(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04N 5/913 (2006.01)

(45) 공고일자 2006년03월30일
(11) 등록번호 10-0565469
(24) 등록일자 2006년03월22일

(21) 출원번호 10-2000-7003207
(22) 출원일자 2000년03월24일
번역문 제출일자 2000년03월24일
(86) 국제출원번호 PCT/IB1998/001511
국제출원일자 1998년09월22일

(65) 공개번호 10-2001-0030707
(43) 공개일자 2001년04월16일
(87) 국제공개번호 WO 1999/16244
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 97402238.6 1997년09월25일 유럽특허청(EPO)(EP)

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

(72) 발명자
메일라드, 미쳴
프랑스, 에프 78120 람보우일렛, 애버뉴 듀 파크, 13

(74) 대리인
최홍순
조성욱
박세걸
특허법인세신

심사관 : 최훈

(54) 디지털 정보 기록 방법, 디코더 및 스마트 카드의 결합 장치, 및 스마트 카드

요약

암호화된 정보(Ce)의 전송 및 기록을 위한 방법으로서 정보(Ce)는 제 1키에 의해 암호화되고 암호화된 형태로 전송되고, 암호화된 정보(Ce)는 정보를 해독하는데 필요한 제 1 키의 동등물을 포함하는 디코더(2020)에 의해 수신되고, 상기 해독된 정보(Ce)는 디코더(2020) 및/또는 디지털 기록장치(4005)에 의해 수신될 휴대용 지원장치(4004)에 저장된 제 2 키(C2)에 의해 재암호화되고, 재암호화된 정보는 디지털 기록매체(4006)에 기록되는 것을 특징으로 한다. 기록물을 재생할 때, 이 정보가 지원수단(4004)에 저장된 제 2 키(C2)에 의해 해독된다. 특별히 바람직한 실시예로, 이 정보(Ce)는 전송된 데이터를 스크램블 및 디스크램블하는 데 사용되는 제어워드에 해당하고, 재암호화된 제어워드(Ce)는 스크램블된 전송된 데이터와 함께 기록매체(4006)에 저장된다.

대표도

도 5

색인어

암호화된 디지털 데이터, 텔레비젼 방송, 디코더

명세서

기술분야

본 발명은 스크램블된 디지털 데이터, 예를 들어 텔레비젼 방송을 기록하는 방법, 디코더 및 스마트 카드의 결합 장치, 및 스마트 카드에 관한 것이다.

배경기술

암호화된 데이터의 전송은 스크램블된 음성영상 정보가 전송된 프로그램을 시청하기 위하여 디스크램블할 수 있는 디코더 또는 리시버/디코더를 소유한 다수의 가입자에게 전형적으로 위성으로 방송되는 유료 TV 시스템 분야에서 공지되어 있다.

전형적인 시스템에서, 스크램블된 디지털 데이터는 디지털 데이터의 디스크램블링용 제어 워드와 함께 전송되며, 이 제어 워드 자체는 제 1키에 의해 암호화되고 암호화된 형태로 전송되고, 스크램블된 디지털 데이터와 암호화된 코드워드는 암호화된 코드워드를 해독하고 그리고 나서 전송된 데이터를 디스크램블하는 데 필요한 제 1키의 동등물을 갖는 디코더에 의해 수신되고, 디코더는 스크램블된 형태의 디지털 데이터를 디지털 기록장치로 전송한다. 비용을 지불한 가입자는 특정 프로그램을 시청할 수 있도록 암호화된 제어 워드를 해독하는 데 필요한 키를 월별로 수신할 것이다.

디지털 기술의 도래로, 전송된 데이터의 품질이 개선되고 있다. 디지털 데이터와 관련된 특별한 문제점은 복사가 용이하다는 것이다. 디스크램블된 프로그램이 표준 VCR로 시청 및 기록하는 아날로그 링크(예를 들어, "페리텔(Peritel)" 링크)를 통하여 전송될 경우에는 그 품질은 표준 아날로그 카세트 기록과 관련된 품질보다 좋지 않다. 따라서, 해적판을 만들기 위하여 이러한 기록물을 마스터 테잎으로서 사용할 위험성은 아날로그 카세트를 취급하는 일반적인 점포가 갖는 위험성보다 높지 않다.

대조적으로, 직접적인 디지털 링크에 의해 새로운 세대의 디지털 기록장치중 하나(예를 들면, DVHS 레코더)로 전송되는 디스크램블된 디지털 데이터는 원래 전송된 프로그램과 동일한 품질일 수 있기 때문에 화상 또는 음성 품질의 어떠한 저하도 없이 여러번 복사될 수 있다. 따라서, 디스크램블된 데이터가 디지털 복사물 또는 심지어 간단한 아날로그 VHS 복사물을 만들기 위하여 마스터 기록물로서 사용될 수 있는 위험성을 가지고 있다.

프랑스 특허출원 제 95 03859호에는 디스크램블된 디지털 데이터가 디지털 기록매체에 결코 기록될 수 없도록 하는 시스템으로 이 문제를 극복하는 것을 나타낸다. 대신에, 이 출원에 설명된 디코더는 다른 키에 의해 재암호화된 데이터를 디스크램블하는 데 필요한 제어 워드와 함께, 기록 매체에 스크램블된 형태로 데이터를 기록한다. 이 새로운 키는 리시버/디코더에만 알려져 있으며 프로그램의 시청을 위한 코드워드를 얻는데 필요한 제 1키를 대체한다.

이러한 시스템의 장점은, 데이터가 결코 "클리어한" 형태로 저장되지 않으며 리시버/디코더에 저장된 새로운 키를 갖지 않고서는 시청될 수 없다는 것이다. 이 시스템은, 제 1키가 월별로 변경되기 때문에 디지털 테이프에 등록된 제어워드를 재암호화하기 위하여 일정한 키를 사용한다는 것은 가입한 달의 종료후에도 리시버 /디코더가 테이프에 기록된 제어워드를 여전히 해독할 수 있다는 것을 의미한다는 장점을 가지고 있다.

이 특허 출원에서 제시된 시스템의 단점은 기록물이 특정한 리시버/디코더와 결합해서만 시청될 수 있다는 것이다. 이 디코더가 고장나거나 대체되면 기록물을 더 이상 재생할 수 없다. 마찬가지로, 시스템에 리시버/디코더를 연결하지 않고 디지털 레코더에서 직접적으로 기록물을 재생하는 것이 불가능하기 때문에 이미 전송된 필름을 시청할 수 있도록 디코더를 유지하기 위하여 시청자는 유료 TV 회사와의 가입을 지속하여야 한다.

발명의 상세한 설명

본 발명의 목적은 전송된 데이터의 해적판을 만드는 데 용이하게 사용할 수 없는 안전한 디지털 데이터의 기록물을 유지하면서 이 해결책과 관련된 문제를 극복할 수 있는 디코더 및 스마트 카드의 결합 장치, 및 스마트 카드를 제공하는 것이다.

