

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl.⁶
H04N 7/167

(45) 공고일자 2005년05월03일
(11) 등록번호 10-0486865
(24) 등록일자 2005년04월22일

(21) 출원번호	10-1999-7008506	(65) 공개번호	10-2000-0076402
(22) 출원일자	1999년09월17일	(43) 공개일자	2000년12월26일
번역문 제출일자	1999년09월17일		
(86) 국제출원번호	PCT/EP1997/002111	(87) 국제공개번호	WO 1998/43431
국제출원일자	1997년04월25일	국제공개일자	1998년10월01일

(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, 키르기스스탄, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크멘, 터키, 트리니다드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투갈, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 가나, 감비아, 인도네시아, 세르비아 앤 몬테네그로, 시에라리온, 짐바브웨, 기니 비사우,

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

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기스스탄, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크멘,

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

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

(30) 우선권주장 97400650.4 1997년03월21일 유럽특허청(EPO)(EP)

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

(72) 발명자 사르파티,장-클라우드
프랑스,에프-93800엔피나이설세인,플레이스드오베리셀,2-4

메릭,제롬
프랑스,에프-60300셀리스,루드뮤스,55

(74) 대리인 조성욱
최홍순
박세걸
특허법인세신

심사관 : 변형철

(54) 엠팩 수신기/디코더로 데이터를 다운로드하는 방법 및 이를 수행하기 위한 엠팩 송신 시스템

요약

디지털 위성 텔레비전 시스템에서, 텔레비전은 그의 신호를 세트 탑 박스와 같은 수신기/디코더를 통하여 수신하며, 대화식 애플리케이션들은 다운로드될 수 있으며 수신기/디코더상에서 실행될 수 있다. 애플리케이션 코드는 모듈들로서 배열되며, 또한 모듈들의 다운로드에는 특정 국부 어드레스내부에서 디렉토리 모듈을 검색함으로써 진행된다. 모듈들은 부호화되며 디렉토리 모듈은 부호화되고 암호화되어 단일 암호화는 애플리케이션을 구성하는 모든 모듈들에 적용된다. 다중 공개 암호화 키들은 수신기/디코더내의 ROM내에 저장되어, 애플리케이션들은 소스들이 서로의 개인 암호화 키들을 알 필요가 없이 다른 소스들에 의해 생성된다. 설비가 암호화 키가 수신기/디코더내의 RAM내에 일시적으로 저장될 수 있도록 제공되어, 수신기/디코더의 제조업자가 그의 기능성을 체크할 수 있다. 디렉토리의 서명은 디렉토리 모듈의 더미 데이터의 블록에의 가변 위치에 숨겨질 수 있다. 다운로드될 애플리케이션은 수신기/디코더에 저장된 애플리케이션 확인 비트 맵에 대하여 체크될 수 있다.

대표도

도 8

색인어

디지털 위성 텔레비전 시스템, MPEG 수신기/디코더, 애플리케이션, 디렉토리, MPEG 송신 시스템

명세서

기술분야

본 발명은:

- MPEG 수신기/디코더로 데이터를 다운로드하는 방법;
- 상기의 MPEG 수신기/디코더 그 자체; 및
- MPEG 송신 시스템에 관한 것이다.

배경기술

한정하려는 것은 아니지만 특히 위성 텔레비전 시스템에서, 텔레비전 신호를 주로 방송하고자 하는 디지털 송신 시스템의 출현은 상기 시스템을 다른 목적에 이용할 수 있는 가능성을 주었다. 이들 중 하나가 컴퓨터 파일 또는 소프트웨어를 최종 사용자에게 다운로드할 수 있게 하는 것이다.

이것을 수행하는 한 방법은 텔레비전 신호가 수신되는 수신기/디코더에서 애플리케이션을 가동시키는 것이다. 애플리케이션에 대한 코드는 수신기/디코더 내에 영구적으로 저장될 수 있다. 그러나, 이는 다소 제한적이다. 바람직하게는, 수신기/디코더는 필요한 애플리케이션에 대한 코드를 다운로드할 수 있어야 한다. 이러한 방법에서, 더 많은 다양성이 제공될 수도 있으며, 애플리케이션들은 사용자의 측에서 어떠한 조치도 없이 필요할 때 갱신될 수 있다. MPEG 시스템에서, 애플리케이션 코드는 MPEG 테이블에 다운로드될 수도 있다. 그러나, 단일 MPEG 테이블에 의하여 다운로드될 수 있는 일부분의 코드의 크기에 한계가 있다. 게다가, 만일 전체 애플리케이션들이 가동될 수 있기 전에 다운로드될 필요가 있다면, 이는 수용할 수 없는 딜레이를 사용자에게 제공할 수도 있다. 따라서, 다수의 모듈들로서 애플리케이션을 다운로드할 수 있는 것이 바람직하다. 그러나, 이는 이후에 확인할 수 있는 문제를 발생시키고, MPEG 비트스트림으로부터 특정한 애플리케이션에 필요한 모듈들을 추출한다. 본 발명의 제 1 측면은 이 문제에 관련된다.

발명의 상세한 설명

본 발명의 제 1 측면에 의하면, MPEG 수신기/디코더로 애플리케이션의 적어도 일부분을 다운로드하는 방법이 제공되고, 이 방법은 다수의 모듈들로 애플리케이션을 분할하는 단계; 상기 각 모듈들을 동일한 테이블 식별자("TID")와 소정의 TID 확장자 이외의 객체의 상이한 테이블 식별 확장자를 갖는 개개의 MPEG 테이블로서 포맷하는 단계; 동일한 상기 TID 및 상기 소정의 TID 확장자를 갖는 모듈들에 대한 디렉토리 MPEG 테이블을 생성하는 단계; MPEG 비트스트림에서 디렉토리 MPEG 테이블 및 모듈 MPEG 테이블을 순환적으로 전송하는 단계; 및 상기 MPEG 수신기/디코더에서, MPEG 비트스트림을 수신하는 단계; 상기 디렉토리 MPEG 테이블을 다운로드하도록 상기 소정의 TID 확장자를 갖는 MPEG 테이블중 하나를 다운로드하는 단계; 상기 디렉토리 MPEG 테이블의 내용으로부터 상기 모듈 MPEG 테이블의 TID 확장자를 결정하는 단계; 및 상기 다운로드된 디렉토리 MPEG 테이블의 것과 동일한 TID, 및 다운로드된 디렉토리 MPEG 테이블로부터 결정된 TID-확장자를 갖는 모듈 MPEG 테이블들 중 적어도 하나를 다운로드하는 단계를 포함하고, 상기 디렉토리는 상기 각 모듈에 대해 그 모듈의 명칭과 상기 개개의 TID 확장자를 포함한다.

삭제

삭제

삭제

삭제

삭제

삭제

삭제

삭제

삭제

삭제

따라서, 애플리케이션은 필요할 때 적절하게 가동되어 다운로드될 수 있는 다수의 모듈들로 구성되며, 디렉토리 테이블은 특정한 TID 확장자를 갖기 때문에 쉽게 확인될 수 있으며, 일단 다운로드가 되면 수신기/디코더가 각 TID 확장자로부터 모듈 테이블을 확인할 수 있게 한다.

바람직하게, 상기 방법은 상기 전송된 디렉토리 MPEG 테이블에 버전 식별자를 포함하는 단계; 및 상기 수신기/디코더에서, 상기 현재 전송된 디렉토리 MPEG 테이블의 버전 식별자가 상기 현재 다운로드된 디렉토리 MPEG 테이블의 버전 식별자보다 새로운지를 판단하는 단계; 및 상기 현재 전송된 디렉토리 MPEG 테이블의 버전 식별자가 상기 현재 다운로드된 디렉토리 MPEG 테이블의 버전 식별자보다 새로우면, 상기 디렉토리 MPEG 테이블을 다운로드하는 단계, 상기 TID 확장자를 결정하는 단계, 및 상기 모듈 MPEG 테이블중 적어도 하나를 다운로드하는 단계를 반복하는 단계를 더 포함한다.

삭제

삭제

삭제

따라서, 애플리케이션이 변경되어야 하고, 이것은 자동적으로 검출될 수 있으며, 갱신된 디렉토리 및 어떠한 갱신된 모듈이 다운로드될 수 있다. 상기 모듈 MPEG 테이블중 적어도 하나는 MPEG 비트스트림 내에서 개별적으로 송신되는 다수의 MPEG 섹션들로서 포맷될 수 있으며, 각 MPEG 섹션들은 MPEG 테이블내 그 MPEG 섹션의 ID 및 MPEG 테이블내 섹션 번호 표시를 소정 부분에 포함한다.

본 발명의 제 2 측면에 의하면, 본 발명의 제 1 측면의 방법 일부를 수행하는데 이용하기 위한 MPEG 수신기/디코더가 제공되며, 이 MPEG 수신기/디코더는 상기 MPEG 비트스트림을 수신하기 위한 수신기; 저장 수단; 및 상기 소정의 TID 확장자를 갖는 상기 수신된 디렉토리 MPEG 테이블중 하나가 저장 수단으로 다운로드될 수 있도록 하고, 상기 디렉토리 MPEG 테이블의 내용으로부터 상기 모듈 및 MPEG 테이블의 TID 확장자를 결정하며, 상기 다운로드된 디렉토리 테이블로서 동일한 TID를 갖는 상기 모듈 MPEG 테이블중 하나와 상기 다운로드된 디렉토리 MPEG 테이블로부터 결정된 TID 확장자가 상기 저장 수단으로 다운로드되도록 프로그램되는 처리 수단을 포함한다.

삭제

삭제

삭제

바람직하게, 처리 수단은 상기 현재 수신된 디렉토리 MPEG 테이블의 버전 식별자가 상기 다운로드된 디렉토리 MPEG 테이블의 버전 식별자보다 새로운지를 결정하고, 상기 현재 수신된 디렉토리 MPEG 테이블의 버전 식별자가 상기 다운로드된 디렉토리 MPEG 테이블의 버전 식별자보다 새로우면, 상기 디렉토리 MPEG 테이블의 다운로드, 상기 TID 확장자의 결정, 및 상기 모듈 MPEG 테이블중 적어도 하나의 다운로드를 반복하도록 프로그램된다.

수신기/디코더가 개별적으로 전송된 다수의 섹션들로서 포맷된 모듈 테이블들중의 적어도 하나를 수신하도록 배열되는 경우에, 바람직하게 처리 수단은 상기 처리 수단이 다운로드된 섹션들의 섹션 ID 및 섹션 번호 표시로부터 모든 섹션들이 다운로드된 것을 결정할 때까지, MPEG 섹션들이 저장 수단으로 반복적으로 다운로드되도록 프로그램된다.

바람직하게, 수신기/디코더는 적어도 하나의 MPEG 테이블로서 포맷된 애플리케이션을 수신하도록 배열되는 병렬 포트 및/또는 직렬 포트를 또한 포함하며, 이 경우에, 바람직하게는 짧은 MPEG-2 포맷이 채용되며, 바람직하게는 긴 MPEG-2 포맷이 예를 들어, 위성 또는 케이블과 같은 원격 수신에 이용된다.

애플리케이션은 그것이 인공위성 텔레비전 시스템에 걸쳐 전송될 필요없이 다운로드될 수 있기 때문에, 이것은 제조업자가 수신기/디코더의 특정 형태를 검사하고자 하는 경우에 특히 유용하다.

본 발명의 제 3 측면에 의하면, MPEG 수신기/디코더로 다운로드되는 애플리케이션을 다수의 모듈로 분할하기 위한 수단; 상기 각 모듈을 동일한 TID와 소정의 TID 확장자 이외의 개개의 상이한 TID 확장자를 갖는 개개의 MPEG 테이블로서 포맷하기 위한 수단; 동일한 상기 TID 및 상기 소정의 TID 확장자를 갖는 상기 모듈에 대한 디렉토리 MPEG를 생성하기 위한 수단; 및 상기 디렉토리 MPEG 테이블과 상기 모듈 MPEG 테이블들을 MPEG 비트스트림으로 순환적으로 전송하기 위한 수단을 포함하며, 상기 디렉토리는 상기 각 모듈에 대해 그 모듈의 명칭과 상기 개개의 TID 확장자를 포함하는 MPEG 전송 시스템이 제공된다.

바람직하게, 시스템은 상기 디렉토리 MPEG 테이블에 대한 버전 식별자를 생성하기 위한 수단을 더 포함할 수 있고, 상기 디렉토리 MPEG 테이블 생성 수단은 상기 디렉토리 MPEG 테이블에 상기 생성된 버전 식별자를 포함하도록 동작할 수 있다.

모듈 포매팅 수단은 상기 모듈 MPEG 테이블들중 적어도 하나를 다수의 MPEG 섹션들로서 포맷하도록 동작할 수 있으며, 각 섹션은 소정의 부분에 그 MPEG 테이블에서의 그 MPEG 섹션의 식별자 및 그 MPEG 테이블에서 MPEG 섹션 번호의 표시를 포함한다.

