(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년10월22일
(11) 등록번호 10-0989473
(24) 등록일자 2010년10월15일

(51) Int. Cl.
H04N 7/167 (2006.01)
(21) 출원번호 10-2005-7014273
(22) 출원일자(국제출원일자) 2004년01월30일
심사청구일자 2008년11월28일
(85) 번역문제출일자 2005년08월03일
(65) 공개번호 10-2005-0118164
(43) 공개일자 2005년12월15일
(86) 국제출원번호 PCT/EP2004/050060
(87) 국제공개번호 WO 2004/071087
국제공개일자 2004년08월19일
(30) 우선권주장
0301243 2003년02월04일 프랑스(FR)
(56) 선행기술조사문헌
US5461675 A
WO0200046994 A1
JP2001333407 A
전체 청구항 수 : 총 7 항

(73) 특허권자
나그라 톰슨 라이센싱
프랑스 92100 불로뉴 빌랑꾸르 르 갈로 알퐁스 콰이 46
(72) 발명자
드보이즈, 장-뤽
프랑스, 에프-75116 빠리,19 뤼 에우겐 마누엘
(74) 대리인
특허법인정직과특허

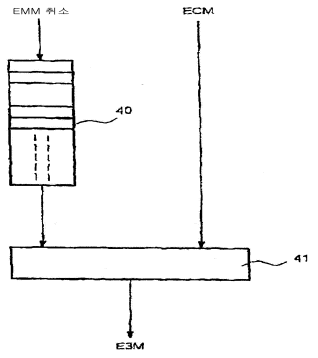
심사관 : 조남신

(54) 유료 텔레비전 시스템, 이와 같은 시스템에서 권리를취소하는 방법, 관련된 디코더 및 스마트 카드, 및 이와같은 디코더로 전송되는 메시지

(57) 요 약

본 발명은 디코더(11)에 의해 수신되는 시청각 프로그램으로의 액세스 권리들을 취소하는 방법에 있어서, 소정 기간동안 수신된 시청각 신호를 디스크램블 하도록 각각 사용되는 암호화된 제어 워드들(CW)을 포함하는 제1 메시지(ECM)들 및 사용자 권리 할당 정보(cues)들을 각각 포함하는 제2 메시지들(EMM)을 상기 디코더에 송출하는 단계, 사용자가 제1 메시지 내에 포함된 정보(cue)들을 액세스하도록 인증받으면, 제어 워드들(CW)을 발생시켜 상기 디코더(11)에 의해 수신되는 상기 시청각 신호를 디스크램블하도록 상기 디코더 또는 이와 관련된 휴대용 객체에서 상기 제1 메시지들을 복호화하는 단계, 적어도 하나의 암호화된 제어 워드, 디코더 어드레스 및 권리 취소 큐(정보, cue)의 조합으로부터 발생되는 제3 하이브리드 메시지들(E3M) 송출하는 단계 로 이루어진다.

대 표 도 - 도3



특허청구의 범위

청구항 1

디코더(11)에 의해 수신되는 시청각 프로그램에 대한 액세스 권리들을 취소하는 방법에 있어서,

2가지 유형의 메시지들 - 사전에 설정된 기간동안 수신된 시청각 신호를 디스크램블 하도록 각각 사용되는 암호화된 제어 워드들(CW)을 포함하는 제1 메시지(ECM)들, 및 사용자 권리 할당 정보를 각각 포함하는 제2 메시지들(EMM) - 을 상기 디코더에 송출하되, 상기 사용자 권리 할당 정보는 상기 디코더의 메모리에 저장되는 단계;

사용자가 상기 시청각 신호를 액세스하도록 인증받으면, 상기 디코더(11)에 의해 수신되는 상기 시청각 신호를 디스크램블하는 제어 워드들(CW)을 생성하기 위하여, 상기 디코더 또는 상기 디코더가 구비된 휴대용 객체에서 상기 제1 메시지들을 복호화하는 단계; 및

제3 하이브리드 메시지들(E3M)을 송출하되, 각각의 제3 하이브리드 메시지는 적어도 하나의 암호화된 제어 워드, 디코더 어드레스, 및 권리 취소 정보의 조합으로부터 발생되고, 상기 디코더는 상기 제3 하이브리드 메시지에 포함된 디코더 어드레스가 상기 디코더의 어드레스와 일치되면 상기 디코더의 메모리에 저장된 사용자 권리 할당 정보를 삭제하는 단계를 포함하는 것을 특징으로 하는 액세스 권리들을 취소하는 방법.

청구항 2

제1항에 있어서, 하이브리드 메시지(E3M)에서, 상기 제어 워드(CW)는 상기 디코더 어드레스 및 권리 취소 정보를 암호화하는데 사용되는 특정 키와 상이한 동작키로 암호화되는 액세스 권리들을 취소하는 방법.

청구항 3

제1항에 있어서, 비대칭 암호작성법이 사용되는 액세스 권리들을 취소하는 방법.