본 발명은 제 1 키에 의해 암호화되고 암호화된 형태로 전송되고 상기 정보를 해독하는 데 필요한 제 1 키의 동등물로 액세스하는 디코더에 의해 수신된 암호화된 디지털 정보의 전송 및 기록 방법을 포함하며, 이 방법은 상기 해독된 정보가 디코더 또는 관련 디지털 레코더에 의해 수신될 휴대용 지원장치에 저장된 제 2키에 의해 재암호화되고 나서 상기 재암호화된 정보가 디지털 레코더에 의해 디지털 기록 매체에 기록되는 것을 특징으로 한다.

이 방식에서, 본 발명은 기록된 데이터의 재생이 디코더의 식별과 무관하기 때문에 종래 기술의 문제점을 극복한다. 기록물을 재생할 경우에 이 정보는 지원 수단에 저장된 제 2키에 의해 해독된다.

새로운 디코더가 제 2키를 포함하는 지원장치를 수용하는 리셉터클을 갖는 한 디코더의 교체하더라도 그 기록물을 무용지물로 하지 않을 것이다. 적절한 리더(reader)가 설치되면, 디지털 레코더는 제 2키를 판독하여 디코더 없이 상기 정보를 재생할 수 있다. 쉽게 고장날 수 있는 비교적 복잡한 장치인 디코더와는 달리 휴대용 지원 장치는 간단한 형태로 구현될 수 있다.

제 2키에 의해 재암호화되고 디지털 기록 매체에 저장된 정보는 음성영상 정보에 해당할 수 있다. 그러나, 바람직한 실시예로, 디지털 정보는 스크램블된 디지털 데이터를 디스크램블하는 제어워드에 해당하며, 스크램블된 디지털 데이터는 제 1키에 의해 암호화된 제어워드와 함께 전송되고 제어워드는 동등한 제 1키에 의해 해독되고 제 2키에 의해 재암호화되고 재암호화된 제어워드와 스크램블된 데이터는 디지털 기록 매체에 기록된다.

특히 바람직한 실시예로, 휴대용 지원장치는 디코더 및/또는 디지털 레코더의 스마트카드 판독기에 수용될 스마트카드이다. 이 출원에서 용어 "스마트카드"는 예를 들면 마이크로프로세서 또는 제 2키 알고리즘을 저장하는 EEPROM을 구비하는 종래의 모든 칩기반 카드 장치를 의미하는 데 사용된다. 이 용어에는 TV 디코더 시스템에서 종종 사용되는 다른 물리적인 형태의 칩 장치, 예를 들면 키 형상 장치도 포함된다.

일 실시예로, 스마트카드는 초기 데이터의 디스크램블을 위한, 예를 들어 텔레비젼 방송 시스템의 경우에 시청을 위한 제어워드를 해독하는 데 사용되는 제 1키의 동등물도 포함한다. 이러한 경우에, 스마트카드는 유료 TV 시스템의 일부를 형성하며 어느 가입자가 월말에 업데이트된 제 1 키를 수신할 것인지를 송신기가 선택적으로 식별할 수 있도록 상기 송신기에 알려진 비밀키도 포함할 수 있다.

다른 실시예로, 제 2키는 제 1키를 저장하기 위해 사용된 것과 다른 스마트카드에 저장된다. 따라서, 이러한 실시예에서, 디지털 매체에 저장된 정보의 판독은 가입자 시스템과 완전히 별개이며, 가입자가 시스템으로부터 탈퇴하여 가입 카드가 탈퇴된 후라도 가입자는 스마트카드를 판독하기 위하여 소유한 디지털 레코더 /플레이어에 제공된 이전에 기록된 필름을 계속 시청할 수 있다.

이러한 시스템에서, 하나의 스마트카드와 제 2키는 다수의 기록용 재암호화 코드워드를 생성하기 위하여 사용될 수 있다. 이러한 방식에서, 하나의 "대출 카드"는 어떠한 수의 기록물을 해독하는 데에도 사용될 수 있다.

일 실시예로, 스마트카드는 기록물이 얼마나 많이 재생될 수 있는 지를 판단하기 위하여 기록물의 부분 재생 또는 완전한 재생만큼 감소하는 다수의 신용단위도 포함할 수 있다. 이 신용단위는 예를 들어 전송된 제 1키와 함께 메시지에 다운로드될 수 있다.

일 실시예로 신용 단위는 기록물의 특정한 세그먼트와 관련되어 있어 기록물의 섹션을 재생, 예를 들어 기록물의 처음 또는 마지막 15분을 이 섹션과 관련된 소정의 신용단위를 감소시킬 것이다. 대안적으로, 신용 단위는 하나의 형태이고 기록물의 어떠한 섹션의 재생으로도 감소된다.

상술한 바와 같이, 본 발명은 기록매체와 관련된 스마트카드에 제 2 키 알고리즘이 저장되는 경우에 특히 적용가능하다. 그러나, 다른 실시예로, 휴대용 지원물은 기록 그 자체에 의해 정의되며, 제 2 키는 디지털 기록매체의 하우징에 내장된 집적 회로에 저장된다.

이러한 기술은 예를 들어 DVHS 카세트의 경우에 하우징의 내부에 집적회로 또는 칩과 같은 전자회로로 유도하는 일련의 금속접점이 카세트 하우징의 외부면에 설치될 수 있는 경우에 이미 제안되었다. 이 접점은 집적회로와 비디오 레코더 사이의 통신이 가능하도록 레코더의 리셉터클의 대응하는 일련의 접점에 의해 결합될 수 있다.

이러한 시스템에서, 키가 기록물로 전송된다는 점에도 불구하고 이 키는 내장된 칩에서 쉽게 복사될 수 없기 때문에 보안성은 여전히 제공된다. 스마트카드 실시예에 관하여 상기에 설명된 변형물은 지원물이 기록 하우징에 의해 정의되는 시스템에 동등하게 적용될 수 있다.
본 발명의 다른 양상에 의하면, 본 발명은 디코더 및 스마트 카드로 이루어진 결합 장치로서, 상기 디코더는 제 1 키에 의해 암호화된 디지털 정보를 수신하고 상기 디지털 정보를 해독하는 데 필요한 상기 제 1 키의 동등물을 액세스하고, 상기 스마트 카드는 상기 디코더의 스마트카드 리더에 수용되고, 디지털 기록매체로의 기록을 위한 디지털 기록장치로의 전송을 위한 상기 해독된 정보를 재암호화하는 제 2 키를 가지고 있고, 기록물이 몇 회 재생될 수 있는 지를 판단한 다수의 신용단위를 포함하며, 각 기록물의 부분 실행 또는 완전한 재생으로 상기 신용 단위의 수를 감소시키도록 배열되는 디코더 및 스마트 카드의 결합 장치를 제공한다.

본 발명은 스크램블된 데이터가 스크램블된 텔레비젼 방송에 전송된 음성영상 데이터를 나타내는 방법에 특히 적용가능하다.

본 발명은 방법과 관련하여 상기에 설명되었지만 장치에도 동등하게 적용가능하다.