바람직하게, 상기 수신기/디코더는 예를 들어, 바이러스를 포함할 수 있는 허가되지 않은(unauthorised) 애플리케이션의 다운로드로부터 보호되어야 한다. 따라서, 애플리케이션의 적어도 일부를 암호화 및 부호화하는 개념은 신중히 고려될 수 있다.

본 발명의 제 4 측면에 의하면, 데이터를 MPEG 수신기/디코더로 다운로드하는 방법이 제공되고, 이 방법은 다운로드되는 상기 데이터에 대한 서명을 생성하는 단계; 개인키를 사용하여 상기 서명을 암호화하는 단계; 다운로드되는 상기 데이터, 상기 암호화된 서명 및 상기 개인키에 대한 식별자를 MPEG 테이블로서 포맷하는 단계; 상기 MPEG 테이블을 전송하는 단계; 및 상기 수신기/디코더에서, 상기 MPEG 테이블을 수신하는 단계; 상기 수신된 MPEG 테이블에서 상기 키 식별자에 따라 다수의 공개키중 하나를 선택하는 단계; 복호화된 서명을 제공하도록 상기 선택된 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 서명을 복호화하는 단계; 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하는 단계; 및 상기 복호화된 서명과 상기 수신된 데이터에 대한 상기 수신기/디코더에서 생성된 서명을 비교하는 단계를 포함한다.

따라서, 수신기/디코더는 소스들이 서로의 개인들을 알 필요가 없이, 하나 이상의 소스로부터 암호화된 서명들을 갖는 애플리케이션을 다운로드하는데 사용될 수 있다.

상기 방법은 소정의 키 식별자를 갖는 개인키를 사용하여 암호화된 서명을 갖는 애플리케이션을 상기 수신기/디코더로 다운로드하는 단계; 상기 수신기/디코더가 추가 키를 수신하도록 상기 수신기/디코더에서 상기 애플리케이션을 실행하는 단계; 및 상기 추가 키를 상기 수신기/디코더의 휘발성 메모리의 영역에 저장하는 단계를 더 포함할 수 있다. 이 경우에 있어서, 애플리케이션을 실행하는 단계 동안, 상기 추가 키가 예를 들어, 수신기/디코더의 병렬 포트, 직렬 포트 또는 스마트카드를 통해 국부적으로 상기 수신기/디코더에 공급될 수 있다. 수신기/디코더가 모뎀 연결을 가지면, 바람직하게 수신기/디코더는 이와 같은 추가 키가 모뎀을 통해 공급되는 것을 방지하도록 배열된다.

이들 형태는 수신기/디코더를 시험하고자 하는 제조업자가 수신기/디코더로 키를 다운로드할 수 있게 한다.

상기 방법은 수신기/디코더에서 상기 수신기/디코더의 메모리의 보호 영역에서 선택된 공개키에 대한 확인 플래그를 조사하는 단계, 및 상기 조사 플래그가 설정되지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하는 단계를 더 포함할 수 있다.

따라서, 다수의 공개키가 수신기/디코더의 메모리로 영구적으로 제공될 수 있지만, 다수의 공개키중 어느 하나가 선택적으로 금지될 수 있으며, 그것은 예를 들어, 특정 공개키와 관련된 개인키의 프라이버시가 파괴되거나 또는 동일한 키를 사용하는 2명의 운영자가 개별의 키들을 갖고자 하는 것을 결정하는 경우에 필요로 될 수 있다.

상기에서 설명된 바와 같이, 상기 수신기/디코더가 소정의 키 식별자를 갖는 개인키를 사용하여 암호화된 서명을 갖는 애플리케이션을 다운로드하도록 배열되는 경우에, 상기 수신기/디코더의 메모리의 보호 영역에서, 상기 소정의 키 식별자를 갖는 상기 개인키는 상기 애플리케이션에 의해 변경될 수 있는 확인 플래그를 가질 수 있으며, 이와 같은 추가 키를 수신할 수 있는 능력은 그 확인 플래그의 상태에 의존하여 결정된다.

이들 후자 형태에 의하면, 공개키에 대한 확인 플래그가 본 발명의 제 4 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 5 측면은 데이터를 MPEG 수신기/디코더로 다운로드하는 방법을 제공하고, 이 방법은 다운로드되는 상기 데이터에 대한 서명을 발생하는 단계; 개인키를 사용하여 서명을 암호화하는 단계; 다운로드되는 상기 데이터, 상기 암호화된 서명 및 상기 개인키에 대한 식별자를 MPEG 테이블로서 포맷하는 단계; 상기 MPEG 테이블을 전송하는 단계; 및 상기 수신기/디코더에서, 상기 MPEG 테이블을 수신하는 단계; 상기 수신기/디코더의 메모리의 보호 영역에서, 상기 수신된 MPEG 테이블에서 식별된 상기 개인키에 해당되는 공개키에 대한 확인 플래그를 조사하는 단계; 및 상기 조사 플래그가 설정되면, 복호화된 서명을 제공하도록 상기 수신된 MPEG 테이블에서 식별된 개인키에 해당되는 상기 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 서명을 복호화하는 단계; 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하는 단계; 및 상기 복호화된 서명과 상기 수신된 데이터용 상기 수신기/디코더에서 생성된 상기 서명을 비교하는 단계를 포함한다.

바람직하게, 본 발명의 제 4 및 제 5 측면의 방법은 다운로드되는 상기 데이터에 대한, 상기 암호화 단계에서 상기 서명으로 암호화되고, 상기 복호화 단계에서 상기 서명으로 복호화되는 확인 코드를 생성하는 단계; 상기 수신기/디코더의 메모리의 보호 영역에서 저장된 확인 코드를 조사하는 단계; 및 상기 조사 확인 코드와 상기 복호화된 확인 코드를 비교하는 단계를 더 포함한다.

따라서, 수신기/디코더는 어떤 애플리케이션 또는 애플리케이션 형태만을 수신하도록 설정될 수 있다.

이들 형태는 본 발명의 제 4 및 제 5 측면과 관계없이 제공될 수 있다. 따라서, 본 발명의 제 6 측면은 데이터를 MPEG 수신기/디코더로 다운로드하는 방법을 제공하고, 이 방법은 다운로드되는 상기 데이터에 대한 확인 코드를 생성하는 단계; 다운로드되는 상기 데이터 또는 일부에 대한 서명을 생성하는 단계; 개인키를 사용하여 상기 확인 코드 및 상기 서명을 암호화하는 단계; 다운로드되는 상기 데이터, 상기 암호화된 확인 코드 및 서명을 적어도 하나의 MPEG 테이블로서 포맷하는 단계; 상기 또는 각 MPEG 테이블을 전송하는 단계; 및 상기 수신기/디코더에서, 상기 또는 각 MPEG 테이블을 수신하는 단계; 상기 개인키에 해당되는 공개키를 사용하여 상기 수신된 MPEG 테이블(들)에서 상기 암호화된 확인 코드 및 서명을 복호화하는 단계; 상기 수신기/디코더의 메모리의 보호 영역에서 저장된 확인 코드를 조사하는 단계; 상기 조사 확인 코드와 상기 복호화된 확인 코드를 비교하는 단계; 상기 수신된 MPEG 테이블(들)에서 상기 데이터 또는 상기 일부에 대한 서명을 생성하는 단계; 및 상기 복호화된 서명과 상기 수신 데이터용 상기 수신기/디코더에서 생성된 상기 서명을 비교하는 단계를 포함한다.

바람직하게, 상기 방법은 상기 확인 코드 비교 단계에서, 상기 조사 확인 코드와 상기 복호화된 확인 코드가 서로 일치하지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하는 단계를 더 포함한다.

본 발명의 제 4 내지 제 6 측면에 의하면, 다운로드되는 상기 데이터의 서명이 상기 데이터 블록의 개시와 상기 서명의 개시 사이에서 선택된 오프셋과 함께 다른 데이터를 포함하는 데이터 블록에 암호화되며, 상기 수신기/디코더에서 상기 수신기/디코더의 메모리의 보호 영역에서 적어도 하나의 저장된 오프셋을 조사하고, 상기 복호화된 데이터 블록의 개시부터 상기 적어도 하나의 조사 오프셋을 사용하여 상기 복호화된 데이터 블록으로부터 상기 서명을 추출하는 단계를 포함하는 방법이 제공될 수 있다.

따라서, 서명은 다른 더미 데이터중에 숨겨져서, 서명의 위치를 확인하는 것을 더 어렵게 만들 수 있다. 대안적으로 또는 추가적으로, 이 형태는 데이터가 하나 이상의 특정 그룹들의 수신기/디코더들에만 이용 가능하게 된다.

이들 형태는 본 발명의 제 4 내지 제 6 측면과 관계없이 제공될 수 있다. 따라서, 본 발명의 제 7 측면은 데이터를 MPEG 수신기/디코더로 다운로드하는 방법을 제공하고, 이 방법은 다운로드되는 상기 데이터에 대한 서명을 생성하는 단계; 상기 서명과, 상기 데이터 블록의 개시와 상기 서명의 개시 사이에 선택된 오프셋을 갖는 데이터 블록에서의 다른 데이터를 포함하는 단계; 개인키를 사용하여 상기 데이터 블록을 암호화하는 단계; 다운로드되는 상기 데이터와 상기 암호화된 데이터 블록을 MPEG 테이블로서 포맷하는 단계; MPEG 테이블을 전송하는 단계; 및 상기 수신기/디코더에서, 상기 MPEG 테이블을 수신하는 단계; 상기 개인키에 해당되는 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 데이터 블록을 복호화하는 단계; 상기 수신기/디코더의 메모리의 보호 영역에 적어도 하나의 저장된 오프셋을 조사하는 단계; 상기 복호화된 데이터 블록의 개시로부터 상기 적어도 하나의 조사 오프셋을 사용하여 상기 복호화된 데이터 블록으로부터 상기 서명을 추출하는 단계; 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하는 단계; 및 상기 복호화된 데이터 블록으로부터 추출된 상기 서명과 상기 수신 데이터용 수신기/디코더에서 생성된 상기 서명과 비교하는 단계를 포함한다.

상기 메모리의 보호 영역이 적어도 2 개의 이와 같은 저장된 오프셋을 갖는 경우에, 상기 비교 단계에서 상기 추출된 서명과 상기 생성된 서명이 일치하지 않으면, 바람직하게 상기 방법은 상기 저장된 오프셋중 또 다른 하나를 사용하는 상기 조사, 추출 및 비교 단계를 반복하는 단계를 포함한다.

데이터 블록에서 상기 다른 데이터의 적어도 일부는 더미 또는 임의 데이터일 수 있지만, 만약 그렇다면, 바람직하게는 더미 데이터의 어떠한 섹션도 서명을 반복하지 않는다.

본 발명의 제 4 내지 제 7 측면에 의하면, 데이터는 복수의 데이터 모듈들로서 다운로드될 수 있으며, 상기 방법은 다운로드되는 데이터의 각 모듈에 대한 모듈 서명을 생성하는 단계; 상기 데이터 모듈을 개개의 모듈 MPEG 테이블로서 포맷하는 단계; 각 모듈 MPEG 테이블의 식별자와 상기 개개의 서명을 포함하고, 서명 발생 단계의 주체인 렉토리를 생성하는 단계; 및 상기 수신기/디코더에서 상기 수신된 모듈 MPEG 테이블에 상기 각 모듈에 대한 개개의 모듈 서명을 생성하는 단계; 상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명과 상기 수신기/디코더에서 생성된 상기 개개의 모듈 서명을 비교하는 단계를 포함할 수 있다.

따라서, 다운로드되는 데이터가 다수의 모듈들로 구성되지만, 단일 암호화 처리만이 모듈들을 암호화하는데 요구되며, 단일 복호화 처리만이 서명을 검사할 수 있게 하는데 요구된다.

이들 형태는 본 발명의 제 4 내지 제 7 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 8 측면은 다수의 데이터의 모듈들을 MPEG 수신기/디코더로 다운로드하는 방법을 제공하고, 이 방법은 다운로드되는 각 데이터 모듈에 대한 모듈 서명을 생성하는 단계; 상기 데이터 모듈을 개개의 모듈 MPEG 테이블로서 포맷하는 단계; 각 모듈 MPEG 테이블의 식별자와 상기 개개의 서명을 포함하는 디렉토리를 생성하는 단계; 상기 디렉토리에 대한 디렉토리 서명을 생성하는 단계; 개인키를 사용하여 상기 디렉토리 서명을 암호화하는 단계; 상기 디렉토리와 상기 암호화된 디렉토리 서명을 디렉토리 MPEG 테이블로서 포맷하는 단계; 상기 디렉토리와 상기 모듈 MPEG 테이블들을 전송하는 단계; 및 상기 수신기/디코더에서 상기 디렉토리와 모듈 MPEG 테이블들을 수신하는 단계; 상기 개인키에 해당되는 공개키를 사용하여 상기 수신된 디렉토리 MPEG 테이블에서 상기 암호화된 디렉토리 서명을 복호화하는 단계; 상기 수신된 디렉토리 MPEG 테이블에서 상기 디렉토리에 대한 디렉토리 서명을 생성하는 단계; 상기 복호화된 디렉토리 서명과 상기 수신기/디코더에서 생성된 상기 디렉토

리 서명을 비교하는 단계; 상기 수신된 모듈 MPEG 테이블에서 상기 각 모듈에 대한 개개의 모듈 서명을 생성하는 단계; 및 상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명을 상기 수신기/디코더에서 생성된 상기 개개의 모듈 서명을 비교하는 단계를 포함한다.