청구항 4

유료 텔레비전 시스템에 있어서,

가입자들의 식별자와 권리들을 저장하는 가입자 관리 유닛(20), EMM 메시지 암호화 유닛(21), 상기 가입자 관리 유닛(20)에 의해 제어되는 가입자 인증 시스템(22), 시청각 프로그램들을 위한 MPEG 압축기(23), ECM 메시지 암호화 유닛(24), 스크램블러/멀티플렉서(25), 스마트 카드(27)와 관련된 적어도 하나의 디코더(26), 통신 서버(30), 슈퍼바이저(31), 및 상기 스크램블러/멀티플렉서(25)과 디코더들(26) 간의 링크(32)를 포함하며,

각 유료 시청각 프로그램 채널에 대해서 EMM 취소 메시지들 큐(queue)(40) 및 멀티플렉서(41)를 포함하는, EMM 메시지 필드 및 ECM 메시지 필드 결합 유닛을 포함하는데, 각 필드 결합 유닛은 스크램블러/멀티플렉서(25)의 입력에 영향받는(disposed at) 것을 특징으로 하는 유료 텔레비전 시스템.

청구항 5

스마트 카드에 있어서,

디코더로 전송하는 하이브리드 메시지를 처리하도록 특별히 개조되고, 각각의 제3 하이브리드 메시지는 적어도 하나의 암호화된 제어 워드, 디코더 어드레스 및 권리 취소 정보의 조합으로부터 발생되는 것을 특징으로 하고,

자신의 메모리에 등록된 권리들을 삭제하고, 제어 워드들을 생성시키기 위하여 현재 동작키로 암호화된 제어 워드들을 복호화하는 수단을 포함하는 스마트 카드.

청구항 6

디코더에 있어서,

디코더로 전송하는 하이브리드 메시지를 처리하도록 특별히 개조되고, 각각의 제3 하이브리드 메시지는 적어도 하나의 암호화된 제어 워드, 디코더 어드레스 및 권리 취소 정보의 조합으로부터 발생되는 것을 특징으로 하고,

자신의 메모리에 등록된 권리들을 삭제하고, 제어 워드들을 생성시키기 위하여 현재 동작키로 암호화된 제어 워드들을 복호화하는 수단을 포함하는 디코더.

청구항 7

삭제

청구항 8

디코더(11)에 의해 수신되는 시청각 프로그램에 대한 액세스 권리들을 취소하는 방법에 있어서,

2가지 유형의 메시지들 - 사전에 설정된 기간동안 수신된 시청각 신호를 디스크램블 하도록 각각 사용되는 암호화된 제어 워드들(CW)을 포함하는 제1 메시지(ECM)들, 및 사용자 권리 할당 정보를 각각 포함하는 제2 메시지들(EMM) - 을 상기 디코더에 수신하되, 상기 사용자 권리 할당 정보는 상기 디코더의 메모리에 저장되는 단계;

사용자가 상기 시청각 신호를 액세스하도록 인증받으면, 상기 디코더(11)에 의해 수신되는 상기 시청각 신호를 디스크램블하는 제어 워드들(CW)을 생성하기 위하여, 상기 디코더 또는 상기 디코더가 구비된 휴대용 객체에서 상기 제1 메시지들을 복호화하는 단계를 포함하는데,

상기 디코더는 제3 하이브리드 메시지들(E3M)을 수신하되, 각각의 제3 하이브리드 메시지는 적어도 하나의 암호화된 제어 워드, 디코더 어드레스, 및 권리 취소 정보의 조합으로부터 발생되고, 상기 디코더는 상기 제3 하이브리드 메시지에 포함된 디코더 어드레스가 상기 디코더의 어드레스와 일치되면 상기 디코더의 메모리에 저장된 사용자 권리 할당 정보를 삭제하는 것을 특징으로 하는 액세스 권리들을 취소하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 유료 텔레비전 시스템, 이와 같은 시스템에서 권리를 취소하는 방법, 관련된 디코더 및 스마트 카드, 및 이와 같은 디코더로 전송되는 메시지에 관한 것이다. 이와 같은 유료 텔레비전 시스템들에서, 시청각 프로그램을 분배시키는 2가지 널리 공지된 모드들이 별개로 또는 결합되어 존재할 수 있다.

[0002] 제1 모드는 시청각 프로그램들에 비암호화된(암호화가 풀린) 액세스(unencoded access)를 위한 전제조건으로서 가입 및/또는 지불을 필요로 한다. 이 경우에, 하나 또는 그 이상의 채널에서 방송되는 시청각 프로그램들에 액세스하기 위하여, 가입자는 가입하여 주기적으로, 예를 들어 매달 비용을 지불하여야 한다.

[0003] 제2 모드는 가입 또는 지불 전 일시적 디스크램블된 미리보기를 제공할 것을 요청한다. 이 경우에, 가입자는 현재 또는 곧 나올 프로그램에 대해 미리 보도록 무료로 그리고 비암호화된(즉, 디스크램블된) 액세스가 허용되거나 가입자가 이 액세스를 요청하였다는 것을, 예를 들어, 자신의 스크린상의 메시지를 통해서 통지받는다. 따라서, 가입자는 비교적 짧은 지속 시간 동안 소정 채널 상에서 암호화되지 않은 프로그램을 일시적으로 시청할 수 있다. 가입자가 이 프로그램을 계속 시청하길 원하면, 가입자는 이 시간의 만료 전, 예를 들어 모뎀을 사용하여 당업자에게 공지된 메커니즘, 예를 들어 소위 페이퍼뷰 방식 또는 임펄스 페이퍼뷰 방식에 따라서 지불(payment transaction)을 행하여야 한다. 이 지불이 시간 만료 전 실행되지 않으면, 프로그램에 대한 비암호화된 액세스는 차단되어 이 프로그램은 가입자의 텔레비전 스크린상에 스크램블된 상태로 나타난다

[0004] 본 발명은 특히 상술된 2개의 모드들에 적용되지만, 더욱 구체적으론 이 제2 모드의 프레임워크 내에서 설명된다.