용어 "스크램블된(scrambled)"와 "암호화된(encrypted)"와 "제어워드(contr ol word)"와 "키(key)"는 언어의 명료성을 위해 여기에 사용되었다. 그러나, "스크램블된 데이터(scrambled data)"와 "암호화된 데이터(encrypted data)"간에 또는 "제어 워드(control word)"와 "키(key)"간에는 근본적인 구별이 있을 필요가 없다는 것이 이해될 것이다. 유사하게, 상세 설명에서 "리시버/디코더(receiver/decoder)"와 "디코더(decoder)"로 언급되었지만, 본 발명은 물리적으로 분리된 리시버와 결합하여 기능하는 디코더 장치에 대하여 디코더와 통합된 리시버를 갖는 실시예에도 동등하게 적용할 수 있다는 것이 이해될 것이다. 본 발명은 디코더가 텔레비젼 또는 디지털 비디오 레코더와 같은 장치와 통합되는 실시예에도 동등하게 확장된다.

첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 예로서만 설명한다.

도면의 간단한 설명

도 1은 본 발명에 따른 디지털 정보 기록 방법에 적용 가능한 디지털 기록장치와 상호동작할 수 있는 디지털 텔레비젼 시스템의 전체 구성도.

도 2는 도 1의 텔레비젼 시스템의 조건부 액세스 시스템을 나타낸 도면.

도 3은 텔레비젼 시스템에서의 다른 레벨의 암호화를 나타낸 도면.

도 4는 영상, 음성 및 텔레텍스트와 ECM 메시지 성분을 포함하는, 텔레비젼 시스템의 전송된 디지털 패킷의 구조도.

도 5는 디지털 기록장치와 디지털 비디오 카세트에 등록될 코드 워드를 암호화하기 위하여 사용된 제 2 알고리즘을 포함하는 스마트카드를 포함하는 본 발명의 제 1 실시예를 나타낸 도면.

도 6은 프로그램이 시청될 수 있는 회수를 판단하는 신용단위와 함께 각각 전송 및 기록된 프로그램을 시청하는 데 필요한 제 1 및 제 2 키를 스마트카드가 포함하는 본 발명의 제 2 실시예를 나타낸 도면.

도 7은 제 2키가 디지털 비디오 카세트의 케이스에 장착된 집적회로에 저장된 본 발명의 제 3 실시예를 나타낸 도면.

실시예

디지털 텔레비젼 시스템

도 1은 본 발명에 따른 디지털 기록 방법에 적용 가능한 디지털 텔레비젼 방송 및 수신 시스템(1000)의 개략도이다. 이 시스템은 압축된 디지털 신호를 전송하기 위하여 공지된 MPEG-2 압축 시스템을 사용하는 가장 종래의 디지털 텔레비젼 시스템(2000)을 포함한다. 보다 상세하게는, 방송 센터의 MPEG-2 압축기(2002)는 디지털 신호 스트림(통상적으로 영상 신호의 스트림)을 수신한다. 압축기(2002)는 링크(2006)에 의해 멀티플렉서 및 스크램블러(2004)에 연결된다. 멀티플렉서(2004)는 다수의 입력신호를 수신하고, 하나 이상의 이송 스트림을 모으고, 물론 텔레콤 링크를 포함하는 다양한 형태를 취할 수 있는 링크(2010)를 경유하여 방송 센터의 송신기(2008)에 압축된 디지털 신호를 전송한다. 송신기(2008)는 업링크(2012)를 경유하여 위성 트랜스폰더 (2014)를 향하여 전자기 신호를 전송하고, 이 전자기 신호는 일반적으로 최종 사용자에 의해 소유 또는 임대되는 접시 형태의 지상 수신기(2018)로 가공의 다운링크 (2016)를 경유해서 전자적으로 처리 및 방송된다. 수신기(2018)에 의해 수신된 신호는 최종 사용자에 의해 소유 또는 임대되고 최종 사용자의 텔레비젼 세트(2022)에 연결된 통합 리시버/디코더(2020)로 전송된다. 리시버/디코더(2020)는 압축된 MPEG-2 신호를 텔레비젼 세트(2022)용 텔레비젼 신호로 디코딩한다.

조건부 액세스 시스템(3000)은 멀티플렉서(2004)와 리시버/디코더(2020)에 연결되고, 방송 센터에 부분적으로 그리고 디코더에 부분적으로 위치한다. 이것은 하나 이상의 방송 공급자로부터의 디지털 텔레비젼 방송을 최종 사용자가 액세스할 수 있도록 한다. 상업적 제공(즉, 방송 공급자에 의해 판매되는 하나 또는 몇 개의 텔레비젼 프로그램)과 관련된 메시지를 해독할 수 있는 스마트카드가 리시버/디코더(2020)에 삽입될 수 있다. 디코더(2020)와 스마트카드를 이용하여, 최종 사용자는 가입 모드 또는 유료시청 모드로 사상을 구매할 수 있다.

멀티플렉서(2004)와 리시버/디코더(2020)에 연결되고 부분적으로 방송 센터에 부분적으로 디코더에 위치된 쌍방향 시스템(4000)은 최종 사용자가 모뎀드 백 채널(4002)을 통하여 다양한 애플리케이션과 대화할 수 있도록 한다.

조건부 액세스 시스템

삭제

도 2를 참조하면, 조건부 액세스 시스템(3000)은 가입자 인증 시스템 (Subscriber Authorization System:SAS)(3002)을 포함한다. SAS(3002)는 (다른 타입의 링크도 사용될 수 있지만) 각 TCP-IP 링크(3006)에 의해 하나 이상의 가입자 관리 시스템(Subscriber Management System:SMS)(3004)에 연결되며, 하나의 SMS는 각 방송공급자용이다. 대안적으로, 하나의 SMS가 두 방송 공급자 사이에서 공유되거나, 또는 하나의 공급자가 2개의 SMS를 사용할 수 있다.

"모(mother)" 스마트카드(3010)를 사용하는 암호화 유닛(3008) 형태의 제 1암호화 유닛은 링크(3012)에 의해 SAS로 연결된다. 모 스마트카드(3016)를 사용하는 암호화 유닛(3014)의 형태인 제 2 암호화 유닛은 링크(3018)에 의해 멀티플렉서 (2004)에 연결된다. 리시버/디코더(2020)는 "도터(daughter)" 스마트카드(3020)를 수용한다. 이것은 모뎀드 백 채널(4002)을 통하여 통신 서버(3022)에 의해 SAS (3002)로 직접 연결된다. SAS는 요구시 도터 스마트카드로 그중에서도 특히 가입자 권한을 전송한다.

스마트카드는 하나 이상의 상업적인 운용자 비밀을 포함한다. "모" 스마트카드는 서로 다른 종류의 메시지를 암호화하고 "도터" 스마트카드는 그렇게 할 수 있는 권한을 가지면 메시지를 해독한다.

제 1 및 제 2 암호화 유닛(3008 및 3014)은 랙(rack)과, EEPROM에 저장된 소프트웨어를 갖는 20개에 이르는 전자카드인 전자 VME 카드와, 각 전자카드에 대하여 ECM을 암호화하는 스마트카드(3016)와, EMM를 암호화하는 스마트카드(3010)인 하나의 스마트카드(3010 및 3016)을 포함한다.