바람직하게, 상기 방법은 모듈 서명 비교 단계에서 상기 수신된 디렉토리 MPEG 테이블에서의 모듈 서명과 그 모듈용 수신기/디코더에서 발생된 개개의 모듈 서명이 서로 일치하지 않으면, 상기 데이터의 이와 같은 모듈의 다운로드를 금지 또는 중지하는 단계를 더 포함한다.

바람직하게, 상기에서 설명된 방법들은 또한 비교 단계(들)에서 상기 또는 각 복호화된 서명과 상기 생성된 서명이 서로 일치하지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하는 단계를 또한 포함한다.

본 발명의 제 9 측면에 의하면, 본 발명의 제 4 측면의 방법의 일부를 수행하는데 사용하기 위한 MPEG 수신기/디코더가 제공되고, 이 MPEG 수신기/디코더는 이와 같은 MPEG 테이블들을 수신하기 위한 수단; 다수의 공개키와 상기 각 공개키에 대한 식별자를 저장하기 위한 수단; 및 상기 수신된 MPEG 테이블에서 상기 키 식별자에 따라 상기 저장된 공개키중 하나를 선택하고, 복호화된 서명을 제공하도록 상기 선택된 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 서명을 복호화하고, 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하며, 상기 복호화된 서명과 상기 수신 데이터용 상기 수신기/디코더에서 생성된 상기 서명을 비교하도록 프로그램되는 처리 수단을 포함한다.

바람직하게, 키 저장 수단은 ROM으로 제공되며, 상기 각 공개키에 대한 상기 식별자는 상기 키 저장 수단에서 그 공개키의 저장 위치로 제공될 수 있다.

상기 수신기/디코더는 휘발성 메모리의 영역을 더 포함할 수 있으며, 상기 처리 소정의 키 식별자를 갖는 개인키를 사용하여 암호화된 서명을 갖는 애플리케이션을 다운로드하고, 상기 추가 키가 상기 휘발성 메모리에 저장되도록 동작될 수 있다.

상기 수신기/디코더는 수신기/디코더의 병렬 포트, 직렬 포트 및/또는 스마트 카드 판독장치와 같은 수신기/디코더에 국부적으로 공급되는 이와 같은 추가 키를 수신하는 수단을 더 포함할 수 있다. 바람직하게, 휘발성 메모리는 RAM으로 제공된다. 더욱이, 수신기/디코더는 모뎀 연결을 가지면, 바람직하게 수신기/디코더는 추가 키가 모뎀을 통해 공급되는 것을 방지하도록 배열된다.

상기 수신기/디코더는 상기 공개키의 적어도 각 일부에 대한 확인 플래그를 저장하기 위한 메모리의 보호 영역을 더 포함할 수 있고, 상기 처리 수단은 상기 메모리의 보호 영역에서 이와 같은 선택된 공개키에 대한 확인 플래그를 조사하고, 상기 조사 플래그가 설정되지 않으면 상기 데이터의 다운로드를 금지 또는 중지하도록 프로그램될 수 있다.

또한, 상기 수신기/디코더는 상기 소정의 키 식별자를 갖는 상기 개인키에 대한 확인 플래그를 저장하기 위한 메모리의 보호 영역을 더 포함할 수 있고, 상기 처리 수단은 그 확인 플래그를 변경하는 상기 애플리케이션을 구동할 때 동작 가능하고, 상기 추가 키가 그 플래그의 상태에 따라 저장될 수 있도록 동작할 수 있다.

이 후자의 형태는 본 발명의 제 9 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 10 측면은 MPEG 수신기/디코더를 제공하며, 이 MPEG 수신기/디코더는 이와 같은 MPEG 테이블들을 수신하기 위한 수단; 공개키와 상기 공개키에 대한 식별자를 저장하기 위한 수단; 상기 공개키에 대한 확인 플래그를 저장하기 위한 메모리의 보호 영역; 및 상기 수신기/디코더의 메모리의 보호 영역에서 상기 수신된 MPEG 테이블에서 식별된 상기 개인키에 해당되는 공개키에 대한 확인 플래그를 조사하고, 상기 조사 플래그가 설정되면, 복호화된 서명을 제공하도록 상기 수신된 MPEG 테이블에서 식별된 개인키에 해당되는 상기 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 서명을 복호화하고, 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하며, 상기 복호화된 서명과 상기 수신된 데이터용 상기 수신기/디코더에 의해 생성된 상기 서명을 비교하도록 프로그램되는 처리 수단을 포함한다.

바람직하게, 키 확인 플래그(들)을 저장하기 위한 메모리는 재기록 가능한 비휘발성 메모리로 제공된다.

다수의 이와 같은 공개키가 저장되는 경우에, 바람직하게 확인 플래그(들)을 저장하기 위한 메모리가 비트맵으로서 배열된다.

본 발명의 제 9 또는 제 10 측면의 수신기/디코더는 확인 코드를 저장하기 위한 메모리의 보호 영역을 더 포함할 수 있고, 상기 처리 수단은 이와 같은 수신된 MPEG 테이블에서 상기 확인 코드를 복호화하고, 상기 저장된 확인 코드를 조사하며, 상기 조사 확인 코드와 상기 복호화된 확인 코드를 비교하도록 프로그램될 수 있다. 후자의 형태는 본 발명의 제 9 또는 제 10 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 11 측면은 MPEG 수신기/디코더를 제공하고, 이 MPEG 수신기/디코더는 이와 같은 MPEG 테이블들을 수신하기 위한 수단; 공개키와 상기 공개키에 대한 식별자를 저장하기 위한 수단; 확인 코드를 저장하기 위한 메모리의 보호 영역; 및 상기 개인키에 해당되는 상기 저장된 공개키를 사용하여 이와 같은 수신된 MPEG 테이블에서 상기 암호화된 확인 코드 및 서명을 복호화하고, 상기 메모리의 보호 영역에서 상기 저장된 확인 코드를 조사하고, 상기 조사 확인 코드와 상기 복호화된 확인 코드를 비교하고, 상기 수신된 MPEG 테이블 또는 상기 부분에서 상기 데이터에 대한 서명을 생성하며, 상기 복호화된 서명과 상기 수신된 데이터용의 상기 수신기/디코더에 의해 생성된 상기 서명을 비교하도록 프로그램되는 처리 수단을 포함한다.

삭제

처리 수단은 상기 조사 확인 코드와 상기 복호화된 확인 코드가 서로 일치하지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하도록 프로그램된다.

바람직하게, 확인 코드들을 저장하기 위한 메모리는 재기록 가능한 비휘발성 메모리로 제공되며, 비트맵으로서 배열될 수 있다.

본 발명의 제 9 내지 제 11 측면의 수신기/디코더는 적어도 하나의 오프셋을 저장하기 위한 메모리의 보호 영역을 더 포함할 수 있고, 상기 처리 수단은 이와 같은 수신된 MPEG 테이블에서 상기 암호화된 데이터 블록을 복호화하고, 상기 메모리의 보호 영역에서 상기 하나의 저장된 오프셋을 조사하며, 상기 복호화된 데이터 블록으로부터 상기 조사 오프셋을 사용하여 상기 복호화된 데이터 블록으로부터 상기 서명을 추출하도록 프로그램될 수 있다.

이 후자의 형태는 본 발명의 제 9 내지 제 11 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 12 측면은 MPEG 수신기/디코더를 제공하고, 이 MPEG 수신기/디코더는 이와 같은 MPEG 테이블들을 수신하기 위한 수단; 공개키와 상기 공개키에 대한 식별자를 저장하기 위한 수단; 적어도 하나의 오프셋을 저장하기 위한 메모리의 보호 영역; 상기 개인키에 해당되는 상기 저장된 공개키를 사용하여 이와 같은 수신된 MPEG 테이블에서 상기 암호화된 데이터 블록을 복호화하고, 상기 복호화된 데이터 블록의 개시로부터 상기 조사 오프셋을 사용하여 상기 서명을 상기 복호화된 데이터 블록으로부터 추출하고, 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하며, 상기 복호화된 데이터 블록으로부터 추출된 상기 서명과 상기 수신된 데이터에 대한 상기 수신기/디코더에서 생성된 상기 서명을 비교하도록 프로그램되는 처리 수단을 포함한다.

바람직하게, 오프셋을 저장하기 위한 메모리는 재기록 가능한 비휘발성 메모리에 의해 제공된다.

본 발명의 제 9 내지 제 12 측면의 수신기/디코더에 있어서, 처리 수단은 수신된 모듈 MPEG 테이블에서 상기 각 모듈에 대한 개개의 모듈 서명을 생성하고, 상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명을 상기 수신기/디코더에 의해 생성된 상기 개개의 모듈 서명과 비교하도록 프로그램될 수 있다.

이 후자의 형태는 본 발명의 제 9 내지 제 12 측면에 관계없이 제공될 수 있다. 따라서, 본 발명의 제 13 측면에 의하면, MPEG 수신기/디코더가 제공되고, 이 MPEG 수신기/디코더는 이와 같은 디렉토리 모듈 MPEG 테이블들을 수신하기 위한 수단; 공개키와 공개키에 대한 식별자를 저장하기 위한 수단; 및 상기 개인키에 해당되는 상기 저장된 공개키를 사용하여 상기 수신된 디렉토리 MPEG 테이블에서 상기 암호화된 디렉토리 서명을 복호화하고, 상기 수신된 디렉토리 MPEG 테이블에서 상기 디렉토리용 디렉토리 서명을 생성하고, 상기 복호화된 디렉토리 서명과 상기 수신기/디코더에 의해 생성된 상기 디렉토리 서명을 비교하고, 상기 수신된 모듈 MPEG 테이블들에서 상기 각 모듈에 대한 개개의 모듈 서명을 생성하며, 상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명과 상기 수신기/디코더에 의해 생성된 상기 개개의 모듈 서명을 비교하도록 프로그램되는 처리 수단을 포함한다.

바람직하게, 처리 수단은 수신된 디렉토리 MPEG 테이블에서의 모듈 서명과 그 모듈에 대한 수신기/디코더에서 생성된 개개의 모듈 서명이 서로 일치하지 않으면, 데이터의 이와 같은 모듈의 다운로드를 금지 또는 중지하도록 프로그램된다.

본 발명의 제 9 내지 제 13 측면의 수신기/디코더에 있어서, 바람직하게 처리 수단은 그 또는 각 복호화된 서명과 생성된 서명이 서로 일치하지 않으면, 데이터의 다운로드를 금지 또는 정지하도록 프로그램된다.

이하 첨부 도면을 참조하여 본 발명의 바람직한 실시예를 단지 예로서 설명한다.

도면의 간단한 설명

도1는 디지털 텔레비전 시스템의 전체 구성을 보여주는 도면.

도2는 도1의 디지털 텔레비전 시스템의 대화식 시스템의 구성을 보여주는 도면.

도3은 도1 및 2의 시스템의 부분을 형성하는 수신기/디코더의 인터페이스의 개략적인 다이어그램.

도4는 디지털 텔레비전 시스템에 사용된 원격 제어기의 개략적인 다이어그램.

도5는 대화식 수신기/디코더의 메모리로 다운로드된 모듈에서의 파일들의 배열을 보여주는 도면.

도6은 MPEG 스트림의 다수의 구성요소 사이의 상호관계를 보여주는 도면. 도7은 애플리케이션이 섹션들로 이루어질 수 있는 모듈들/테이블로 만들어지는 방법을 보여주는 도면.

삭제

도8은 디렉토리 모듈의 내용을 보여주는 도면.

도9는 디렉토리 모듈의 내용 부분을 보다 상세하게 보여주는 도면.

도10은 텔레비전 시스템의 수신기/디코더에서의 메모리의 다양한 영역을 보여주는 도면.