[0005] 본 특허 출원에서, 용어 시청각 프로그램은 임의의 비디오 및/또는 오디오 프로그램을 가리킨다.

배 경 기 술

[0006] 유료 텔레비전에서 사용되는 기술은 2가지 독립적인 메커니즘들, 즉, 한편으론 비디오 및/또는 오디오 프로그램(또는 프로그램들)의 스크램블링/암호화, 다른 한편으론 보안 메시지들로서 전송되는 상업적 권리들(commercial rights)을 디스크램블링 박스 또는 디코더에 (제어 액세스와 함께) 할당하는 기능을 토대로 한다. 스크램블링/암호화는 디지털 비트 스트림에 손쉽게 적용될 수 있다. 모든 비트들은 예를 들어 블록방식 암호(blockwise cipher)를 사용하여 스크램블/암호화될 수 있다. 스크램블링은 아날로그 전송에 사용된다. 이와 같은 스크램블링을 사용함으로써, 신호의 포맷은 변경되며, 동기화 신호들은 억제되어 암호화된 형태로 별개로 전송된다. 오디오 신호는 디지털 신호로 변환된 후 암호화될 수 있다. 암호화된 디지털 오디오 신호는 비디오 신호에 삽입될 수 있다.

[0007] 전송된 시청각 프로그램은 키들에 의해서 스크램블되거나 암호화되는데, 이 스크램블되거나 암호화된 시청각 프로그램은 오직 이들 키들의 동등물들, 소위 제어 워드들(CW)에 의해서만 디스크램블되거나 복호화될 수 있다. 대칭 암호화 모드에서, 암호화/스크램블링 키들은 제어 워드와 동일하다. 비대칭 암호화 모드에서, 암호화 스크램블링 키들은 제어 워드들과 다르다. 제공된 시청각 프로그램 각각에 대해서, 디코더들에 전송된 제어 워드 값들은 예를 들어 1초 정도의 비교적 높은 빈도로 주기적으로 변경된다. 시청각 프로그램의 수신시 복호화를 하기 위하여, 자격 제어 메시지들(ECM: "Entitlement Control Messages") 및 자격 관리 메시지들(EMM:"Entitlement Management Messages")이 디코더들에 전송된다.

[0008] 이들 2가지 유형의 메시지들(ECM 및 EMM)은 디코더를 통해서 스마트 카드 또는 PCMCIA 카드, 스마트 키...,와 같은 어떤 휴대용 객체에 디스패치(dispatch)될 수 있는데, 이는 사용자 권리들의 복호화 및 저장 기능을 위하여 제공된다. 본 설명에서, 용어 카드는 디코더와 결합하여 동작하는 임의의 휴대용 객체를 가리킨다.

[0009] ECM 메시지는 암호화된 제어 워드들을 포함하는데, 이 제어 워드들은 디코더가 시청각 프로그램을 디스크램블/복호화하도록 한다. ECM 메시지들은 암호화된 제어 워드들을 복호하고 이들 제어 워드들(CW)을 디코더에 디스패치하는 카드에 전송한다. 이 카드는 사용자가 현재 텔레비전 프로그램에 액세스하도록 인증받은 경우에만 암호화된 제어 워드들을 복호화하는 동작을 실행한다. 이를 위하여, 카드는 자신의 메모리 영역에 관련 사용자에게 할당된 권리들을 저장한다. 따라서, 사용자가 가입에 의해 스마트 카드와 관련될 때, 액세스 인증이 카드에 저장된 권리 할당 데이터("자격 데이터(entitlement data)")로 표시된다.

[0010] EMM 메시지들은 큐들(cues)(정보, 이하에서 cue는 정보를 의미하고, queue는 대기행렬을 뜻한다.)을 포함하는데, 이 큐들(cues)은, 예를 들어 카드에 저장된 데이터를 수정함으로써 사용자의 권리 할당 데이터를 갱신할 수 있다. 일시적 디스크램블된 미리보기를 제공하는 경우에, 종래 기술을 따르면, 제1 EMM 메시지는 디코더로 디스패치되어, 소정 채널 상에서 프로그램을 액세스하는데 필요로 되는 권리들을 가입자에게 일시적으로 제공한다. 어떤 지불 거래의 실패가 운영자의 권리 관리 시스템에 의해 수신되면, 또 다른 EMM 메시지가 디스패치되어, 이들 권리들을 취소시킨다.

[0011] ECM 및 EMM 메시지들은 메시지의 무결성(integrity)을 보장하는 디지털 서명 필드(예를 들어, 해시 코드(hash code))를 갖는다. 이는 메시지의 내용들의 어떠한 악의적인 또는 우발적인 손상을 검출할 수 있다.