이상과 같이, ECM 또는 자격관리 메시지는 전송된 프로그램의 데이터 스트림에 포함된, 프로그램의 해독에 필요한 제어워드를 포함하는 암호화 메시지이다. 주어진 리시버/디코더의 인증은 EMM 또는 자격관리 메시지에 의해 제어되고, 예를 들어 매달 전송되고, 인증된 리시버/디코더에 ECM을 디코딩하는 데 필요한 키를 제공한다.

이하, 텔레비젼 시스템(2000) 및 조건부 액세스 시스템(3000)의 다양한 부품을 참조하여 디지털 텔레비젼 시스템의 조건부 액세스 시스템(3000)의 동작이 보다 상세히 기술된다.

멀티플렉서 및 스크램블러

삭제

도 1및 2를 참조하면, 방송센터에서 디지털 영상 신호는 MPEG-2 압축기 (2002)를 사용하여 압축되거나 (또는 비트율이 감소된다). 그리고, 이 압축된 신호는 링크(2006)를 통하여 멀티플렉서 및 스크램블러(2004)로 전송되어 다른 압축 데이터와 같은 데이터와 함께 멀티플렉스된다.

스크램블러는 스크램블링 처리에서 사용되고 멀티플렉서(2004)의 MPEG-2 스트림에 포함된 제어워드 Ce를 생성한다. 제어워드 Ce는 내부적으로 생성되고 최종 사용자의 통합 리시버/디코더(2020)가 프로그램을 디스크램블할 수 있도록 한다. 프로그램이 어떻게 상업화되는 지를 나타내는 액세스 기준도 MPEG-2 스트림에 부가된다. 프로그램은 다수의 "가입" 방식중 하나 및/또는 다수의 "유료시청 방식(Pay Per View:PPV)" 또는 사상중 하나로 상업화될 수 있다. 가입 방식에서, 최종 사용자는 하나 이상의 상업적 제공, "보우케이(bouquets)"에 가입하여 그 보우케이 내의 모든 채널을 볼 권한을 얻게 된다. 바람직한 실시예로, 960개에 이르는 상업적 제공이 채널의 보우케이로부터 선택될 수 있다. 유료 시청 방식에서는 최종 사용자가 원하는 만큼 사상을 구매할 수 있는 능력이 제공된다. 이것은 미리 사상을 사전 예약("사전 예약 방식")함으로써 또는 방송되자마자 사상을 구매("임펄스 방식")함으로써 이루어질 수 있다.

삭제

제어 워드(Ce)와 액세스 기준은 자격관리 메시지(Entitlement Control Message:ECM)를 형성하기 위해 사용되고; 이것은 하나의 스크램블된 프로그램과 관련하여 전송된 메시지이고; 이 메시지는 (프로그램의 디스크램블링을 가능케하는) 제어워드 및 방송 프로그램의 액세스 기준을 포함한다. 액세스 기준 및 제어 워드는 링크(3018)를 통하여 제 2 암호화 유닛(3014)으로 전송된다. 이 유닛에서, ECM이 생성되고, 제 1키 Cex로 암호화되고 멀티플렉서 및 스크램블러(2004)로 전송된다.

방송 공급자에 의해 방송되는 데이터 형태의 각 서비스는 다수의 별개의 성분을 포함하고; 예를 들어 텔레비젼 프로그램은 영상성분 V, 음성성분 S, 부제 또는 텔레텍스트 성분 T 등을 포함한다(도 4 참조). 이러한 서비스 성분의 각각은 트랜스폰더(2014)로의 후속 방송을 위하여 개별적으로 스크램블 및 암호화된다. 각각의 스크램블된 서비스 성분에 대하여 별개의 ECM이 요구된다.

프로그램 전송

삭제

멀티플렉서(2004)는 SAS(3002)로부터 암호화된 EMM, 제 2암호화 유닛(3014)으로부터 암호화된 ECM, 및 압축기(2002)로부터 압축된 프로그램을 포함하는 전기 신호를 수신한다. 멀티플렉서(2004)는 프로그램을 스크램블하고 스크램블된 프로그램, (존재한다면) 암호화된 EMM 및 암호화된 ECM을 전기적 신호로서 링크(2010)를 통하여 방송센터(2008)의 송신기(2008)로 전송한다. 송신기(2008)는 업링크(2012)를 통하여 위성 트랜스폰더(2014)를 향해 전자기 신호를 전송한다.

프로그램 수신

삭제

위성 트랜스폰더(2014)는 송신기(2008)에 의해 전송된 전자기 신호를 수신 하여 처리하고 다운링크(2016)를 경유해서, 일반적으로 최종 사용자에 의해 소유 또는 임대되는 접시 형태의 지상 수신기(2018)로 신호를 전송한다. 수신기(2018)에 의해 수신된 신호는 최종 사용자에 의해 소유 또는 임대되고 최종 사용자의 텔레비젼 세트(2022)에 연결되는 통합 리시버/디코더(2020)로 전송된다. 리시버/ 디코더 (2020)는 스크램블된 프로그램을 암호화된 EMM과 암호화된 ECM으로 얻기 위하여 신호를 디멀티플렉스한다.

프로그램이 스크램블되지 않으면, 리시버/디코더(2020)는 데이터를 압축해제하고 이 신호를, 텔레비젼 세트(2022)로 전송하기 위한 영상 신호로 변환시킨다.

프로그램이 스크램블되면, 리시버/디코더(2020)는 MPEG-2 스트림으로부터 그 대응하는 ECM을 추출하고 최종 사용자의 "도터" 스마트카드(3020)"로 ECM을 전송한다. 이것은 리시버/디코더(2020)의 하우징으로 인입된다. 도터 스마트카드(3020)는 ECM을 해독하고 프로그램에 액세스할 권한을 최종 사용자가 가지고 있는 지를 제어한다.

사용자가 필요한 권한을 갖지 않으면, 프로그램이 디스크램블될 수 없다는 것을 나타내기 위하여 네가티브 상태가 리시버/디코더(2020)로 전송된다. 최종 사용자가 권한을 가지면, ECM은 해독되고 제어 워드가 추출된다. 그리고, 디코더(2020)는 이 제어워드를 사용하여 프로그램을 디스크램블할 수 있다. MPEG-2 스트림은 압축해제되고 텔레비젼 세트(2022)로 전송하기 위한 영상 신호로 변환된다.

사용되는 암호화 레벨이 하기에 도 3을 참조하여 보다 상세하게 설명된다.

가입자 관리 시스템(SMS)

삭제

가입자 관리 시스템(SMS)(3004)은 그중에서도 특히 모든 최종 사용자 파일, 상업적 제공(요금 및 상품 등), 가입, PPV 항목, 및 최종 사용자 소비 및 인증에 관한 데이터를 관리하는 데이터베이스(3024)를 포함한다. SMS는 SAS로부터 물리적으로 이격될 수 있다.