실시예

본 발명에 따른 디지털 텔레비전 시스템(1000)의 전체 구성이 도 1에 도시된다. 본 발명은 알려진 MPEG-2 압축 시스템을 사용하는 통상적인 종래 디지털 텔레비전 시스템(2000)을 포함하여 압축된 디지털 신호를 전송한다. 더 상세하게는, 방송 센터의 MPEG-2 압축기(2002)는 디지털 신호 스트림(통상적으로 비디오 신호의 스트림)을 수신한다. 압축기(2002)는 링크(linkage:2006)에 의해 멀티플렉서 및 스캐램블러(2004)에 연결된다. 멀티플렉서(2004)는 복수의 부가적인 입력 신호를 수신하고, 하나 이상의 이송 스트림을 모으고 압축된 디지털 신호를 링크지(2010)를 경유해서 방송 센터의 송신기(2008)에 전송하고, 여기서, 링크(2010)는 통신 링크를 포함하는 폭넓고 다양한 형태일 수 있다. 송신기(2008)는 업링크(2012)를 통해 위성 트랜스폰더(2014)를 향하여 전자기적 신호를 전송하고, 전자기적 신호들은 위성 트랜스폰더(2014)에서 전자적으로 처리되고, 관념상의 다운링크(notional downlink:2016)를 통해 최종 사용자에게 의하여 소유 또는 임대된 접시 형태의 지상 수신기(2018)로 방송된다. 수신기(2018)에 의해 수신된 신호가 최종 사용자에게 의해 소유 또는 임대된 통합 수신기/디코더(2020)로 전송되며, 최종 사용자의 텔레비전 세트(2022)에 연결된다. 수신기/디코더(2020)는 그 압축된 MPEG-2 신호를 텔레비전 세트(2022)용 텔레비전 신호로 디코딩한다.

조건부 액세스 시스템(3000)은 멀티플렉서(2004) 및 수신기/디코더(2020)에 연결되고, 방송 센터에 부분적으로 위치되고 디코더에 부분적으로 위치된다. 조건부 액세스 시스템(3000)은 최종 사용자로 하여금 하나 이상의 방송 공급자로부터 디지털 텔레비전 방송을 액세스할 수 있게 한다. 상업적 제공(commercial offers:즉, 방송 공급자에 의해 판매된 하나 이상의 텔레비전 프로그램)에 관련한 메시지를 복호화할 수 있는 스마트카드를 수신기/디코더(2020)에 삽입될 수 있다. 디코더(2020) 및 스마트카드를 사용할 때, 최종 사용자는 예약 모드(subscription mode) 또는 매 시청(pay-per-view) 모드로 상업적 제공을 구매할 수 있다.

멀티플렉서(2004) 및 수신기/디코더(2020)에 역시 연결되고 다시 방송 센터에 부분적으로 및 디코더에 부분적으로 위치된 대화식 시스템(interactive system:4000)은 최종 사용자로 하여금 모뎀 백 채널(modemed back channel:4002)을 통해 각종의 애플리케이션과 상호 작용할 수 있게 한다.

도 2는 본 발명의 디지털 텔레비전 시스템(1000)의 대화식 텔레비전 시스템(4000)의 일반적인 구조를 도시한다.

예를 들면, 대화식 시스템(4000)은 최종 사용자로 하여금 온 스크린(on-screen)의 카탈로그로부터 물품을 구매하도록 하고, 지방 뉴스 및 기상 지도를 요구시 문의하게 하며, 게임을 그 텔레비전 세트를 통해 즐기게 한다.

대화식 시스템(4000)은 다음과 같은 4개의 주요 구성요소를 구비한다.

- 방송 공급자로 하여금 애플리케이션을 생성하고 전개하고, 디버그하고 시험하게 하기 위한 방송 센터(또는 그 외에서)의 저작 툴(authoring tool:4004)
- 방송 공급자로 하여금 멀티플렉서 및 스캐램블러(2004)에 전달되는 애플리케이션 및 데이터를 최종 사용자에게 방송되는 MPEG-2 이송 스트림(통상적으로 프라이빗 섹션(private section))으로 삽입하기 위해 준비, 인증 및 포맷할 수 있도록 하는 저작 툴(4004)에 연결된 방송센터에서의 애플리케이션 및 데이터 서버(4006);
- 최종 사용자로 하여금 애플리케이션을 실행용 디코더(2020)의 작업 메모리로 수신, 인증, 압축해제, 로드시킬 수 있게 하기 위해, 최종 사용자에게 의해 소유 또는 임대된 수신기/디코더(2020)에 설치된 실행가능한 코드인 실행 시간 엔진(run time engine: RTE)(4008)을 포함하는 가상 계산기(virtual machine). 또한, 엔진(4008)은 상주, 범용 애플리케이션을 구동한다. 엔진(4008)은 하드웨어 및 동작 시스템과 무관하다.
- 서버(4006)에 명령하는 신호로 하여금 데이터 및 애플리케이션을 최종 사용자의 요구시 MPEG-2 이송 스트림으로 삽입하게 할 수 있기 위한 수신기/디코더(2020)와 애플리케이션 및 데이터 서버(4006)간의 모뎀 백 채널(4002).

대화식 시스템은 수신기/디코더의 기능 및 그 내부에 포함된 각종 장치를 제어하는 "애플리케이션"을 사용해서 동작시킨다. 애플리케이션은 "자원 파일(resource files)"로서 엔진(4008)에 표시된다. "모듈"은 자원 파일 및 데이터 세트이다. 수신기/디코더의 "메모리 볼륨"은 모듈용 저장 공간이다. "인터페이스"는 모듈을 다운로드시키기 위해 사용된다. 모듈은 MPEG-2 이송 스트림으로부터 수신기/디코더(2020)로 다운로드될 수 있다.

수신기/디코더(2020)의 물리적인 인터페이스는 데이터를 다운로드하기 위해 사용된다. 도 3을 참고로, 디코더(2020)는 예를 들어, MPEG 흐름 튜닝(4028), 직렬 인터페이스(4030), 병렬 인터페이스(4032), 모뎀(4034), 2개의 카드 판독기(4036)의 6개의 다우로당 장치를 포함한다.

본 명세서의 목적상, 애플리케이션은 바람직하게 수신기/디코더(2020)의 하이 레벨 기능(high level function)을 제어하는 컴퓨터 코드의 일부이다. 예를 들면, 최종 사용자가 텔레비전 세트(2022)의 스크린상에 보여지는 버튼 객체(object)상에 원격 제어기의 초점을 위치설정하고 확인 키를 누를 때, 버튼과 연관된 명령 시퀀스는 실행된다.

대화식 애플리케이션은 메뉴를 제시하고 최종 사용자의 요구시 명령을 실행하고 애플리케이션의 목적에 관련된 데이터를 제공한다. 애플리케이션은 수신기/디코더(2020)의 ROM(또는 FLASH 또는 기타의 비휘발성 메모리)에 저장되거나 수신기/디코더(2020)의 RAM 또는 FLASH 메모리로 방송되고 다운로드되는 상주(resident) 애플리케이션이다.

애플리케이션들의 예는 다음과 같다:

● 초기화 애플리케이션(Initiating Application). 수신기/디코더(2020)는 수신기/디코더(2020)로 하여금 MPEG-2 환경에서 즉시 동작할 수 있게 하는 모듈의 적용가능한 집합(이후에 보다 상세하게 정의됨)인 상주 초기화 애플리케이션이 구비된다. 필요하다면, 애플리케이션은 방송 공급자에 의하여 변경될 수 있는 핵심적인 특징들을 제공한다. 또한, 이것은 상주 애플리케이션과 다운로드된 애플리케이션간의 인터페이스를 제공한다.

● 시동 애플리케이션(Startup Application). 시동 애플리케이션은 다운로드되거나 상주하는 애플리케이션으로 하여금 수신기/디코더(2020)상에서 구동할 수 있게 한다. 상기 애플리케이션은 애플리케이션을 시작하기 위해 서비스의 도달시에 실행되는 부트스트랩(bootstrap)으로서 작용한다. 시동은 RAM에 다운로드되고 쉽게 갱신될 수 있다. 그것은 각 채널에서 이용가능한 대화식 애플리케이션이 다운로드후에 또는 프리로딩(preloading)후에 즉시 선택되거나 구동될 수 있도록 구성된다. 프리로딩의 경우에, 애플리케이션은 메모리(2024)에 로드되며, 필요할 때 시동에 의하여 작동된다.

● 프로그램 안내(Program Guide). 프로그램 안내는 프로그래밍에 관한 충분한 정보를 제공하는 대화식 애플리케이션이다. 예를 들어, 프로그램 안내는 디지털 텔레비전 세트의 각 채널에 제공되는 가령 일주일의 텔레비전 프로그램들에 관한 정보를 제공할 수 있다. 원격제어기(2026)의 키를 누른 것에 의하여, 최종 사용자는 텔레비전 세트(2022)의 화면 상에 보이는 이벤트에 오버레이되는 애드 온(add-on) 스크린에 액세스한다. 이 애드 온 스크린은 디지털 텔레비전 세트의 각 채널의 현재 및 다음 이벤트상에서 정보를 제공하는 브라우저이다. 원격 제어기(2026)상의 다른 키를 누른 것에 의하여, 최종 사용자는 일주일에 걸친 이벤트상에 정보 리스트를 표시하는 애플리케이션에 액세스한다. 또한, 최종 사용자는 이벤트를 간단하며 주문제조된 기준으로 조사 및 분류할 수 있다. 또한, 최종 사용자는 선택된 채널에 직접 액세스할 수 있다.

● 매 시청 지불 애플리케이션. 매 시청 지불 애플리케이션은 조건부 액세스 시스템(3000)과 관련하여 디지털 TV 세트의 각 PPV 채널에서 이용할 수 있는 대화식 서비스이다. 최종 사용자는 TV 안내 또는 채널 브라우저를 이용하여 애플리케이션에 액세스할 수 있다. 또한, 애플리케이션들은 PPV 이벤트가 PPV 채널에서 검출되자마자 자동적으로 시작한다. 이후 최종 사용자는 자신의 도터(daughter) 스마트 카드(3020)를 통해 또는 통신 서버(3022)(모뎀, 전화 및 DTMF 코드, MINITEL 등을 사용하는)를 경유해서 현재의 이벤트를 구매할 수 있다. 애플리케이션은 수신기/디코더(2020)의 ROM에 상주하거나 디코더(2020)의 RAM에 다운로드될 수 있다.

● PC 다운로드 애플리케이션. 요청시, 최종 사용자는 PC 다운로드 애플리케이션을 이용하여 컴퓨터 소프트웨어를 다운로드할 수 있다.

● 매거진 브라우저 애플리케이션(Magazine Browser application). 매거진 브라우저 애플리케이션은 온 스크린(on-screen) 버튼을 통해 최종 사용자가 향배하는 이미지의 순환 비디오 방송을 구비한다.

● 퀴즈 애플리케이션. 퀴즈 애플리케이션은 바람직하게 방송 퀴즈 프로그램과 동기화된다. 예를 들어, 다수의 선택 문제들이 텔레비전(2022)의 스크린상에 표시되고, 사용자는 원격 제어기(2026)를 이용하여 답을 선택할 수 있다. 퀴즈 애플리케이션은 답이 정확한지 아닌지를 사용자에게 알려줄 수 있으며, 사용자의 점수를 카운트할 수 있다.

● 텔레쇼핑 애플리케이션. 텔레쇼핑 애플리케이션의 한 예에서, 판매용 물품의 매물이 수신기/디코더(2020)에 전송되어 텔레비전 세트(2022)에 표시된다. 원격 제어기를 사용하여, 사용자는 구매할 특정한 물품을 선택할 수 있다. 물품에 대한 주문은 모뎀 백 채널(4002)을 통하여 애플리케이션 및 데이터 서버(4006) 또는 별도의 판매 시스템으로 전송되며, 그 판매 시스템의 전화 번호는 수신기/디코더(2020)의 카드 판독기(4036)중 하나에 삽입된 신용 카드에 대한 계정에 요금 청구하는 주문과 가능하게는 함께 수신기/디코더에 다운로드되었다.

● 텔레뱅킹 애플리케이션. 텔레뱅킹 애플리케이션의 한 예에서, 사용자는 은행 카드를 수신기/디코더(2020)의 카드 판독기(4036)중 하나로 삽입한다. 수신기/디코더(2020)는 은행 카드에 저장되거나 수신기/디코더에 저장된 전화번호를 이용하여 사용자의 은행에 다이얼하고, 이후 애플리케이션은 예를 들어 계정 계산서를 전화선을 통해 다운로드하고, 계정들간의 자금을 이동하고, 수표장을 요청하는 원격 제어기(2026)를 사용하여 선택될 수 있다.

