른 일련번호를 추가하기 위하여 거부할 수 있으며, 동시에 해독된 볼륨 요소를 디코더로 전송하기 위하여 거부할 수도 있다. 이러한 비교는 해독단계 이전에 행해질 수 있으므로, 카드는 판독기 번호가 허가된 판독기의 완전한 리스트에서 찾을 수 없는 경우에 볼륨 요소를 해독하기 위하여 거부할 것이다.
일련번호가 서로 순차적으로 기록된 실시예와 비교하여, 어떠한 부당한 의도없이 사용자에 의해 합리적으로 요구될 수 있기 때문에 사용자가 무한한 시간을 리스트의 어떠한 판독기 사이에서도 진행할 수 있다는 이점을 이 실시예는 포함한다.
상술한 구현물의 변형물은 이 기술분야의 당업자에게는 명백할 것이다. 예를 들면, 본 발명이 미리기록된 디스크 또는 디바이스와 관련하여 특별히 기술되었지만, 상술한 바와 같이 스마트카드 등과 관련하여 암호화될 수 있는 볼륨 디스크립터에 설치되기 때문에 동일한 원리가 블랭크 디지털 디스크 또는 카세트와 같은 블랭크 지원물에 적용될 수 있다.

삭제

삭제

디스크로의 매체의 첫번째 삽입에서, 관련 집적회로의 존재는 판독기가 어떠한 데이터를 블랭크 매체에 기록하기 이전에 볼륨 요소를 해독하는 데 필요할 것이다. 집적회로의 존재는 또한 매체에 최종적으로 기록된 정보의 무한한 복사물을 방지하기 위하여 이후의 모든 매체의 판독시 의무적일 것이다.

이상과 같이, 해독된 볼륨 디스크립터 요소는, 예를 들어 랜덤하게 생성된 키를 이용하여 그리고 블랭크 유닛에서 기록장치로 또는 지원에서 행해지는 두 가지 연속적인 기록 사이에서 지원의 합성의 변경과 관련된 볼륨 디스크립터 요소에 포함된 정보의 모든 변경을 고려하여 지원에서 재암호화 및 재기록될 수 있다.

(57) 청구의 범위

청구항 1.

제 1 해독키(Kf)를 포함하는 집적회로를 사용하여 디지털 지원매체(2)에 기록된 디지털 데이터로의 액세스를 제한하는 방법으로서:

대응하는 암호화 키(Kf)로 상기 지원매체의 볼륨 디스크립터(V)의 하나 이상의 요소를 암호화하는 단계;

상기 암호화된 볼륨 디스크립터 요소를 상기 지원매체의 비암호화 데이터와 함께 기록하는 단계; 및

상기 지원매체를 액세스할 경우에, 상기 볼륨 디스크립터의 암호화된 요소를 해독하고 이 요소를 판독기(5)에 제공하여 상기 지원매체의 비암호화 데이터의 판독 및/또는 기록을 가능하게 하도록 하는 집적회로 해독키를 사용하는 단계를 포함하고,

상기 볼륨 디스크립터의 하나 이상의 요소는 상기 지원매체에서 상기 비암호화 데이터를 액세스하는 데 미리 필요한 것을 특징으로 하는 방법.

청구항 2.

청구항 2은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 집적회로는 지원매체(2)와 관련된 스마트카드(4)에 내장되며, 상기 스마트카드는 암호화된 볼륨 요소를 해독하고 이것을 판독기로 전송하여 상기 기록된 데이터의 판독 및/또는 기록을 가능케하도록 하는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 3.

청구항 3은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 제 1 키(Kf)는 디지털 지원 매체의 하우징에 내장된 집적회로에 저장되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 4.

청구항 4은(는) 설정등록료 납부시 포기되었습니다.

제 1항 내지 3항중 어느 한 항에 있어서, 상기 제 1 키는 지원매체 또는 기록된 데이터의 식별과 관련된 값을 나타내는 상수(Cf)를 제작함으로써 다양화된 키(Kf)를 포함하는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 5.

청구항 5은(는) 설정등록료 납부시 포기되었습니다.

제 1항 내지 3항중 어느 한 항에 있어서, 상기 제 1 키(Kf)는 대칭 암호화 알고리즘에 사용가능한 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 6.

청구항 6은(는) 설정등록료 납부시 포기되었습니다.

제 1항에 있어서, 상기 볼륨 요소(V)는 집적회로에 생성 및 저장된 새로운 키(R)에 따른 집적회로에 의해 재암호화되며, 상기 재암호화된 볼륨요소는 이후에 판독기에 의해 매체에 기록되어 상기 이전에 암호화된 데이터를 대체하는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 7.

청구항 7은(는) 설정등록료 납부시 포기되었습니다.

제 6항에 있어서, 상기 새로운 키(R)는 집적회로의 랜덤 또는 수도 랜덤 넘버 생성기(GEN)에 의해 생성되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 8.

청구항 8은(는) 설정등록료 납부시 포기되었습니다.

제 6항에 있어서, 상기 집적회로에 의해 생성된 새로운 키(R)는 판독기로부터 집적회로에 의해 판독된 판독기의 식별과 관련된 값(Ns)에 의해 다양화되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 9.

청구항 9은(는) 설정등록료 납부시 포기되었습니다.

제 8항에 있어서, 상기 집적회로는 판독기로부터 판독하고, 그리고 둘 사이에 차이가 있는 경우에 지원매체로부터 이전의 판독기 식별값을 사용하여 볼륨 요소를 해독하고 그 후에 판독기로부터 얻은 새로운 판독기 식별값을 사용하여 볼륨 요소를 재암호화하는 지원매체에 저장된 판독기 식별 값(Ns)를 포함하는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 10.

청구항 10은(는) 설정등록료 납부시 포기되었습니다.