[0012] ECM 메시지는 전송된 스크램블된 신호와 함께 송출된다. 이는 3개의 필드들을 포함한다. 제1 필드는 특정 액세스 파라미터들을 포함한다. 이들 파라미터들은 텔레비전 프로그램에 액세스를 허용하는 조건을 규정한다. 이 필드는, 예를 들어 부모의 평가(부가적인 핀 코드가 디코더에 필요로 된다) 및 지역적 텔레비전 방송금지(어떤 필름은 모든 유럽 국가에서 이용될 수 없다)를 허용한다. 제2 필드는 암호화된 형태의 제어 워드를 포함한다. 최종 필드는 관련된 ECM 메시지를 위한 데이터 무결성 제어 큐들을 포함한다.

[0013] EMM 메시지는 통상적으로 4개의 필드들을 포함한다. 각 EMM 메시지는 개별 디코더를 선택하는 어드레스 필드로 시작된다. 2가지 어드레싱 모드들, 즉 개별 디코더를 위한 한 모드 및 일군의 디코더들을 위한 다른 한 모드가 존재한다. 제2 필드는 소정 사용자를 위한 권리 할당을 포함한다. 제3 필드는 암호화된 형태의 동작 키를 포함한다. 최종 필드는 관련된 EMM 메시지를 위한 데이터 무결성 제어 큐(cues)들을 포함한다. EMM 메시지들은 또한 명령을 디코더로 디스패치 하도록 사용될 수 있다. EMM 메시지의 송출은 일반적으로, 운영자에 대한 사용자의 어떤 행위(가입) 또는 행위 불이행("일시적 디스크램블된 미리보기의 지불" 모드에서 미납)의 결과이다. 이들 메시지들은 일반적으로 개별적이다. 이들의 내용은 디코더(또는 관련된 카드) 또는 이들 특정 권리들이 관련되는 제한된 수의 디코더들에 의해 해석된다. EMM 메시지들은, 자신들이 적용되는 텔레비전 프로그램과 동시에 송출되지 않는다. 이들은 미리 전송되어, 인증된 사용자가 소정 프로그램에 액세스하도록 한다. 이들 EMM 메시지들을 수신기에 전송하도록 임의의 네트워크-모뎀, 메일 또는 전파 방송-가 사용될 수 있다.

[0014] EMM 메시지가 사용자에 의해 수신되는 것을 확인하기 위하여, 예를 들어 가입을 갱신하도록 하기 위하여, 후자가 여러 번 디스패치 된다. 따라서, EMM 메시지들은 송출을 위한 소정 기간에 따라서 주기적으로 구성된다. 이와 같은 주기의 지속 기간은 긴 시간 동안 디코더를 스위치 오프하고 있는 사용자가 권리할당을 얻을 때까지 기다리는 최대 대기시간을 정한다.

[0015] 따라서, 도 1에 스크램블러(10), 통상적으로 디코더(도시되지 않음)와 일체로 된 디스크램블러(11), 스마트 카드(12) 및 ECM과 EMM 메시지들이 도시되어 있다. 스마트 카드(12)는 특히:

[0016] - 고정된 카드 어드레스

[0017] - EMM에 의해 주기적으로 갱신되는 적어도 하나의 동작 키(sk)

[0018] - 고정된 특정 키(Q)를 저장한다.

[0019] 상술된 바와 같이, ECM 메시지는 3개의 필드들을 포함하는데, 이 3개의 필드들은 각각:

[0020] - 액세스 파라미터들,

[0021] - 동작 키에 의해 암호화된 제어 워드(E_{Sk}CW로 표시됨)

[0022] - 고려되는 ECM 메시지를 위한 데이터 무결성 제어 필드(해시 코드)를 저장한다.

[0023] EMM 메시지는 4개의 필드들을 포함하는데, 이 4개의 필드들은 각각:

[0024] - 어드레스,

[0025] - 사용자의 권리들,

[0026] - 암호화된 동작 키, sk:E_Q(sk)로 표시됨,

[0027] - 고려되는 EMM 메시지를 위한 데이터 무결성 제어 워드(해시 코드)를 포함한다.

[0028] 연속적인 제어 워드들(CW)은 스크램블러(10)에 그리고 동시에 디코더에 디스패치되어, 전송된 데이터의 스크램블링 및/또는 암호화 및 디스크램블링 및/또는 복호화를 각각 허용한다.

[0029] 따라서, 비디오 및/또는 오디오 신호들은 연속적인 제어 워드들(CW)을 사용하여 스크램블링될 수 있다. 주기적으로(예를 들어, 매 10초 마다) ECM 메시지가 스크램블된 신호와 함께 송출된다. 이들 ECM 메시지들은 현재 유효한 동작 키(sk)로 암호화되고 EMM 메시지로 전송되는 제어 워드들을 포함하여, 디코더 또는 카드 판독기가 제공된 디코더와 관련되는 카드(예를 들어, 스마트 카드 또는 PCMCIA 카드)에 저장되도록 한다.