● 인터넷 브라우저 애플리케이션. 인터넷 브라우저 애플리케이션의 한 예에 있어서, 특정의 URL을 갖는 웹 페이지를 보는 요청 등과 같은 사용자로부터의 지시는 원격 제어기(2026)를 이용하여 입력되고, 이들은 모뎀 백 채널(4002)에 의해 애플리케이션 및 데이터 서버(4006)로 전송된다. 적절한 웹 페이지는 방송 센터로부터의 전송에 포함되고, 업 링크(2012), 트랜스폰더(2014) 및 다운링크(2016)를 통하여 수신기/디코더(2020)에 의하여 수신되어, 텔레비전 세트(2022)에 표시된다.

애플리케이션은 수신기/디코더(2020)의 메모리 위치에 저장되고 자원 파일로서 표시된다. 자원 파일은 그래픽 객체 설명 유닛 파일(graphic object description unit file), 가변 블록 유닛 파일, 지시 시퀀스 파일, 애플리케이션 파일 및 데이터 파일을 구비한다.

그래픽 객체 설명 유닛 파일은 스크린, 즉 애플리케이션의 사용자 기계 인터페이스(man-machine interface)를 설명한다. 가변블록 유닛 파일은 애플리케이션에 의해 취급된 데이터 구조를 설명한다. 지시 시퀀스 파일은 애플리케이션의 처리 동작을 설명한다. 애플리케이션 파일은 애플리케이션에 엔트리 포인트를 제공한다.

상기 방법으로 방법으로 구성된 애플리케이션은 아이콘 라이브러리 파일, 이미지 파일, 문자 폰트(font) 파일, 컬러 테이블 파일 및 ASCII 텍스트 파일 등의 데이터 파일을 사용할 수 있다. 대화식 애플리케이션은 입력 및/또는 출력을 유효하게 함으로써 온-라인 데이터를 얻을 수 있다.

엔진(4008)만은 그것이 설정된 시간에 필요로 하는 그 자원 파일을 그 메모리로 로드시킨다. 이 자원 파일은 그래픽 객체 설명 유닛 파일, 지시 시퀀스 파일 및 애플리케이션 파일로부터 관독되고; 가변블록 유닛 파일은 모듈을 로딩하기 위한 절차의 호출에 후속하여 메모리에 저장되고, 모듈을 로딩하지 않는 절차의 특정한 호출이 이루어질 때까지 거기에 잠긴(lock) 채로 남아있다.

도 3을 참조하면, 텔레쇼핑 모듈 등의 모듈(4010)은 자원 파일 및 데이터 세트이고, 그 세트는, 단일 애플리케이션 파일(4012)과; 결정되지 않은 수의 그래픽 객체 설명 유닛 파일(4014)과; 결정되지 않은 수의 가변블록 유닛 파일(4016)과; 결정되지 않은 수의 지시 시퀀스 파일(4018)과; 적합하게는 아이콘 라이브러리 파일, 이미지 파일, 문자 폰트(font) 파일, 컬러 테이블 파일 및 ASCII 텍스트 파일 등의 데이터 파일(4020)을 구비한다.

삭제

삭제

삭제

삭제

삭제

도5을 참고하면, 텔레쇼핑 모듈과 같이 모듈(4010)은 다음으로 이루어진 한 세트의 자원 파일(resource files)과 데이터이다:

단일 애플리케이션 파일(4012);

미결정된 수의 그래픽 목표물 설명 유닛 파일(4014);

미결정된 수의 가변 블록 유닛 파일(4016);

미결정된 수의 명령 시퀀스 파일(4018); 및

적절할 때, 아이콘 라이브러리 파일, 이미지 파일, 문자 폰트 파일, 컬러 테이블 파일 및 ASCII 텍스트 파일과 같은 데이터 파일(4020).

코드의 일부를 다운로드하는 개념과 더불어 모듈(4010)의 개념은 애플리케이션의 획기적인 발전을 허용한다. 작은 조각들은 상주한 소프트웨어나 방송용으로 단지 최종 사용자에게 의해 필요될 때 디코더 (2020)의 램상으로 전송되기 위하여 디코더 (2020)의 영속적인 플래시 메모리상으로 전송될 수 있다.

반송 신호로부터 모듈 (4010)을 전송하기 위해, 반송 신호에 액세스할 수 있는 디렉토리가 우선 다운로드된다. 이 디렉토리는 반송 신호로부터 다운로드될 수 있는 모듈(4010)의 명칭을 단순히 열거한다. 일단 이 디렉토리가 다운로드되면, 애플리케이션이 하나 이상의 모듈(4010)을 다운로드할 수 있게 된다. MPEG 흐름도상의 경우에 있어서, 디렉토리는 한 개의 단독 MPEG 테이블로 전송된다. 더욱이, 하나의 모듈(4010)은 한 개의 단독 MPEG 테이블로 전송된다. MPEG 튜너 (4028)로 전송된 모듈의 경우에 있어서, 긴 헤더와 CRC 코드를 갖는 긴 MPEG-2 형식이 사용된다. 또한 보다 짧은 헤더와, CRC가 없는 "쇼트" MPEG-2 포맷이 사용되는 것을 제외하고, 이는 다섯 개의 다른 인터페이스 (직렬 인터페이스 (4030), 병렬 인터페이스 (4032), 모뎀 (4034) 와 두 개의 카드 관독 장치(4036))를 갖는 경우이다.

특히 도 6을 참조하면, MPEG-2 비트스트림은 0의 패킷 식별("PID")을 갖는 프로그램 접근 테이블("PAT")를 포함한다. 상기 PAT는 다수의 프로그램들의 프로그램 맵 테이블들("PATs")의 PID에 대한 기준(reference)를 포함한다. 각각의 PMT는 프로그램용 비디오 MPEG 테이블(16)과 오디오 MPEG 테이블(14)의 스트림의 PID에 대한 기준을 포함한다. 0의 PID를 갖는 프로그램 접근 테이블(10)인 패킷은 모든 MPEG 접근을 위한 진입점(entry point)을 제공한다.

애플리케이션들과 이들의 데이터를 다운로드하기 위해서, 두가지 새로운 스트림 형태들이 정의되며, 적절한 PMT는 또한 MPEG 테이블들 18(또는 이것들의 구역들)과 데이터 MPEG 테이블들 20(또는 이것들의 구역들) 애플리케이션의 스트림의 PID에 대한 기준을 포함한다.

도 7을 참조하여, 애플리케이션(22)을 다운로드하기 위해서, 애플리케이션은 MPEG 테이블에 의해 각각 형성되는 모듈 (24)들로 분할되고, 이들중 일부는 단일 구역(18)으로 구성되고, 나머지는 다수의 구역(18)에 의해 형성된다.

전형적인 섹션(18)은 1 바이트의 테이블 식별("TID":28)을 포함하는 헤더(26), 테이블에서의 그 섹션의 섹션 번호(30), 테이블에서의 섹션의 합계(32) 및 2 바이트 TID 확장자(34)를 가진다. 또한, 각 섹션은 데이터 부분(36)과 CRC(38)를 포함한다. 특정 모듈/테이블(24)에 대해, 테이블(24)을 이루는 섹션(18) 전체는 동일 TID(28)와 동일 TID 확장자(34)를 갖는다. 특정 애플리케이션(22)에 대해, 애플리케이션(22)을 이루는 테이블(24) 전체는 동일 TID(28)를 갖지만, 각각 상이한 TID 확장자를 갖는다.

각각의 애플리케이션(22)에 대해, 디렉토리로서 사용되는 단독의 각 MPEG 테이블(24)이 있으며, 도 8에서 보다 상세하게 도시된다. 디렉토리 테이블(40)은 헤더(26), 디렉토리부(42), 키 식별자(44), 암호화된 서명(46) 및 CRC(38)를 포함한다.

상기로부터, 디렉토리 테이블(40)은 자신의 헤더(26)에 애플리케이션을 구성하는 다른 모듈들/테이블(24)로서 동일 TID(28)를 갖는 것이 이해될 것이다. 그러나, 디렉토리 테이블은 소정의 0의 TID 확장자(34)를 갖고, 나머지 모듈(24) 전체는 0이 아닌 TID 확장자들을 갖는다. 또한, 헤더는 디렉토리 테이블(40)용의 버전 번호(48)를 포함한다. 애플리케이션(22)을 구성하는 나머지 모듈/테이블(24)의 각각에 대해, 디렉토리부(42)는 그 모듈의 명칭(50), 그 모듈에 대한 TID 확장자(34), 및 그 모듈의 서명(52)을 포함한다. 나머지 모듈/테이블(24) 각각에 대해, 디렉토리부(42)는 또한 그 모듈의 길이와 모듈의 버전 번호를 포함할 수 있다.

삭제

다시 도 6을 참조하면, 작동시, PAT(10), PMT(12) 및 애플리케이션과 데이터 스트림 구성요소(18, 20)는 주기적으로 전달되며, 필요시 업데이트된다. 전송되는 각 애플리케이션은 각각 소정의 TID(28)를 갖는다. 애플리케이션을 다운로드하기 위해, 적합한 TID와 0의 TID 확장자를 갖는 MPEG 테이블은 수신기/디코더(2020)로 다운로드된다. 따라서, 이것은 요구된 애플리케이션에 대한 디렉토리 테이블(40)이다. 그후, 디렉토리의 데이터는 요구된 애플리케이션을 구성하는 모듈 테이블의 TID 확장자(34)를 결정하도록 수신기/디코더(2020)에 의해 처리되고, 디렉토리 테이블로서 동일 TID를 갖는 어떠한 요구된 모듈 테이블과 디렉토리로부터 결정된 TID 확장자가 다운로드될 수 있다.

수신기/디코더(2020)는 디렉토리 테이블의 어떠한 갱신에 대한 디렉토리 테이블들을 검사하기 위해 배열된다. 이것은 예를 들어, 30 초, 1 분 또는 5분마다 주기적으로 다시 디렉토리 테이블을 다운로드함으로써 행해질 수 있고, 이전에 다운로드된 디렉토리 테이블과 새롭게 다운로드된 디렉토리 테이블의 버전 번호를 비교할 수 있다. 새롭게 다운로드된 버전 번호가 보다 나중에 다운로드되면, 모듈은 이전 디렉토리 테이블 또는 최근의 버전 번호인 어떤 이와 같은 모델들과 연관된 모듈이 설치되지 않고, 최근의 모듈이 다운로드되어 설치된다. 대안적인 배열에 있어서, 수신 비트스트림은 TID, 애플리케이션의 TID를 설정하는 값을 갖는 TID 확장자와 버전 번호, 0의 TID 확장자와 현재 다운로드된 디렉토리의 버전 번호보다 하나 큰 버전 번호에 대응하는 마스크를 사용하여 필터된다. 따라서, 버전 번호의 증가가 검출될 수 있고, 일단 검출되면, 상기에서 설명된 바와 같이 디렉토리가 다운로드되고, 애플리케이션이 업데이트된다. 더욱이, 이와 같은 필터링(filtering)의 설명은 출원중인 출원서(대리인의 참조 번호 PDC/ASB/19716)에 포함된다. 애플리케이션이 전송되면, 다음 버전 번호를 갖는 빈 디렉토리는 디렉토리에서 어떠한 모듈들의 리스트 없이 전송된다. 이와 같은 빈 디렉토리의 수신에 응답하여, 수신기/디코더(2020)는 애플리케이션을 설치하지 않도록 프로그램된다.

애플리케이션 테이블에 대한 서명과 암호화의 사용이 하기에서 보다 상세하게 설명된다.

상기에서 설명된 바와 같이, 디렉토리 테이블(40)에서 각 모듈에 대한 엔트리(entry)는 모듈 서명을 포함한다. 모듈 서명은 각각의 모듈 테이블의 데이터를 처리하는 알려진 MD5 서명을 이용하여 생성된다.

더욱이, 디렉토리 테이블(40)은 암호화된 서명(46)을 포함하고, 도 9를 참조하여 설명되는 방법으로 생성된다. 데이터의 64 바이트들의 블록(54)이 만들어진다. 제 1 바이트(56)는 0이다. 다음의 3 바이트(58)는 더미(dummy) 또는 임의의 데이터를 포함한다. 다음의 8 바이트(60)는 애플리케이션 확인 비트맵을 제공하고, 이는 하기에서 보다 설명될 것이다. 마지막 4 바이트(62)는 남겨지게 된다. 나머지 32 바이트들은 애플리케이션 확인 비트맵에 후속하는 제 1 바이트 이후에 0 바이트와 31 바이트 사이의 오프셋(offset)에서 시작되는 16 바이트의 서명(64)을 포함한다. 더미 데이터(66)은 애플리케이션 확인 비트맵(60)과 서명(64) 사이, 및/또는 서명(64)과 남겨진 바이트(62) 사이에 삽입된다. 서명(64)은 전체 디렉토리(42)의 처리를 디렉토리 테이블(40)에서 발생시키는 알려진 MD5 서명을 이용하여 만들어진다. 그후, 블록(54)은 암호화된 서명 및 애플리케이션 확인 비트맵(46)을 만들기 위해 알려진 암호화 처리 및 특정 개인키를 사용하여 암호화된다. 이 데이터 블록(46)은 디렉토리 테이블(40)에 포함되며, 블록을 암호화하는데 사용되는 개인 키의 1 바이트 식별자는 키 식별자(44)로서 디렉토리 테이블(40)에 포함된다.