각 SMS(3004)는 자격관리 메시지(EMM)의 수정물 또는 작성물이 최종 사용자에게 전송될 수 있도록 각 링크(3006)를 통하여 SMS(3002)로 메시지를 전송한다.
SMS(3004)는 EMM의 변형 또는 작성을 의미하지 않고, (제품 주문시 최종 사용자에게 인증 또는 최종 사용자가 지불할 양에 관련된) 최종 사용자의 상태변경만을 의미하는 메시지를 SAS(3002)로 전송한다.

자격관리 메시지(EMM)

삭제

삭제

EMM은 (하나의 스크램블된 프로그램만 또는 일련의 스크램블된 프로그램들에 전용되는 ECM과 대조적으로) 개개의 최종 사용자(가입자) 또는 최종 사용자의 그룹에 전용된 메시지이다. 그룹은 설정된 수의 최종 사용자를 포함할 수 있다. 이러한 그룹 구성은 대역폭을 최적화하는 것을 목적으로 하며, 즉 한 그룹으로의 액세스는 많은 수의 최종 사용자로의 도달을 가능케 할 수 있다.

다양한 형태의 EMM이 본 발명을 실행하는 데 사용된다. 개개의 EMM은 개개의 가입자에게 전용되고, 전형적으로 유료 시청 방식 서비스 제공시 사용되며, 이것은 그룹 식별자와 이 그룹의 가입자 위치를 포함한다. 소위 "그룹" 가입 EMM은 가령 256개의 개별적인 사용자 그룹에 전용되고, 전형적으로 가입 서비스의 관리에 사용된다. 이 EMM은 그룹 식별자 및 가입자의 그룹 비트맵을 갖는다. 시청자(Audience) EMM은 모든 시청자에게 전용되고, 예를 들어 소정의 무료 서비스를 제공하기 위하여 특별한 운용자에 의해 사용될 수 있다. "시청자"는 동일한 운용자 식별자 (Operater Identifier:OPI)를 갖는 스마트카드를 구비한 가입자의 완전성이다. 결국, "유일한" EMM이 스마트카드의 유일한 식별자에 어드레스된다.

시스템의 암호화 레벨

삭제

도 3을 참조하여 방송 시스템의 암호화 레벨이 설명된다. 디지털 데이터의 방송과 관련된 암호화 단계는 참조부호(4001)로 나타내고, 전송 채널(예를 들면, 상술한 바와 같은 위성 링크)는 참조부호(4002)로 나타내고, 수신기의 해독 단계는 참조부호(4003)로 나타낸다.

디지털 데이터(N)는 멀티플렉서 Mp로 전송되기 이전에 제어워드 Ce에 의해 스크램블된다. 도 4에서 알 수 있듯이, 전송된 데이터는 제 1암호화 키 Cex에 의해 제어된 암호화기 Ch1에 의해 암호화된 그중에서 특히 제어워드 Ce를 포함하는 ECM을 포함한다. 리시버/디코더에서, 신호는 시청을 위하여 텔레비젼(2022)으로 전송되기 이전에 디멀티플렉서 DMp 및 디스크램블러 D에 의해 전송된다. 키 Cex를 갖는 해독 유닛 DCh1은 신호를 디스크램블하는 데 사용되는 제어워드 Ce를 얻기 위하여 디멀티플렉스된 신호의 ECM을 해독한다.

보안성을 이유로, 암호화된 ECM에 내장된 제어워드 Ce는 평균적으로 10초마다 변경된다. 대조적으로, ECM을 디코드하기 위해 수신기에 의해 사용되는 제 1암호화키 Cex는 EMM에 의해 매달 변경된다. 암호화키 Cex는 디코더의 식별에 대응하는 비밀키 Cg를 사용하여 제 2 유닛 ChP에 의해 암호화된다. 디코더가 업데이트된 키 Cex를 수용하기 위하여 선택된 것중 하나라면, 디코더의 해독 유닛 DChP은 해당 달의 키 Cex를 얻기 위하여 키 Cg를 사용하여 메시지를 해독한 것이다.

해독 유닛(DChp 및 DCh1)과 관련 키는 가입자에 제공된, 디코더의 스마트카드 리더에 삽입되는 스마트카드에 유지된다. 키는 DES등의 공지된 대칭 키 알고리즘에 의해 생성될 수 있다. 공개/비밀키 알고리즘을 사용하는 다른 실시예도 가능하다.
상기 스마트 카드는 제 1 키에 의해 암호화된 디지털 정보를 수신하고 상기 디지털 정보를 해독하는 데 필요한 제 1 키의 동등물을 액세스한다. 상기 스마트 카드는 디지털 기록매체로의 기록을 위한 디지털 기록장치로의 전송을 위한 상기 해독된 정보를 재암호화하는 제 2 키를 가지고 있고, 기록물이 몇 회 재생될 수 있는 지를 판단한 다수의 신용단위를 포함하며, 기록물의 연속적인 부분 또는 완전한 재생으로 상기 신용 단위의 수를 감소시키도록 배열되어 있다.
디지털 데이터의 기록

삭제

서두에서 설명했듯이, 허가되지 않은 복사 및 저작권 침해에 관련하여 야기되는 위험성의 측면에서 디스크램블된 디지털 데이터가 기록될 수 있도록 하는 것은 현명하지 않은 것이다. 도 5에 나타낸 것과 같이, 본 발명은 이 문제를 극복하는 수단을 제공한다.

시스템은 리시버/디코더의 스마트카드 슬롯에 삽입할 수 있는 스마트카드 (4004)와 함께, DVHS 카세트 등의 디지털 기록매체(4006)를 포함하는 디지털 레코더(4005), 예를 들어 DVHS 레코더를 포함한다.

이 실시예에서, 수신된 제어 워드는 디코더에 삽입되는 관련 스마트카드 (3020)에 의해 해독된다(도2 참조). 그리고 (액세스 제어정보 등의 ECM을 형성하는 데이터와 함께) 디코딩된 제어워드 Ce는 스마트카드(4004)에 내장된 마이크로프로세서로 전송된다. 제 2 암호화 키 C2 및 제 2 암호화 알고리즘 Ch2을 사용함으로써 스마트카드(4004)는 도면에서 ECM'로 나타낸 새로운 ECM을 생성한다. 그리고 이 자격관리 메시지는 참조부호(4007)로 나타낸 디멀티플렉서 DMp로부터 스크램블된 데이터 스트림의 ECM을 대체하는 데 사용되고 스크램블된 데이터와 새로운 자격관리 메시지 ECM'의 결합은 DVHS 카세트(4006)에 기록된다. 자격관리 메시지 ECM'는 시프트 제어 레지스터 R를 순환하는 데이터 스트림에 삽입될 수 있다.

이 수단에 의해, 본 발명은 디코드된 음성영상 정보가 카세트에 기록되지 않도록 한다. 카세트를 실행시키기 위해, 카드가 디코더에 재삽입되고, 키 C2는 자격관리 메시지 ECM'를 디코딩하는데 사용되고, 시청용 프로그램을 디스크램블하기 위하여 인출된 제어워드 Ce는 디코더를 제어하는 데 사용된다.