제 9항에 있어서, 상기 새로운 판독기 식별값(Ns)은 지원매체에 저장된 이전의 판독기 식별값을 대체하며, 상기 식별값의 대체의 소정의 수 만이 허용되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 11.

청구항 11은(는) 설정등록료 납부시 포기되었습니다.

제 9항에 있어서, 상기 새로운 판독기 식별값(Ns)은 지원매체의 허가된 판독기의 리스트에 저장되며, 상기 판독기의 선택된 번호만이 리스트에 허용되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 12.

청구항 12은(는) 설정등록료 납부시 포기되었습니다.

제 1항 내지 3항, 제 6항 내지 11항중 어느 한 항에 있어서, 상기 지원매체(2)는 비암호화된 디지털 데이터로 미리 기록되는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 13.

청구항 13은(는) 설정등록료 납부시 포기되었습니다.

제 1항 내지 3항, 제 6항 내지 11항중 어느 한 항에 있어서, 상기 지원매체(2)는 판독기로의 첫번째 삽입 이전에는 블랭크이며, 관련 집적회로의 존재는 판독기가 블랭크 매체에 어떠한 데이터를 기록하기 이전에 볼륨 요소를 해독하는 데 필요한 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 14.

청구항 14은(는) 설정등록료 납부시 포기되었습니다.

제 1항 내지 3항, 제 6항 내지 11항중 어느 한 항에 있어서, 상기 데이터는 시청각 데이터를 포함하는 것을 특징으로 하는 기록된 디지털 데이터로의 액세스를 제한하는 방법.

청구항 15.

제 1키에 의해 지원매체와 관련된 볼륨 디스크립터의 하나 이상의 요소를 암호화하고, 지원매체와 관련된 집적회로에 볼륨 디스크립터를 해독하는 데 필요한 제 1 키의 등가물을 저장하는 단계를 포함하는 제 1항 내지 3항중 어느 한 항의 방법에 사용하기 위한 디지털 지원매체 및 집적회로를 제조하는 방법.

청구항 16.

청구항 16은(는) 설정등록료 납부시 포기되었습니다.

제 15항에 있어서, 상기 집적회로는 디지털 지원매체와 관련된 스마트카드에 내장되는 것을 특징으로 하는 디지털 지원매체 및 집적회로를 제조하는 방법.

청구항 17.

청구항 17은(는) 설정등록료 납부시 포기되었습니다.

제 15항에 있어서, 상기 집적회로는 디지털 지원매체의 하우징에 내장되는 것을 특징으로 하는 디지털 지원매체 및 집적회로를 제조하는 방법.

청구항 18.

볼륨 디스크립터(V)에 하나 이상의 요소를 포함하는 디지털 지원매체에 기록된 디지털 데이터의 보호 시스템으로서, 상기 시스템은:

제 1 해독키(Kf)를 포함하는 집적회로;

대응하는 암호화 키(Kf)로 상기 볼륨 디스크립터(V)의 하나 이상의 요소를 암호화하는 암호화 수단;

상기 암호화된 볼륨 디스크립터 요소를 상기 지원매체의 비암호화 데이터와 함께 기록하는 기록 수단; 및

상기 지원매체를 액세스할 경우에 상기 볼륨 디스크립터의 암호화된 요소를 해독하고 이 요소를 판독기(5)에 제공하여 상기 지원매체의 비암호화 데이터의 판독 및/또는 기록을 가능하게 하도록 하는 집적회로 해독키를 사용하는 수단을 포함하고,

상기 볼륨 디스크립터의 하나 이상의 요소는 상기 지원매체에서 상기 비암호화 데이터를 액세스하는 데 미리 필요한 것을 특징으로 하는 시스템.

청구항 19.

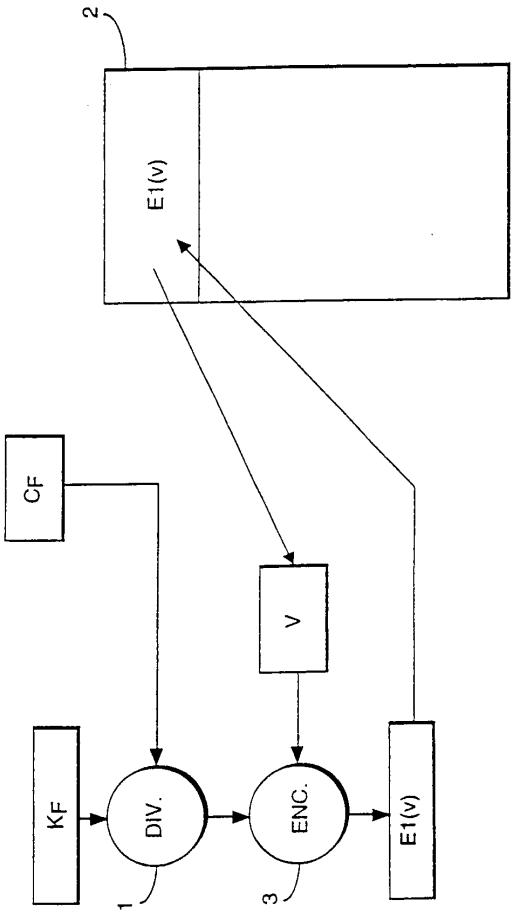
제 18항의 시스템에 사용되는 디지털 지원매체와 집적회로를 제조하는 장치로서, 상기 장치는:

제 1 키에 의해 상기 지원매체와 관련된 볼륨 디스크립터의 하나 이상의 요소를 암호화하는 수단; 및

상기 지원매체와 관련된 집적회로에서 볼륨 디스크립터를 해독하는데 필요한 상기 제 1 키의 등가물을 저장하는 수단을 포함하는 장치.

도면

도면1



도면2