삭제

애플리케이션과 애플리케이션의 전송의 발생을 요약하기 위해, 다음과 같은 단계들이 포함된다:

- 애플리케이션을 다수의 모듈로서 생성하는 단계;
- 애플리케이션에 대한 소정의 TID(28)를 표시하는 단계;
- 명칭 및 0이 아닌 TID 확장자(34)를 모듈에 할당하는 단계;
- 각 모듈을 MPEG 테이블(24) 또는 MPEG 테이블의 섹션(18)으로서 포맷하는 단계;
- 각 모듈의 MD5 서명을 생성하는 단계;
- 디렉토리(42)를 생성하는 단계;
- 디렉토리에 대한 MD5 서명을 생성하는 단계;
- 애플리케이션 확인 비트(60)를 선택하는 단계;
- 오프셋을 선택하는 단계;
- 블록(54)을 생성하는 단계;

- 선택된 개인키를 갖는 암호화를 이용하여 블록(54)을 암호화하는 단계;
- 디렉토리 MPEG 테이블(40)을 할당된 TID(28), 0의 TID 확장자, 디렉토리(42), 개인키의 식별자(44) 및 암호화된 서명(46)으로 생성하는 단계;
- 디렉토리 테이블(40)과 모듈 테이블(24) 또는 섹션(18)을 전송하는 단계.

애플리케이션을 다운로드하는 동안 서명과 복호화를 처리하는 수신기/디코더(2020)의 동작이 하기에 설명될 것이다. 도 10을 참조하면, 수신기/디코더(2020)는 EEPROM(68), ROM(70) 및 RAM(72)을 포함한다. EEPROM(68)은 가상 계산기에 의해 사용되는 보호 구역(74)을 포함하며, 여기서 가상 계산기(그리고 정상적인 애플리케이션이 아닌)만이 기록할 수 있다. 보호 구역(74)은 16 혹은 256 비트의 키 확인 비트맵(76, 64)을 포함하고, 64비트의 애플리케이션 확인 비트맵(78) 및 32비트의 오프셋 비트맵(80)을 포함한다. 하나의 실시예에 있어서, RAM(70)은 16비트의 키 확인 비트맵이 이용되는 경우에 16개의 공개키(82)를 포함하고, 또 다른 실시예에 있어서, 256비트의 키 확인 비트맵이 이용되는 경우에 256개의 공개키를 포함한다. 공개키는 ROM(70)의 물리적인 위치에 의해 식별되거나, 록업 테이블에 대안적으로 포함되어 질 수 있고, 특정 키 식별자는 대응 공개키를 산출할 것이다. RAM(72)은 임시키(temporary key:84)를 저장하는데 사용될 수 있다.

상기에서 설명된 바와 같이, 애플리케이션이 다운로드될 때, 우선 그 애플리케이션에 대한 소정의 TID를 갖는 디렉토리(40)의 TID 확장자가 다운로드된다. 그 후, 키 식별자(44)가 디렉토리 테이블로부터 추출되고, 검사는 추출된 키 식별자(44)에 해당되는 비트가 설정되는 보호 메모리(74)에서 키 확인 비트맵(76)으로 구성된다. 만약 그렇지 않으면, 추가 애플리케이션의 다운로드가 중지된다. 그러나, 적합한 키가 설정되면, 공개키(82)는 추출된 키 식별자(44)에 해당되는 ROM(70)으로부터 선택된다. 그 후, 선택된 공개키 및 알려진 복호화 처리가 블록(54)을 만들기 위해 디렉토리 테이블(40)에서 암호화된 블록(46)을 복호화하는데 사용된다. 그 후, 애플리케이션 확인 비트맵(60)은 복호화된 블록(54)으로부터 추출되고, 보호 메모리(74)에 저장된 애플리케이션 확인 비트맵(78)으로 논리곱된다. 논리곱 연산의 결과가 0이면, 추가 애플리케이션의 다운로드가 중지된다. 그러나, 만약 논리곱 연산의 결과가 0이 아니면, 보호 메모리(74)의 오프셋 비트맵(80)에 포함된 오프셋이 조사되거나, 하나 이상의 오프셋 비트가 설정되면, 각 오프셋 비트는 차례대로 조사되고, 데이터의 16 바이트가 애플리케이션 확인 비트맵(60) 이후의 제 1 바이트로부터의 조사 오프셋으로 시작되는 복호화된 블록(54)으로부터 추출된다. 상기 또는 각 조사 오프셋에 대해, 16 바이트가 디렉토리 테이블(40)과 함께 전송된 서명으로서 처리된다. 디렉토리 테이블(40)의 디렉토리(42)에서의 전체 서명은 알려진 MD5 처리를 이용하여 계산되고, 계산된 서명은 블록(54)으로부터 추출된 서명과 비교된다. 상기 혹은 각 오프셋에 대한 2개의 서명이 일치하지 않으면, 추가 애플리케이션의 다운로드가 중지된다. 그러나, 서명중 하나가 일치되면, 디렉토리(42)에 지정된 모듈의 다운로드가 처리될 수 있다. 상기에서 설명된 바와 같이, 특정 모듈을 다운로드하기 위해, 모듈에 대한 TID 확장자는 디렉토리(42)로부터 획득되고, 디렉토리 테이블로서 동일한 TID와 획득된 TID 확장자를 갖는 MPEG 테이블(24) 또는 섹션(18)이 다운로드된다. 일단 모듈 MPEG 테이블이 다운로드되면, 수신기/디코더(2020)는 알려진 MD5 처리를 이용하여 다운로드된 테이블의 서명을 계산하고, 그 후, 계산된 서명과 디렉토리 엔트리에 포함된 서명을 비교한다. 서명이 일치하면 모듈이 채택되지만, 일치하지 않으면 모듈은 거절된다.

삭제

따라서, 애플리케이션의 모듈 전체는 상기에서 기술된 방법으로 다운로드될 수 있어, 애플리케이션은 수신기/디코더(2020)에 의해 동작될 수 있다.

수신기/디코더(2020)를 설치하고 수신기/디코더(2020)의 설정을 변경하는데 사용된 일부 측면이 일반적으로 이용되는 다운로드 처리의 측면을 기술하여 설명될 것이다.

수신기/디코더(2020)는 보호 메모리 영역(74)이 변경될 수 있도록 프로그램되지만, 키 식별자중 특정 하나, 예를 들어 키(15)를 사용하여, 그리고 애플리케이션 확인 비트맵(60) 이후의 제 1 바이트로부터의 0바이트의 오프셋으로 다운로드되는 애플리케이션에 의해서만이다. 보호 메모리(74)는 예를 들어, 동일한 공개키를 사용하는 2명의 운영자가 상이한 공개키를 사용하고자 하는 것을 결정하거나, 대응 공개키가 키 확인 비트맵(76)에서 무효로서 표시되는 경우에 개인키의 내용(content)이 알려지면, 변경될 필요가 있을 수 있다.

수신기/디코더(2020)가 배치될 수 있어, 키들중 하나 예를 들어, 키(15)는 키가 키 확인 비트맵(76)에서 비트를 요구하지 않는 경우에 항상 이용 가능하다. 따라서, 그 비트는 또 다른 목적으로 사용될 수 있다. 특히, 키(15)를 사용하여 인증되는 애플리케이션은 수신기/디코더(2020)가 임시키(84)를 RAM(72)으로 로드되도록 프로그램되지만, 직렬 인터페이스(4030), 병렬 인터페이스(4032) 또는 2개의 카드 관독 장치(4036)중 하나를 통해서만인 경우에, 그 특정 비트를 1로 설정되도록 배열될 수 있다. 이 설비는 예를 들어, 임시키를 수신기/디코더(2020)로 로드될 수 있도록 사용하는 애플리케이션이 제공될 수는 수신기/디코더(2020)의 제조업자에 의해 사용될 수 있어, 수신기/디코더(2020)가 검사될 수 있다.

상기에서 설명된 암호화 및 서명 장치는 다수의 중요한 측면을 제공한다. 특히 다음과 같은 측면을 제공한다:

삭제

- 애플리케이션은 단지 수신기/디코더(2020)가 다운로드된 디렉토리 테이블에서 키 식별자(44)에 해당되는 수신기/디코더의 메모리에 저장된 적합한 공개키를 가지면, 다운로드될 수 있다;
- 키중 하나를 제외한 전체 키에 대해, 애플리케이션은 단지 수신기/디코더(2020)의 메모리에서의 키 확인 비트맵(76)이 그 키를 이용할 수 있도록 설정되면, 특정 키를 사용하여 다운로드될 수 있다;

- 애플리케이션은 단지 수신기/디코더(2020)의 메모리에 저장된 오프셋 비트맵(80)에서의 설정 비트가 디렉토리 테이블을 생성하는데 사용된 오프셋과 일치하면, 다운로드될 수 있다;
- 애플리케이션은 수신기/디코더(2020)의 메모리에서의 애플리케이션 확인 비트맵(78)이 적합하게 애플리케이션을 다운로드할 수 있도록 설정되면, 다운로드될 수 있다;
- 애플리케이션은 단지 그 서명이 최초로 생성된 후에 변조되지 않으면, 다운로드될 수 있다.
- 애플리케이션의 각 모듈은 단지 수신기/디코더(2020)의 메모리에서의 애플리케이션 확인 비트맵(78)이 애플리케이션을 다운로드할 수 있도록 적합하게 설정되면 다운로드될 수 있다.
- 하나의 암호화 동작만이 몇 개의 MPEG 테이블로 구성되는 애플리케이션임에도 불구하고 다운로드동안 애플리케이션을 준비하는데 요구되고, 하나의 복호화 동작만이 완전한 애플리케이션을 다운로드하도록 수신기/디코더(2020)에 요구된다; ● 다중 키가 이용될 수 있어, 상이한 서비스 제공업자들이 상이한 개인키를 가질 수 있다;

삭제

- 임시 키는 예들 들어 제조업자에 의해 공장장에 의해서 검사 목적으로 사용될 수 있다.

산업상 이용 가능성

본 발명은 예로써 상술되었고, 상세한 내용의 변경은 본 발명의 범위내에서 이루어질 수 있다.

상세한 설명, (적합한) 청구범위 및 도면에 개시된 각 특징은 독립적으로 또는 적합한 결합으로 구비될 수 있다.

상기에 언급된 바람직한 실시예에 있어서, 본 발명의 소정의 특징은 컴퓨터 소프트웨어를 사용해서 수행되었다. 그러나, 상기 특징중 일부가 하드웨어를 사용해서 수행되는 것은 당업자에게는 물론 명백하다. 또한, 하드웨어, 컴퓨터 소프트웨어 등에 의해 수행된 기능이 전기 및 유사 신호를 사용해서 수행된다.

참고문헌은 같은 출원일을 갖는 동시계류중인 출원이고 그 출원의 명칭은 신호 발생 및 방송(Signal Generation and Broadcasting)(대리인 문서번호 PC/ASB/19707), 암호화된 방송 신호의 수신기와 사용하는 스마트카드 및 수신기(Smartcard for use with a Receiver of Encrypted Broadcast Signal and Receiver)(대리인 문서번호 PC/ASB/19708), 방송 및 수신 시스템 및 그것을 위한 조건부 액세스 시스템(Broadcast and Reception System and Conditional Access System therefor)(대리인 문서번호 PC/ASB/19710), 송신기로부터 수신기/디코더를 경유해서 컴퓨터로의 컴퓨터 파일의 다운로드(Downloading a Computer File from a Transmitter via a Receiver/Decoder to Computer)(대리인 문서번호 PC/ASB/19711), 텔레비전 프로그램 및 다른 데이터의 송신 및 수신(Transmission and Reception of Television Programmes and Other Data)(대리인 문서번호 PC/ASB/19712), 다운로드 데이터(Downloading Data)(대리인 문서번호 PC/ASB/19713), 컴퓨터 메모리 구조(Computer Memory Organisation)(대리인 문서번호 PC/ASB/19714), 텔레비전 또는 라디오 제어 시스템 개발(Television or Radio Control System Development)(대리인 문서번호 PC/ASB/19715), 송신된 데이터 스트림으로부터 인출하는 데이터 섹션(Extracting Data Sections from a Transmitted Data Stream)(대리인 문서번호 PC/ASB/19716), 액세스 제어시스템(Access Control System)(대리인 문서번호 PC/ASB/19717), 데이터 처리시스템(Data Processing System)(대리인 문서 번호 PC/ASB/19718), 방송 및 수신 시스템 및 수신기/디코더 및 그것을 위한 원격 제어기(대리인 문서 번호 PC/ASB/19720)이다. 상기 서류의 개시는 참고로 본원에서 결부된다. 출원들의 리스트는 본 발명을 포함한다.