[0030] 동작 키들(sk)은 EMM 메시지들에 의해 덜 빈번하게, 예를 들어 매달 갱신된다. 이 동작 키들(sk)은 스마트 카드 또는 디코더에 안전한 방식으로 저장되는 하나 이상의 개별적인 특정 키들(Q)로 암호화된다.

[0031] 보안 문제는 본 설명의 서두에 제공된 2가지 모드들 중 한 모드에 따라서 동작하는 유료 텔레비전 시스템들에서 발생될 수 있다. 특히, 프로그램으로의 가입 권리들의 취소 또는 가입자 권리들의 취소는 (개별적인 EMM 또는 특정 EMM 메시지 유형의)EMM 가입자 메시지를 디스패치함으로써 종래 기술에 따라서 행해진다. 권리 할당 EMM 메시지를 디스패치함으로써 가입이 획득되거나 일시적 디스크램블된 미리보기가 가입자에 제공된 후 취소가 실행되지 못하도록 하여, 개인(또는, "해커")이 이와 같은 동작 방식으로부터 이득을 얻고자 할 수 있다. 그러므로, 개인은 EMM 메시지들로부터 ECM 메시지들을 구별하고자 하는 기술을 개발할 수 있다. 그 후, 그는 "블로커들(blockers)"을 사용하여 EMM 메시지들을 필터링함으로써 식별 및 억제할 수 있다. 이와 같은 기술은, EMM 메시지가 디코더에 의해 수신될 때까지 그리고 사용자 권리들이 EMM 메시지를 통해서 디코더(또는, 이와 관련된 카드)에 의해 수신될 때까지 EMM 메시지들을 수신하지 않도록 MPEG 필터들의 필터링 파라미터들을 수정한다는 점에서, 예를 들어 MPEG("동영상 전문가 그룹") 디지털 기술에 포함된다. 따라서, 적절한 EMM 메시지들의 사전 디스패칭에 의해, 카드가 일시적 디스크램블된 미리보기 모드로 액세스될 수 있는 소정 프로그램을 디스크램블하도록 인증되면, 개인은 예를 들어 모든 EMM 메시지들을 필터링 및 거부할 수 있다. 하나 이상의 프로그램들로의 액세스가 인증된 후, 다음 EMM 메시지들의 억제는 인증 상태를 수정하는 것을 방지한다.

[0032] 따라서, 인증 데이터는 수정될 수 없고, 이로 인해, 일시적 디스크램블된 미리보기 채널 상에 전달되는 모든 프로그램들로의 인증되지 않은 액세스는 EMM 메시지들의 필터링 전 카드에 저장된 동작 키들의 유효 지속기간과 동일한 지속기간 동안 얻어진다.

[0033] 이 문제를 해결하기 위하여, 액세스 제어 방법을 설명하는 미국 특허 제5,461,675호는 스마트 카드가 지정되거나 그렇지 않은 적어도 하나의 EMM 메시지를 수신하여만 하는 기간을 카드에 제공한다. 이 요건이 충족되지 않으면, 스마트 카드는 시청각 프로그램을 디스크램블하기 위한 정확한 정보를 제공하지 못한다.

[0034] 본 발명의 목적은 메시지들을 디스패칭 하는데 필요로 되는 대역폭을 제한하면서 미국 특허 제5,461,675호에 서술된 해결책과 구별되는 해결책으로 상술된 문제를 해결하고자 하는 것이다.

발명의 상세한 설명

[0035] 그러므로, 본 발명은 디코더에 의해 수신되는 시청각 프로그램으로의 액세스 권리들을 취소하는 방법을 제공하

는 것인데, 상기 방법은:

[0036] -2가지 유형의 메시지들, 즉 소정 기간동안 수신된 시청각 신호를 디스크램블 하도록 각각 사용되는 암호화된 제어 워드들을 포함하는 제1 메시지들 및 사용자 권리 할당 큐들(cues)을 각각 포함하는 제2 메시지들을 상기 디코더에 송출하는 단계;

[0037] - 사용자가 제1 메시지 내에 포함된 큐들(cues)을 액세스하도록 인증받으면, 제어 워드들을 발생시켜 상기 디코더에 의해 수신되는 상기 시청각 신호를 디스크램블하도록 상기 디코더 또는 이와 관련된 휴대용 객체에서 상기 제1 메시지들을 복호화하는 단계를 포함하는데,

[0038] 제3 하이브리드 메시지들 각각의 송출은 적어도 하나의 암호화된 제어 워드, 디코더 어드레스 및 권리 취소 큐(cue)의 조합으로부터 발생되는 것을 특징으로 한다.

[0039] 가입 권리들 또는 가입자 권리들을 무효화하기 위하여 하이브리드 메시지들(E3M)을 사용하면, 이 취소가 수신되도록 보장할 수 있음으로(그 이유는 수신된 하이브리드 메시지가 없다면, 텔레비전을 시청할 수 없기 때문이다), 위에 언급된 유형의 시스템 무단복제를 할 수 없게 된다.