도 5에 나타낸 시스템에서 스마트카드(4004)는 도 2에 도시된 텔레비젼 시스템의 스마트카드(3020)와 다르며 프로그램을 시청하는 데 필요한 암호화 키를 포함한다. 그러나, 도 6에 나타낸 다른 실시예에서, 스마트카드(3020)는 프로그램의 시청 및 기록에 필요한 제 1 및 2 암호화 키 Cex 및 C2 모두를 포함한다. 설명했듯이, 키 Cex는 프로그램을 시청하도록 디스크램블러 D에 의해 사용되고 새로운 자격관리 메시지 ECM'를 형성하도록 키 C2에 의해 암호화된 제어 워드(Ce)를 생성하기 위하여 ECM의 해독을 제어한다.

알고리즘 DCh1 및 DCh2은 공간적인 이유로 도시하지 않았다. 카드(3020)는, 카드의 메모리에 제공된 월별 키 Cex를 얻기 위하여 EMM의 해독을 가능케하는 비밀키 Cg(도시되지 않음)로 사실상 초기화된다. 스마트카드가 실질적으로 사각형 카드의 형태로 도시되었지만, 키 형태 등의 물리적인 형태도 물론 가능하다.

프로그램으로 전송되고 카드에 의해 해독되는 ECM은 카드에 저장되어 기록된 필름의 시청 횟수를 제어하는 신용단위 U도 포함할 수 있다. 가장 간단한 실시예로, 신용 단위는 ECM'이 디코더에 의해 전송될 때마다 기록된 필름의 재생동안 감소될 수 있다. 신용 횟수가 기록물이 설정된 횟수를 시청하였다는 것을 나타내는 제로로 감소되며, 신용 단위가 재충전되지 않는 한(예를 들어, EMM에 전송된 충전 명령에 의해) 메시지는 필름의 추가 시청을 방지하기 위하여 디코더로 전송된다.

다른 실시예로, 신용 단위는 몇 십 또는 몇 백개의 ECM' 메시지마다 감소될 수 있다. 또 다른 구현으로, 신용 단위는 필름의 소정 부분(예를 들면, 필름의 처음 또는 마지막 10분)에 대응할 수 있으므로 이 부분의 실행은 그와 관련된 신용 단위를 감소시킬 것이다. 따라서 이 부분은 ECM' 메시지를 이 부분에 태그함으로써 식별될 수 있다.

본 발명의 다른 실시예가 도 7에 도시되어 있다. 본 실시예에서, 새로운 자격 관리 메시지(EMM')의 생성은 제 2 암호화 키 C2를 소유하고 기록된 카세트 (4006)의 케이싱에 내장된 집적 회로 또는 칩(4008)에 의해 제어된다. 기록 매체의 하우징의 마이크로프로세서의 결합은 공지된 기술로서 예를 들어 DVHS 카세트의 경우에 제안되었다. 이 실시예에서, 일련의 금속 접점은 카세트 하우징의 외부면에 설치될 수 있으며, 이 접점은 하우징의 내부에서 집적 회로 또는 칩 등의 전자 회로로 유도한다. 이 접촉부는 집적회로와 비디오 레코더 사이의 통신을 가능케하도록 일련의 접점에 의해 레코더의 리셉터클에 결합될 수 있다.

산업상 이용 가능성

알 수 있듯이, 기록된 (및 스크램블된) 디지털 데이터를 복사하는 것이 수월하지만, 칩에 저장된 데이터는 복사하기가 어려우며, 이전의 실시예에서처럼 스크램블된 데이터로 디스크램블러에 의해 사용된 제어 워드를 얻기 위하여 ECM'을 해제하는 데 필요한 키 C2 없이는 사용될 수 없을 것이다.

이해하듯이, 설명된 모든 실시예에서, 디지털 레코더는 스마트카드 및/또는 제어워드 Ce가 ECM' 메시지에서 추출되면 프로그램을 디스크램블하는 데 필요한 부품을 수용하는 스마트카드 슬롯을 포함하므로 리시버/디코더 및 디지털 기록 장치의 부품은 결합되거나 또는 교체될 수 있다. 디코더 및/또는 디지털 레코더는 예를 들어 텔레비젼 등의 장치와 함께 통합될 수 있다.

(57) 청구의 범위

청구항 1.

디코더에 의해 디지털 정보를 제 1 키에 의해 암호화된 정보를 수신하는 단계;

상기 암호화된 정보를 해독하는 데 필요한 상기 제 1 키의 동등물을 액세스하는 단계:

상기 해독된 정보를 상기 디코더의 스마트카드 리더에 수용되는 스마트카드에 저장된 제 2 키에 의해 재암호화하는 단계; 및

상기 재암호화된 정보를 상기 디지털 레코더에 의해 상기 디지털 기록매체에 기록하는 단계를 포함하고, 상기 스마트카드는 기록물이 몇 회 재생될 수 있는 지를 판단하기 위하여 다수의 신용단위를 포함하며, 상기 신용 단위의 수는 각 기록물의 연속적인 부분 또는 완전한 재생으로 감소되는 디지털 정보 기록 방법.

청구항 2.

삭제

청구항 3.
삭제

청구항 4.
삭제

청구항 5.
삭제

청구항 6.
삭제

청구항 7.
삭제

청구항 8.

제 1항에 있어서, 상기 기록물의 섹션에 대한 재생이 상기 섹션과 관련된 소정의 신용 단위를 감소시키도록 상기 신용단위가 상기 기록물의 특정 세그먼트와 관련되도록 하는 디지털 정보 기록 방법.

청구항 9.

제 8항에 있어서, 상기 신용 단위는 단일 타입으로 되어 있고, 기록물의 어떤 섹션을 재생하면 감소되는 디지털 정보 기록 방법.

청구항 10.

제 1, 8, 및 9 중의 어느 한 항에 있어서, 상기 제 2 키는 상기 디지털 기록매체의 하우징에 내장된 집적 회로에 저장되는 디지털 정보 기록 방법.

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.

제 1, 8, 및 9 중의 어느 한 항에 있어서, 상기 제 2 키는 상기 디지털 기록매체와 관련된 스마트 카드에 저장되는 디지털 정보 기록 방법.

청구항 15.

디코더 및 스마트 카드로 이루어진 결합 장치로서,

상기 디코더는 제 1 키에 의해 암호화된 디지털 정보를 수신하고 상기 디지털 정보를 해독하는 데 필요한 상기 제 1 키의 동등물을 액세스하고,

상기 스마트 카드는 상기 디코더의 스마트카드 리더에 수용되고, 디지털 기록매체로의 기록을 위한 디지털 기록장치로의 전송을 위한 상기 해독된 정보를 재암호화하는 제 2 키를 가지고 있고, 기록물이 몇 회 재생될 수 있는 지를 판단한 다수의 신용단위를 포함하며, 각 기록물의 부분 실행 또는 완전한 재생으로 상기 신용 단위의 수를 감소시키도록 배열되는 디코더 및 스마트 카드의 결합 장치.

청구항 16.

제 15항에 있어서, 상기 신용단위는 기록물의 특정 세그먼트와 관련되어 있으므로, 기록물의 섹션이 재생되면 상기 스마트 카드는 상기 섹션과 관련된 소정의 신용을 감소시키도록 배열되어 있는 디코더 및 스마트 카드의 결합 장치.