(57) 청구의 범위

청구항 1.
삭제

청구항 2.
삭제

청구항 3.
삭제

청구항 4.
삭제

청구항 5.
삭제

청구항 6.
삭제

청구항 7.
삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

청구항 18.
삭제

청구항 19.
삭제

청구항 20.
삭제

청구항 21.
삭제

청구항 22.

데이터를 MPEG 수신기/디코더로 다운로드하는 방법으로서,

다운로딩되는 상기 데이터에 대한 서명을 생성하는 단계;

상기 서명과, 상기 데이터 블록의 개시와 상기 서명의 개시 사이에 선택된 오프셋을 갖는 데이터 블록에서의 다른 데이터를 포함하는 단계;

개인키를 사용하여 상기 데이터 블록을 암호화하는 단계;

다운로딩되는 상기 데이터와 상기 암호화된 데이터 블록을 MPEG 테이블로서 포맷하는 단계;

MPEG 테이블을 전송하는 단계; 및

상기 수신기/디코더에서

상기 MPEG 테이블을 수신하는 단계;

상기 개인키에 해당되는 공개키를 사용하여 상기 수신된 MPEG 테이블에서 상기 암호화된 데이터 블록을 복호화하는 단계;

상기 수신기/디코더의 메모리의 보호 영역에 적어도 하나의 저장된 오프셋을 조사하는 단계;

상기 복호화된 데이터 블록의 개시로부터 상기 적어도 하나의 조사 오프셋을 사용하여 상기 복호화된 데이터 블록으로부터 상기 서명을 추출하는 단계;

상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하는 단계; 및

상기 복호화된 데이터 블록으로부터 추출된 상기 서명과 상기 수신 데이터용 수신기/디코더에서 생성된 상기 서명과 비교하는 단계를 포함하는 방법.

청구항 23.

제 22 항에 있어서, 상기 메모리의 보호 영역은 적어도 2 개의 이와 같은 저장된 오프셋을 가지며, 상기 비교 단계에서 상기 추출된 서명과 상기 생성된 서명이 일치하지 않으면, 상기 저장된 오프셋중 또 다른 하나를 사용하는 상기 조사, 추출 및 비교 단계를 반복하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 24.

제 22 항 또는 제 23 항에 있어서, 데이터 블록에서 상기 다른 데이터의 적어도 일부는 더미 또는 임의 데이터인 것을 특징으로 하는 방법.

청구항 25.

제 22 항에 있어서, 상기 데이터는 복수의 데이터 모듈들로서 다운로드되며,

다운로드되는 데이터의 각 모듈에 대한 모듈 서명을 생성하는 단계;

상기 데이터 모듈을 개개의 모듈 MPEG 테이블로서 포맷하는 단계;

각 모듈 MPEG 테이블의 식별자와 상기 개개의 서명을 포함하고, 제 22 항의 서명 발생 단계의 주체인 렉토리를 생성하는 단계; 및

상기 수신기/디코더에서

상기 수신된 모듈 MPEG 테이블에 상기 각 모듈에 대한 개개의 모듈 서명을 생성하는 단계;

상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명과 상기 수신기/디코더에서 생성된 상기 개개의 모듈 서명을 비교하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 26.

삭제

청구항 27.

제 26 항에 있어서, 모듈 서명 비교 단계에서 상기 수신된 디렉토리 MPEG 테이블에서의 모듈 서명과 그 모듈용 수신기/디코더에서 발생된 개개의 모듈 서명이 서로 일치하지 않으면, 상기 데이터의 이와 같은 모듈의 다운로드를 금지 또는 중지하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 28.

제 22 항 또는 제 25 항에 있어서, 상기 비교 단계에서 상기 또는 각 복호화된 서명과 상기 생성된 서명이 서로 일치하지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하는 단계를 더 포함하는 것을 특징으로 하는 방법.

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

청구항 38.
삭제

청구항 39.
삭제

청구항 40.
삭제

청구항 41.
삭제

청구항 42.
삭제

청구항 43.
삭제

청구항 44.
삭제

청구항 45.
삭제

청구항 46.
삭제

청구항 47.

제 22항의 방법의 일부를 수행하는데 사용하기 위한 MPEG 수신기/디코더로서,

이와 같은 MPEG 테이블들을 수신하기 위한 수단;

공개키와 상기 공개키에 대한 식별자를 저장하기 위한 수단;

적어도 하나의 오프셋을 저장하기 위한 메모리의 보호 영역;

상기 개인키에 해당되는 상기 저장된 공개키를 사용하여 이와 같은 수신된 MPEG 테이블에서 상기 암호화된 데이터 블록을 복호화하고, 상기 복호화된 데이터 블록의 개시로부터 상기 조사 오프셋을 사용하여 상기 서명을 상기 복호화된 데이터 블록으로부터 추출하고, 상기 수신된 MPEG 테이블에서 상기 데이터에 대한 서명을 생성하며, 상기 복호화된 데이터 블록으로부터 추출된 상기 서명과 상기 수신된 데이터에 대한 상기 수신기/디코더에서 생성된 상기 서명을 비교하도록 프로그램되는 처리 수단을 포함하는 MPEG 수신기/디코더.

청구항 48.

제 47항에 있어서, 적어도 2개의 이와 같은 오프셋은 상기 메모리의 보호 영역에 저장되며, 상기 추출된 신호와 상기 생성된 신호가 서로 일치하지 않으면, 상기 처리 수단은 상기 저장된 오프셋중 또 다른 하나를 사용하여 검색하고, 추출하며 비교하는 것을 반복하도록 동작될 수 있는 것을 특징으로 하는 수신기/디코더.

청구항 49.

제 48 항에 있어서, 상기 오프셋을 저장하기 위한 상기 메모리는 재기록 가능한 비휘성 메모리로 제공되는 것을 특징으로 하는 수신기/디코더.

청구항 50.

제 25항에 청구된 방법에 사용하기 위한 제 47 내지 49 항중 어느 항에 있어서, 상기 처리 수단은 상기 수신된 모듈 MPEG 테이블에서 상기 각 모듈에 대한 개개의 모듈 서명을 생성하고, 상기 수신된 디렉토리 MPEG 테이블에서의 각 모듈 서명을 상기 수신기/디코더에 의해 생성된 상기 개개의 모듈 서명과 비교하도록 프로그램되는 것을 특징으로 수신기/디코더.

청구항 51.

삭제

청구항 52.

제 50 항에 있어서, 상기 처리 수단은 상기 수신된 디렉토리 MPEG 테이블에서의 모듈 서명과 그 모듈에 대한 수신기/디코더에서 생성된 상기 개개의 모듈 서명이 서로 일치하지 않으면, 상기 데이터의 이와 같은 모듈의 다운로드를 금지 또는 중지하도록 프로그램되는 것을 특징으로 하는 수신기/디코더.

청구항 53.

제 47 내지 49 항중의 어느 항에 있어서, 상기 처리 수단은 상기 또는 각 복호화된 서명과 상기 생성된 서명이 서로 일치하지 않으면, 상기 데이터의 다운로드를 금지 또는 중지하도록 프로그램되는 것을 특징으로 하는 수신기/디코더.

청구항 54.

삭제

청구항 55.

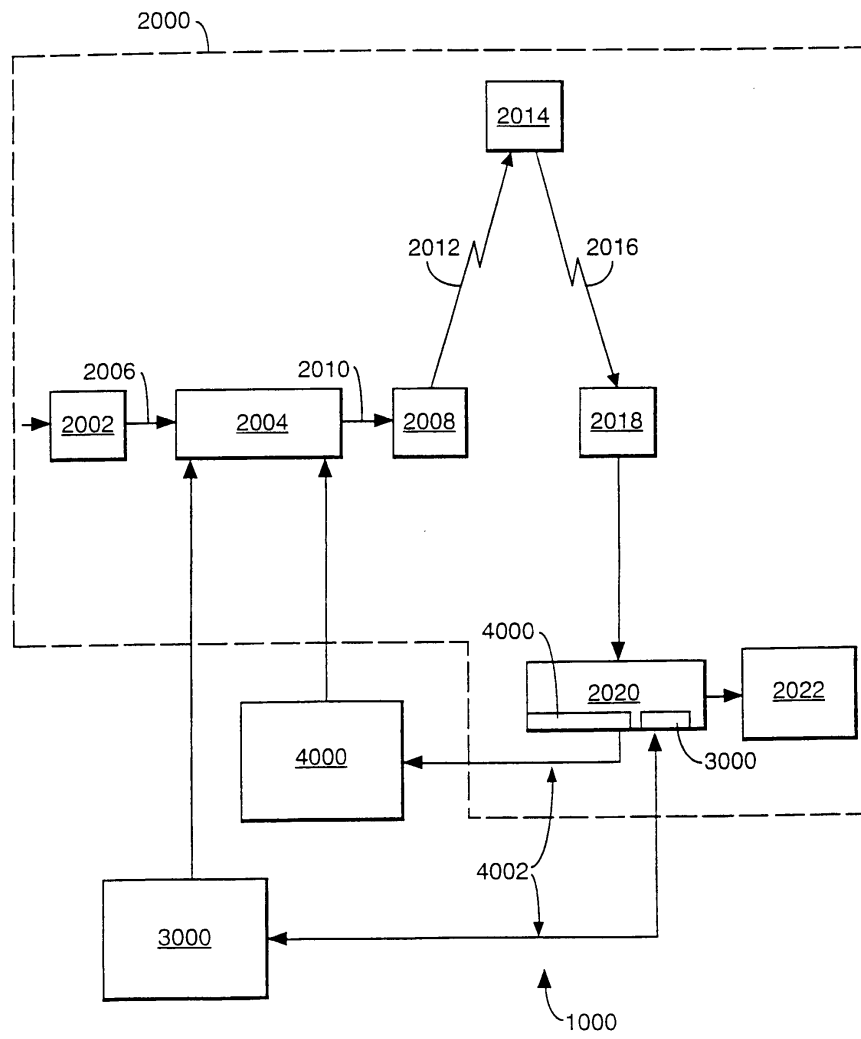
삭제

청구항 56.

