(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년10월20일
(11) 등록번호 10-0989015
(24) 등록일자 2010년10월13일

(51) Int. Cl.
H04N 7/167 (2006.01) *H04N 7/24* (2006.01)
(21) 출원번호 10-2009-7022281(분할)
(22) 출원일자(국제출원일자) 2002년12월13일
심사청구일자 2009년11월20일
(85) 번역문제출일자 2009년10월23일
(65) 공개번호 10-2009-0115900
(43) 공개일자 2009년11월09일
(62) 원출원 특허 10-2009-7003356
원출원일자(국제출원일자) 2002년12월13일
심사청구일자 2009년03월20일
(86) 국제출원번호 PCT/US2002/040045
(87) 국제공개번호 WO 2003/065724
국제공개일자 2003년08월07일
(30) 우선권주장
10/037,498 2002년01월02일 미국(US)
2,406,329 2002년10월01일 캐나다(CA)
(56) 선행기술조사문헌
Computer and Graphics, Vol.22. No.4, 1998., L. Qiao et al., "Comparison of MPEG Encryption Algoritms", pp.437-448
Electronics & Communication Engineering Journal, Vol.9. Issue 1, 1997.02., David J. Cutts, "DVB Conditional Access", pp.21-27
전체 청구항 수 : 총 5 항

(73) 특허권자
소니 일렉트로닉스 인코포레이티드
미국, 뉴저지 07656, 파크 리지, 원 소니 드라이브
(72) 발명자
운거, 로버트, 알란
미국 92019 캘리포니아주 엘 카존 비스타 허모사 웨이 2072
캔들로어, 브란트, 엘.
미국 92029-6502 캘리포니아주 에스콘디도 쿠아일 글렌 웨이 10124
페드로우, 레오, 엠., 주니어
미국 92065 캘리포니아주 라모나 가르잔 레인 17193
(74) 대리인
주성민, 이중희, 백만기

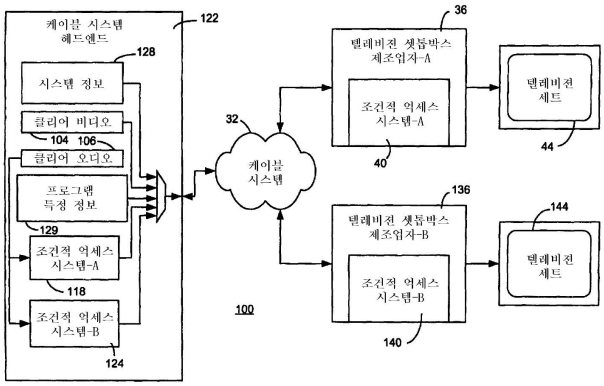
심사관 : 조남신

(54) 부분적으로 암호화된 정보의 암호해독 및 디코딩

(57) 요 약

TV 프로그램(100)의 멀티플 암호화를 위한 암호화 배열이 개시된다. 본 발명의 실시예에 따른 시스템은 텔레비젼 프로그램의 전체 표현에 요구되는 일부의 데이터(118,124)만을 멀티플 암호화하여 복수 제조업자들의 셋톱박스에 연관된 복수의 CA 암호화 시스템이 하나의 시스템에 공존할 수 있도록 한다. 단지 일부 프로그램(188,124)만을 암호화함으로써 모든 프로그램 데이타의 멀티플 암호화에 비해 상당히 적은 대역폭이 소모되며, 따라서 동일 대역폭에 보다 많은 프로그램을 운반하는 한편 복수의 CA 시스템(36,136)이 하나의 케이블 TV 시스템에 공존할 수 있도록 한다.

대 표 도



특허청구의 범위

청구항 1

부분적으로 암호화된 디지털 비디오 콘텐트를 디코딩하는 방법에 있어서,

암호화되지 않은 데이터, 제1 암호화 방식으로 암호화된 제1 데이터 및 제2 암호화 방식으로 암호화된 제2 데이터를 포함하는 부분적으로 암호화된 디지털 비디오 콘텐트 - 상기 제1 데이터 및 제2 데이터는 암호화되지 않았을 때에 동일함 - 를 수신하는 단계;

상기 암호화된 제2 데이터를 암호해독하는 단계;

상기 암호화되지 않은 데이터 및 상기 암호해독된 제2 데이터를 디코딩하여 상기 부분적으로 암호화된 디지털 비디오 콘텐트를 디코딩하는 단계;

상기 암호화되지 않은 데이터 및 상기 암호해독된 제2 데이터를 포함하는 디코딩된 디지털 비디오 콘텐트를 출력하는 단계; 및

상기 콘텐트의 1차 패킷 식별자(PID)와 상기 콘텐트의 2차 PID를 식별하는 메시지를 수신하는 단계를 포함하며,

상기 1차 PID는 상기 암호화되지 않은 데이터 및 상기 제1 데이터 중 적어도 하나를 식별하고, 상기 2차 PID는 상기 제2 데이터를 식별하고,

상기 암호해독하는 단계는 상기 2차 PID를 갖는 패킷을 암호해독하는 단계를 포함하는 디코딩 방법.