[0040] 본 발명의 방법은 디스패칭된 메시지의 양을 감소시키는 것을 가능하도록 한다. 실제로, 가입자를 위한 오퍼(offer)를 억제하기 위하여 권리 할당 관리 메시지(EMM)를 디스패칭하는 것을 더 이상 필요로 하지 않는다. 하이브리드 메시지(E3M)를 사용함으로써 이것을 직접 행하는 것이 가능하다. 가입 오퍼들 자체를 초과하여, 가입 종료에 대한 가입내용(키, 진부화(obsolescence) 날자, 그룹)을 삭제할 수 있다. 유용하게도, 하이브리드 메시지에서, 제어 워드는 디코더 어드레스 및 취소 큐(cue, 정보) 를 암호화하기 위하여 사용된 특정 키와 상이한 동작 키에 의해 암호화된다. 유용하게도, 비대칭 암호작성법이 사용될 수 있다.

[0041] 또한, 본 발명은 가입자들의 식별자와 그들의 권리들을 데이터베이스의 형태로 저장하는 가입자 관리 유닛(SMS), EMM 메시지 암호화 유닛, SMS 유닛에 의해 제어된 가입자 인증 시스템, 시청각 프로그램의 MPEG 압축기, ECM 메시지 암호화 유닛, 스크램블러/멀티플렉서, 각각의 스마트 카드와 관련된 디코더들, 가입자 인증 시스템 및 디코더에 링크된 통신 서버, 스크램블러/멀티플렉서에 링크된 슈퍼바이저, 위성, 지상 또는 스크램블러/멀티플렉서와 디코더 간의 케이블에 의한 링크를 포함하는 유료 텔레비전 시스템에 관한 것이며, 각각의 유료 시청각 프로그램 채널에 대하여, 취소 EMM 메시지 큐(message queue) 및 멀티플렉서를 포함하는 ECM 메시지 필드와 EMM 메시지 필드를 결합하는 유닛을 구비하며, 필드들을 결합하는 이 유닛은 스크램블러/멀티플렉서의 입력에 배치된다.

[0042] 본 발명은 또한 하이브리드 메시지를 처리하고 그 메모리 내에 등록된 권리를 삭제하는 수단을 구비하며 제어 워드를 생성하기 위하여 현재 동작 키로 암호화된 제어 워드를 복호화하는 디코더 또는 스마트 카드에 관한 것이다.

[0043] 본 발명은 최종적으로 유료 텔레비전 시스템에서의 하나 이상의 디코더로 전송된 메시지에 관한 것이며, 상기 유료 텔레비전 시스템은 적어도:

[0044] - 암호화된 제어 워드 필드로서, 상기 제어 워드는 소정 기간 동안, 디코더에 의해 수신된 시청각 신호를 디스크램블하도록 하는, 상기 암호화된 제어 워드 필드;

[0045] - 디코더 어드레스 필드; 및

[0046] - 상기 어드레스 필드 내의 어드레스에 의해 어드레스되는 하나의(또는 그 이상의) 디코더(들)로 할당된 권리에 대한 취소 필드를 포함한다.

실 시 예

[0050] 본 발명의 방법에서, 일시적 디스크램블된 미리보기 프로그램을 전달하는 하나 이상의 채널로의 액세스의 권리를 억제하는 것은 ECM 및 EEM 메시지와 상이한, E3M으로 표시된 제3 형태의 메시지의 도움으로 수행된다.

[0051] 유료 텔레비전 시스템에서 하나 이상의 디코더로 전송된 이러한 E3M은 적어도:

[0052] - 암호화된 제어 워드 필드,

[0053] - 디코더 어드레스 필드, 및

[0054] - 어드레스 필드 내의 단일/그룹화된 어드레스에 의해 어드레스되는 하나(또는 그 이상)의 디코더(들)로 할당된

권리에 대한 취소 필드를 포함한다.

[0055] 더구나, 각각의 하이브리드 메시지는 전형적으로 EMM 식별자 헤더 필드와 상이한 ECM 식별자 헤더 필드를 포함한다. 이와 같은 식별자 헤더 필드는 수신시 ECM 및 EMM 메시지를 구별하는 것을 가능하게 한다.

[0056] 제어 워드 및 권리 취소 정보(cue)를 둘 다 각각 포함하는 E3M 메시지에서 일시적 디스크램블된 미리보기 프로그램을 전달하는 채널로의 액세스의 권리를 취소한다는 사실은, 도용자가 현재 프로그램으로의 준-순시 액세스(quasi-instantaneous access)를 더 이상 할 수 없다는 두려움으로 인해 "블로커들"을 사용할 수 없기 때문에, 무단복제를 제한한다. 이것은 도용자가 스트램블된 시청각 프로그램의 디스크램블에 사용된 제어 워드로의 임의의 액세스를 차단하기 때문이다.

[0057] 구체적으로, 소정 순간 to 에 요구시 또는 오퍼를 통하여 일시적 디스크램블된 미리보기(또는 프로그램)를 갖는 프로그램에 액세스하고, 이 오퍼에게 지불하지 않기 위하여 to+△t(△t는 가능한 매우 짧게 된다)의 순간에서 명백한 요청 또는 거래의 디폴트를 통하여 이를 취소하는 가입자는, 요청받는 오퍼를 무료로 보기 위하여 그 다음 EMM 메시지에 대한 "EMM 블로커"를 사전에 사용할 수 있다(두 개의 EMM 갱신 사이클의 최대 시간 스케일 동안, 이것은 전형적으로 휴대형 카드는 두 개의 동작 키-현재 키 및 미래 키-를 저장하기 때문이다).