청구항 17.

제 16항에 있어서, 상기 신용단위는 단일 타입으로 되어 있고, 기록물의 어떤 섹션이 재생되면 상기 스마트 카드는 상기 신용 단위를 감소시키도록 배열되어 있는 디코더 및 스마트 카드의 결합 장치.

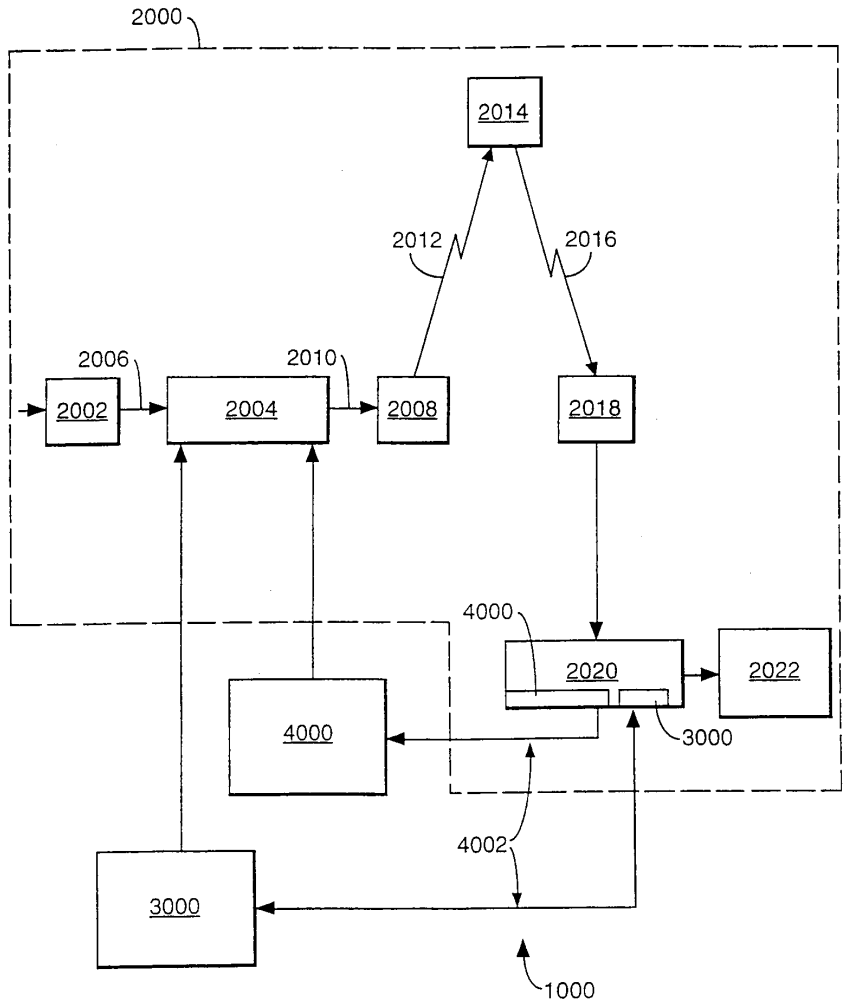
청구항 18.

디코더의 스마트카드 리더에 수용되고, 제 1 키에 의해 암호화된 디지털 정보를 수신하고 상기 디지털 정보를 해독하는 데 필요한 제 1 키의 동등물을 액세스하는 스마트 카드로서,

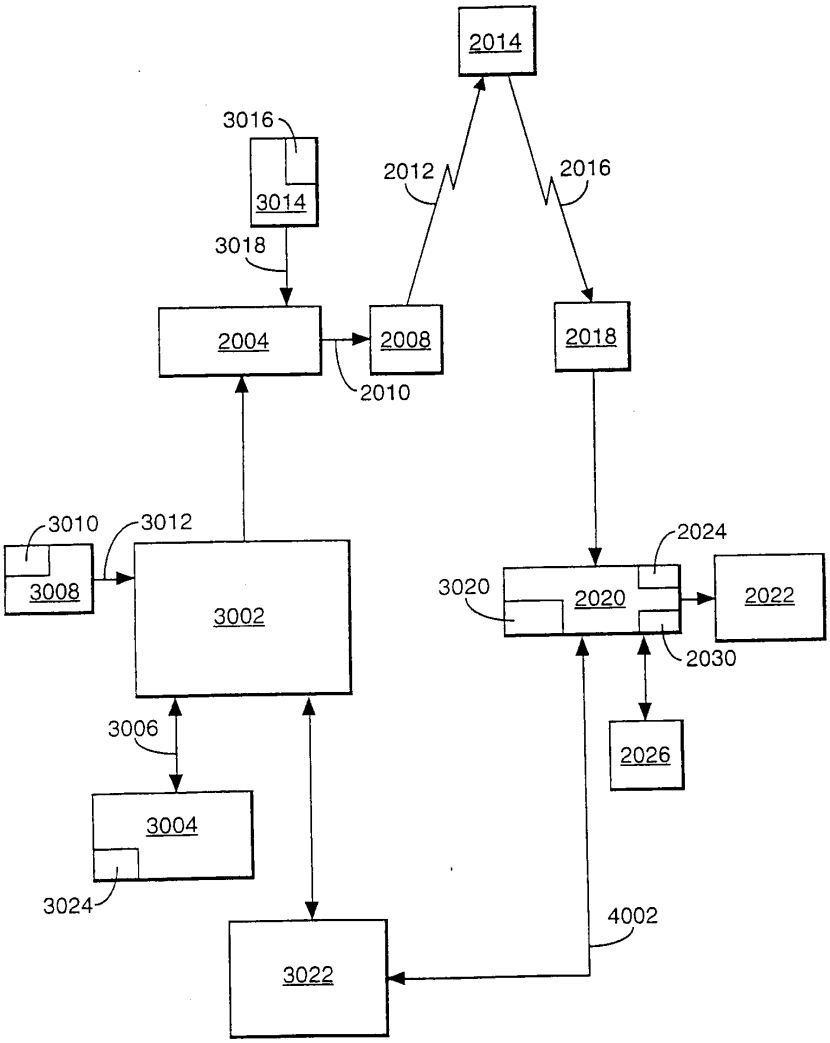
디지털 기록매체로의 기록을 위한 디지털 기록장치로의 전송을 위한 상기 해독된 정보를 재암호화하는 제 2 키를 가지고 있고, 기록물이 몇 회 재생될 수 있는 지를 판단한 다수의 신용단위를 포함하며, 상기 스마트 카드는 기록물의 연속적인 부분 또는 완전한 재생으로 상기 신용 단위의 수를 감소시키도록 배열되어 있는 스마트 카드.