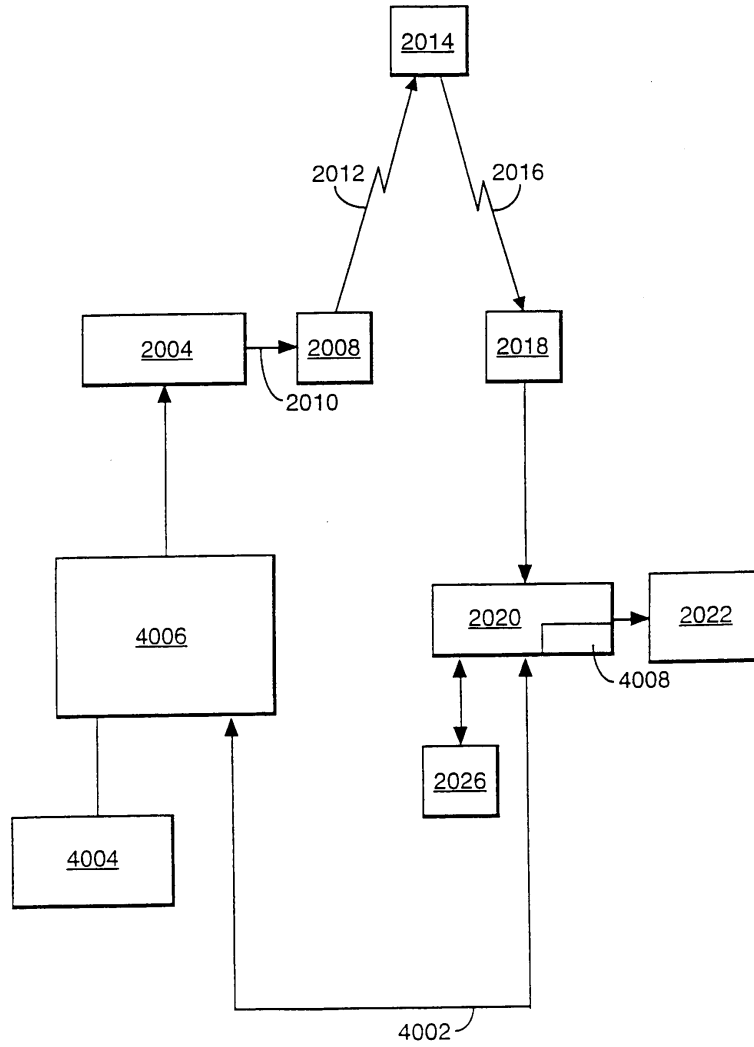
삭제

도면

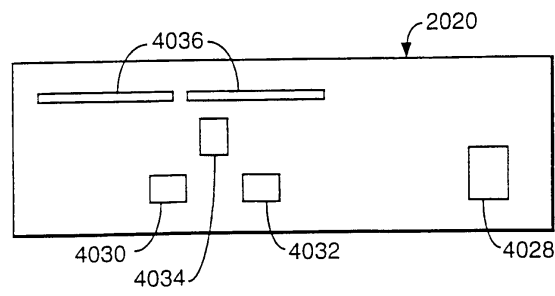
도면1



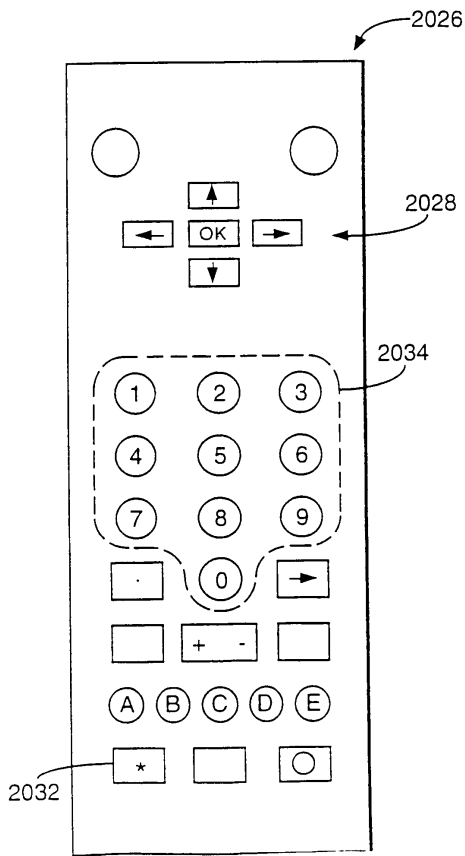
도면2



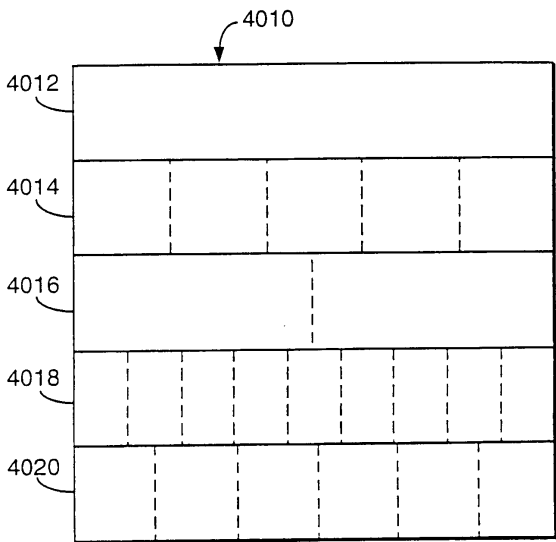
도면3



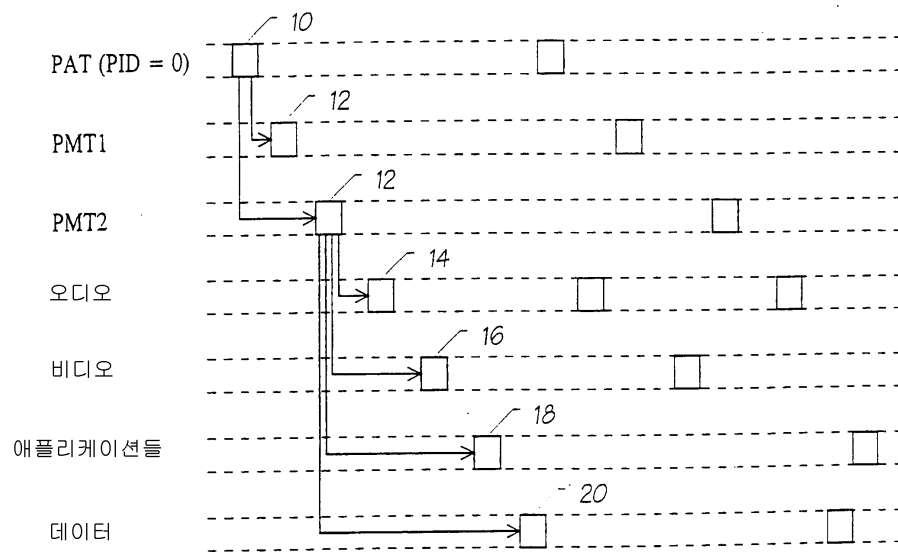
도면4



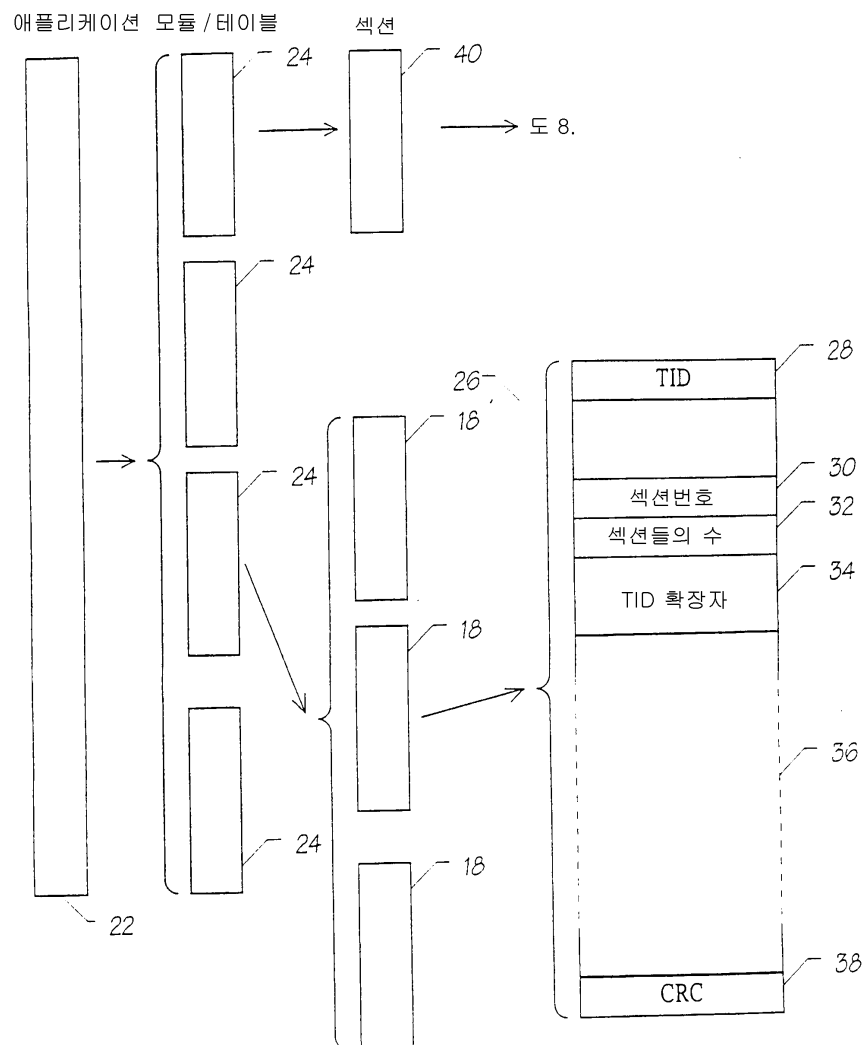
도면5



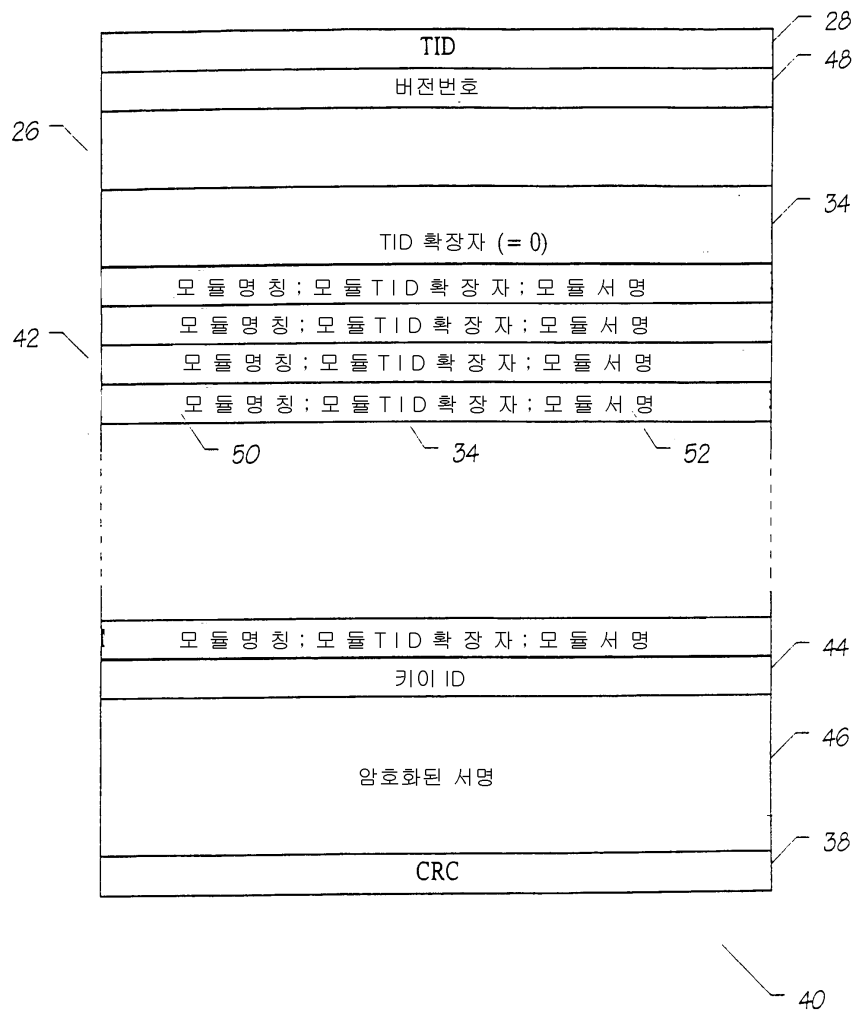
도면6



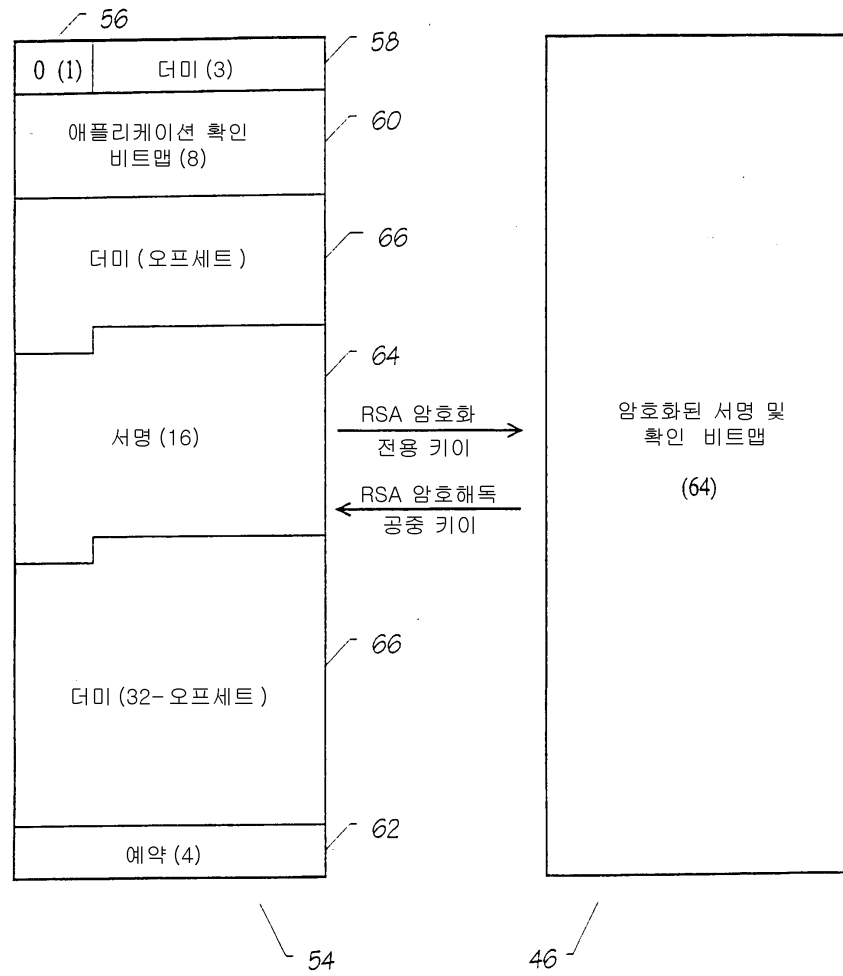
도면7



도면8



도면9



도면10