[0058] "E3M 메시지 블로커"를 사용하는 것은 더 이상 불가능한데, 그 이유는 E3M 메시지를 차단하는 것은 그 자체가 요청받은 프로그램을 보지 못하도록 하기 때문이다.

[0059] 상업적인 오퍼의 철회(또는 가입의 종료)는 E3M 메시지의 수단에 의해 달성된다. 각각의 E3M 메시지는 EMM 메시지에 의해 전달된 임의의 큐(cue, 정보) 및 ECM 메시지에 의해 전달된 임의의 큐(cue, 정보)의 조합(또는 결합)에 기인하는데, 즉, 각각의 E3M 메시지는 하나 이상의 암호화된 제어 워드, 디코더 어드레스 및 권리 취소 큐(cue, 정보)를 포함한다.

[0060] 도 2에 도시된 바와 같이, 유료 텔레비전 시스템의 예에 의해 제공된 구조는, 가입자들의 식별자와 그들의 권리들을 데이터베이스의 형태로 저장하는 가입자 관리 유닛(SMS)(20), EMM 메시지 암호화 유닛(21), SMS 유닛(20)에 의해 제어된 가입자 인증 시스템(22), 시청각 프로그램의 MPEG 압축기(23), ECM 메시지 암호화 유닛(24), 스크램블러/멀티플렉서(25), 각각의 스마트 카드(27)와 관련된 디코더들(26), 가입자 인증 시스템(22) 및 디코더(26)에 링크된 통신 서버(30), 스크램블러/멀티플렉서(25)에 링크된 슈퍼바이저(31), 위성, 지상 또는 스크램블러/멀티플렉서(25)와 디코더(26) 간의 케이블에 의한 링크(32)를 포함한다. 이 형태의 시스템의 동작 방식에 대한 상세한 설명은 예를 들어, 특허 출원 WO98/43430에 제공된다.

[0061] 도 3에 나타낸 바와 같이, EMM 메시지 필드들 및 ECM 메시지 필드들을 결합하는 유닛은 통상적으로 각각의 유료 시청각 프로그램 채널에 대하여, 취소 EEM 큐(queue)(40) 뿐만 아니라, 멀티플렉서(41)를 구비한다. 필드들을 결합하는 이 유닛은 통상적으로 도 2의 스크램블러/멀티플렉서의 입력에 배치된다.

[0062] 통상적으로, 소정 채널에 대하여, 취소 EMM 메시지가 발생될 때, 이 메시지는 큐(queue)(40)에 저장된다. ECM 메시지가 (통상적으로 1 초 정도의 빈도로) 발생될 때, 임의의 취소 EMM 메시지 및 ECM 메시지 필드들을 결합하여 하이브리드 E3M 메시지를 발생시키기 위하여 멀티플렉싱이 수행된다. 이와 같은 E3M 메시지는 멀티플렉서(41)의 출력에서, 통상적으로:

[0063] - ECM 메시지로부터 나오는 암호화된 제어 워드 필드,

[0064] - 취소 EMM 메시지로부터 나오는 디코더 어드레스 필드, 및

[0065] - 동일한 EMM 메시지로부터 나오는 상기 어드레스 필드 내의 어드레스에 의해 어드레스된 디코더 또는 디코더들의 세트에 할당된 권리에 대한 취소 필드를 포함한다.

[0066] 특히, EMM 메시지들은 특정하며, 개별적이거나 그룹 메시지들일 수 있다.

[0067] ECM 메시지들의 변경 사이클이 2와 10초 사이인 경우, 300 내지 1800의 상이한 변경들에 대해 시간당 한 사이클을 가질 수 있다.

[0068] 동작 키를 인지할 수 있는 권한이 있는 동시 사용자 부분에 대한 무단복제(정확하게 서명된 삭제 메시지들을 디스패칭하는 무단복제)를 배제하기 위하여, 이러한 삭제는 동작 키를 사용하여 (서명되고 인증된) ECM 메시지에 포함되는 가입자의 특정 키(Q)에 의해 서명된 EMM 메시지를 통하여 수행될 수 있다.

[0069] 본 발명의 방법의 주요 제약은 각각의 ECM 메시지의 전체 크기에 대응하며 이러한 ECM 메시지 내용들의 처리의

지속기간에 또한 대응한다.

[0070] 그러나, 이와 같은 제약은 현재 불편하지 않다. ECM 메시지의 크기는 (연쇄 모드를 사용하지 않고) 실제로 256 바이트에 이르고, 스마트 카드들에 존재하는 동적 RAM 메모리들이 충분하다.

[0071] 또한, 프로세서(CPU)의 속도 및 크립토프로세서(cryptoprocessor)의 용도는 적절한 프로세싱 시간을 달성하는 것을 가능하게 한다.