도면

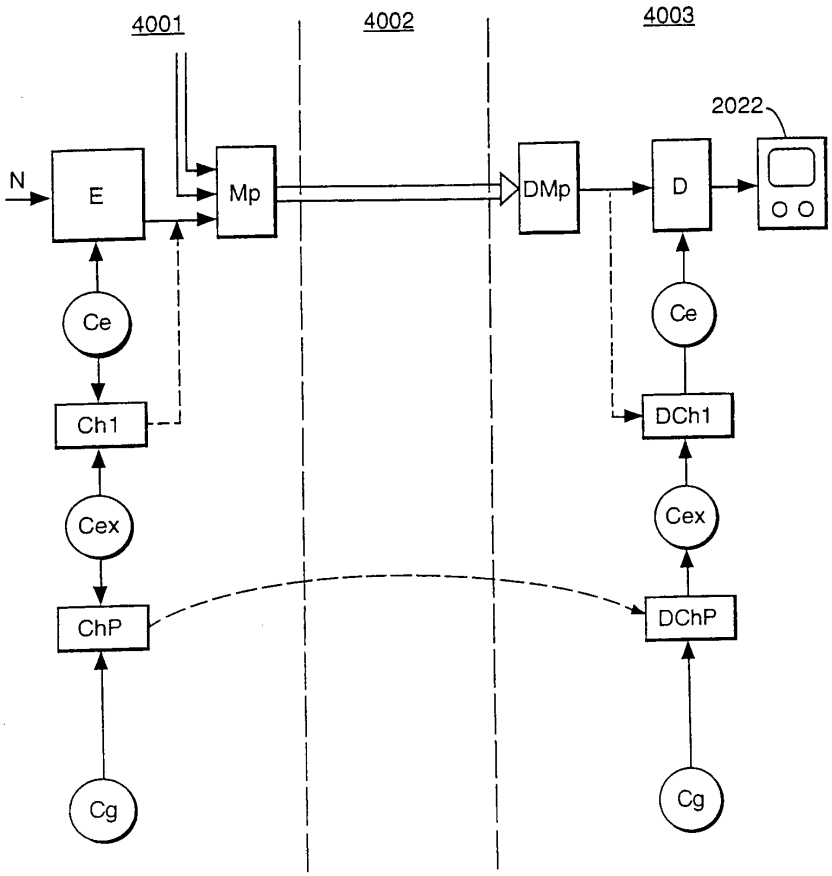
도면1


2000
2014
2012
2016
2006
2010
2002
2004
2008
2018
4000
2020
2022
4000
3000
4002
3000
1000

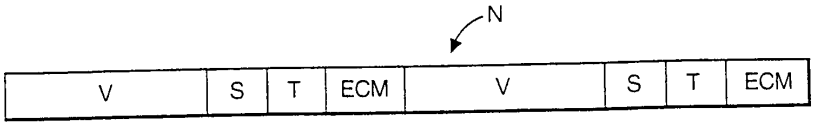
도면2


2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
3006
2026
3004
3024
4002
3022

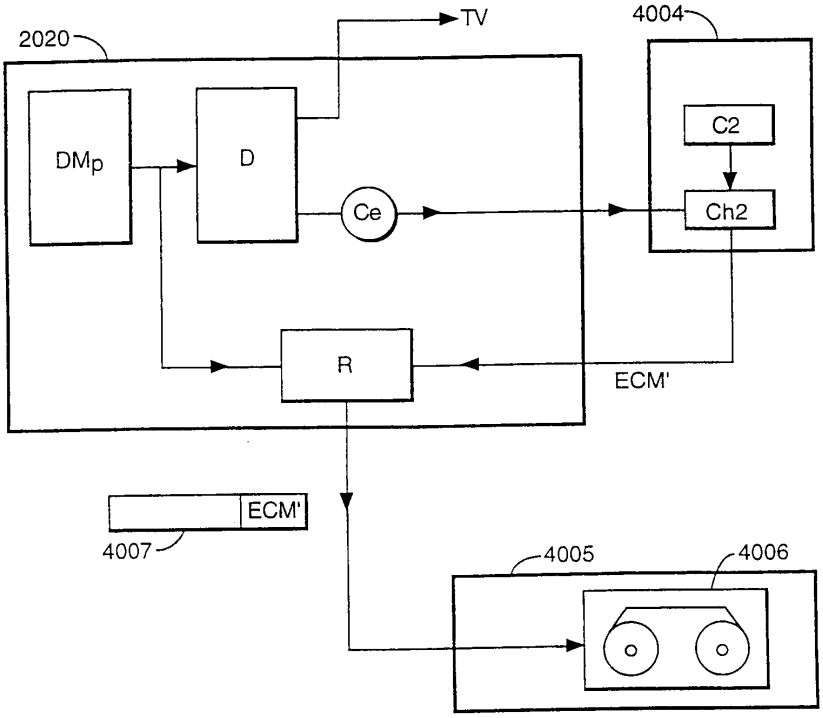
도면3


4001
4002
4003
2022
N
E
Mp
DMp
D
Ce
Ch1
Cex
ChP
Cg
Ce
DCh1
Cex
DChP
Cg

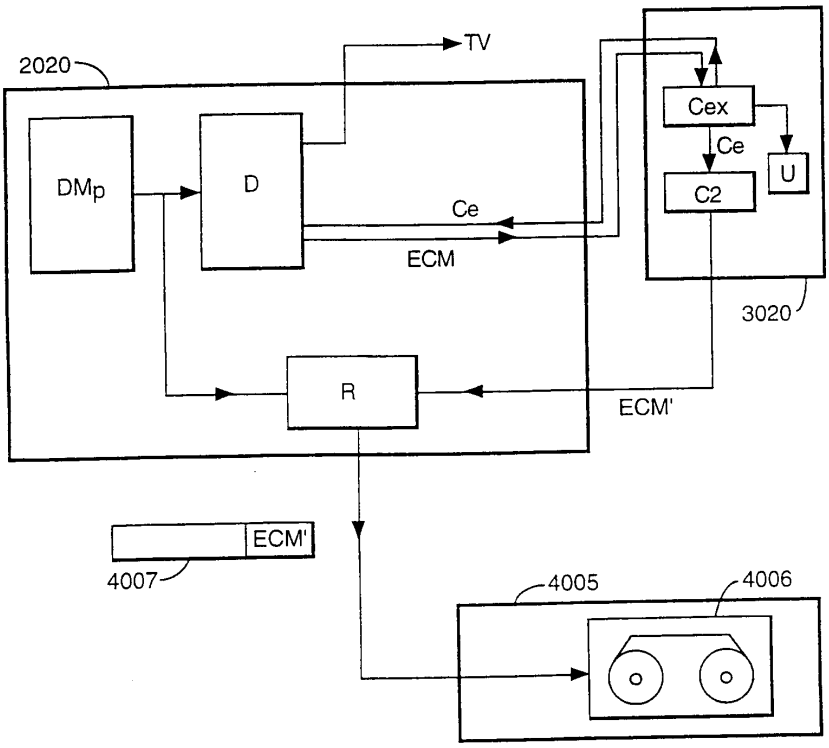
도면4


N
V
S
T
ECM
V
S
T
ECM

도면5


2020
TV
4004
DMp
D
Ce
C2
Ch2
R
ECM'
ECM'
4007
4005
4006

도면6


2020
TV
DMp
D
Ce
ECM
Cex
Ce
C2
U
3020
R
ECM'
ECM'
4007
4005
4006

도면7