[0072] 수반하는 사용자(concurrent user)로부터 발생하는 임의의 시스템 공격을 방지하기 위하여, 비대칭 형태의 암호법이 사용된다: 특히, 이 사용자는 이전에 비대칭 키들을 해독하지 않으면, 가입자들의 스마트 카드들에 의해 수용된 EMM 또는 ECM 메시지들을 만들어 낼 수 없다. 따라서, 타원형 곡선 또는 RSA-형 알고리즘들이 사용된다: 전자의 형태의 알고리즘들은 메모리에서 더 적은 공간을 차지하는 장점을 가지며, 더 중요한 메시지들의 유용한 내용들을 갖는 것이 가능하다는 장점을 갖는다.

[0073] 본 발명에 따르면, 스마트 카드는 세가지 형태들의 메시지들을 처리할 수 있는데, 즉, 종래의 방식으로:

[0074] - 가입자의 권리의 변경 및 그것의 보호된 메모리 내에 저장하는 동작 키를 고려하기 위하여 EMM 메시지들을 처리하고,

[0075] - 제어 워드들을 발생시키기 위하여 현재 동작 키로 ECM 메시지들의 암호화된 제어 워드들을 복호화하고,

[0076] 본 발명에 따라서:

[0077] - 그것의 메모리 내에 등록된 권리의 삭제에 의해 이전에 할당된 권리를 취소하기 위하여 하이브리드 E3M 메시지들을 처리하고, 제어 워드들을 발생시키기 위하여 현재 동작 키로 E3M 메시지들의 암호화된 현재 워드들을 복호화할 수 있다는 것을 주의해야만 한다.

[0078] 이와 같은 기능은 또한 카드 대신에 디코더 내에 전체적으로 또는 부분적으로 포함될 수 있다.

도면의 간단한 설명

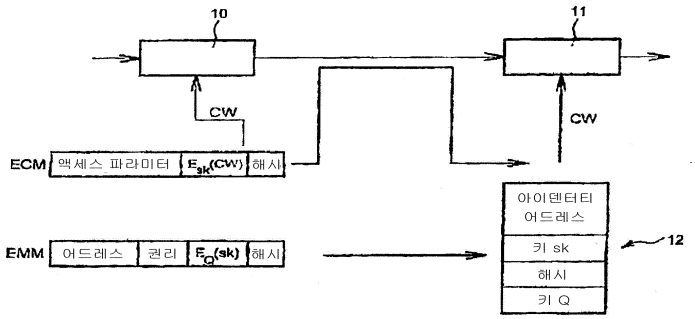
[0047] 도 1은 디지털 텔레비전 영역내에서 동작하는 종래 기술의 코딩/디코딩 시스템을 도시한 도면.

[0048] 도 2는 유료 텔레비전 시스템의 일반적인 구조의 도면.

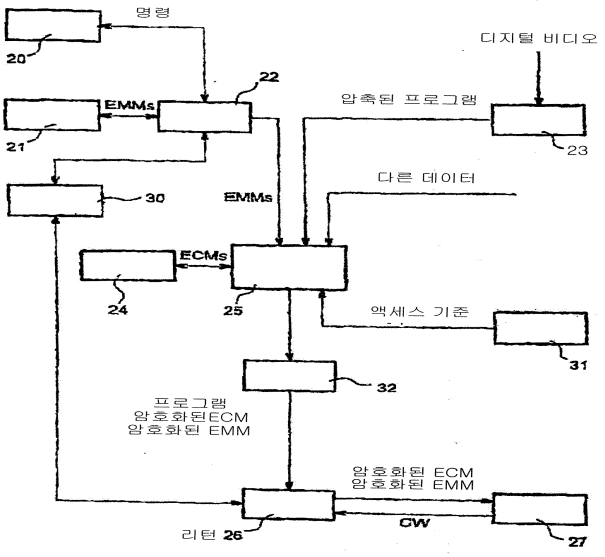
[0049] 도 3은 도 2의 구조의 멀티플렉서에 포함된 본 발명에 따른 필드 결합 유닛의 블럭도.

도면

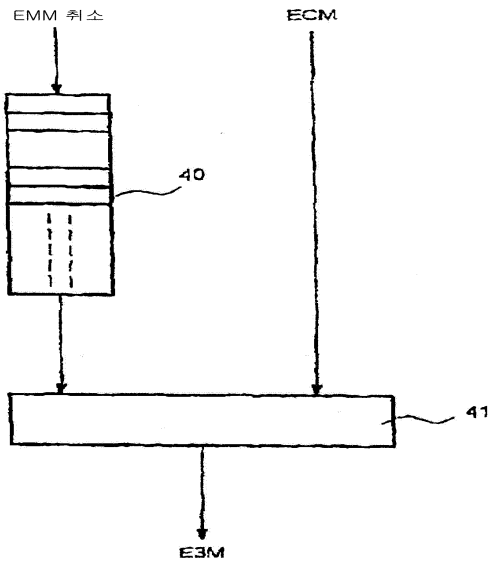
도면1



도면2


명령
20
22
EMMs
21
디지털 비디오
압축된 프로그램
23
다른 데이터
30
EMMs
ECMs
24
25
액세스 기준
31
32
프로그램
암호화된ECM
암호화된 EMM
암호화된 ECM
암호화된 EMM
CW
리턴 26
27

도면3


EMM 취소
ECM
40
41
E3M