청구항 2

제1항에 있어서, 상기 수신, 암호해독 및 디코딩 단계가 TV 장치에서 수행되는 디코딩 방법.

청구항 3

제2항에 있어서, 상기 TV 장치는 TV 셋톱박스를 구비하는 디코딩 방법.

청구항 4

부분적으로 암호화된 콘텐트를 디코딩하는 방법에 있어서,

암호화되지 않은 콘텐트, 제1 암호화 방식하에서 암호화된 제1 콘텐트 및 제2 암호화 방식하에서 암호화된 제2 콘텐트를 포함하는 부분적으로 암호화된 콘텐트를 수신하는 단계;

암호화된 상기 제2 콘텐트를 암호해독하는 단계;

상기 암호화되지 않은 콘텐트 및 암호해독된 상기 제2 콘텐트를 디코딩하여 상기 부분적으로 암호화된 콘텐트를 디코딩하는 단계; 및

상기 콘텐트의 1차 패킷 식별자(PID)와 상기 콘텐트의 2차 PID를 식별하는 메시지를 수신하는 단계를 포함하고,

상기 1차 PID는 상기 암호화되지 않은 콘텐트 및 상기 제1 콘텐트 중 적어도 하나를 식별하고, 상기 2차 PID는 상기 제2 콘텐트를 식별하고,

상기 암호해독하는 단계는 상기 2차 PID를 갖는 패킷을 암호해독하는 단계를 포함하는 디코딩 방법.

청구항 5

삭제

청구항 6

TV 장치에 있어서,

복수의 암호화되지 않은 기본(elementary) 스트림 패킷 및 복수의 이중 암호화된 패킷의 쌍들 - 각 쌍의 상기 암호화된 패킷들 중 한 쪽의 패킷은 제1 암호화 알고리즘하에서 암호화되고, 각 쌍의 암호화된 패킷들 중 다른 쪽의 패킷은 제2 암호화 알고리즘하에서 암호화되며, TV 신호는 각 쌍의 암호화된 패킷들 중 한 쪽과암호화되

지 않은 패킷 둘 다에 의해 구성됨 - 을 수신하는 수신기;

상기 암호화된 패킷을 암호해독하는 암호해독기; 및

상기 암호화되지 않은 패킷과 상기 암호해독된 패킷을 디코딩하여 상기 TV 신호를 생성하는 디코더를 포함하고,

상기 수신기는, 상기 패킷의 1차 패킷 식별자(PID)와 상기 패킷의 2차 PID를 식별하는 메시지를 수신하고,

상기 1차 PID는 상기 암호화되지 않은 기본 스트림 패킷 및 상기 제1 암호화 알고리즘하에서 암호화된 패킷 중 적어도 하나를 식별하고, 상기 2차 PID는 상기 제2 암호화 알고리즘하에서 암호화된 패킷을 식별하고,

상기 암호해독기는 또한 상기 2차 PID를 갖는 패킷을 암호해독하는 TV 장치.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 일반적으로 암호화 시스템 분야에 관한 것이다. 특히, 본 발명은 디지털 텔레비젼 신호의 부분적 암호화 및 암호해독을 제공하는 시스템, 방법 및 장치에 관한 것이다.

[0002] 이 출원은 명칭이 "일부 콘텐트에 대한 비디오, 및 그외 콘텐트에 대한 오디오의 듀얼 캐리지와 비디오 및 오디오의 듀얼 캐리지를 클리어하게 전송함으로써 다수의 CA 제공자가 콘텐트 전달 시스템을 공동 사용가능하게 해주는 방법"으로 2001년 6월 6일 출원된 캔들로어 등의 U.S. 가특허출원 시리얼 번호 60/296,673 및 명칭이 "듀얼 캐리지에 대한 프로그램 콘텐트의 독립 선택 암호화"로서 2001년 7월 10일자 출원된 운거 등의 U.S. 가특허출원 시리얼 번호 60/304,241, 및 명칭이 "타임 슬라이스 기반으로 콘텐트를 부분적으로 스크램블링함으로써 다수의 CA 제공자가 콘텐트 전달 시스템을 공동 사용가능하게 해주는 방법"으로 2001년 7월 10일에 출원된 가특허출원 시리얼 번호 60/304/131, 및 명칭이 "텔레비젼 암호화 시스템"이고 서류 번호가 SNYR4646P인 2001년 10월 26일자로 출원된 캔들로어 등의 U.S. 가특허출원 시리얼 번호 60/343,710에 관한 것이다. 이들은 참조로서 본 명세서에 통합된다.

[0003] 이 출원은 명칭이 "주요 패킷 부분적 암호화"이고 서류번호 SNY-R4646.01인 언거 등의 특허출원, 시리얼 번호 10/038,217; 명칭이 "시분할 부분적 암호화"이고 서류 번호 SNY-R4646.02인 캔들로어 등의 특허출원, 시리얼 번호 10/038,032; 명칭이 "엘리멘터리 스트림 부분적 암호화이고 서류 번호 SNY-R4646.03인 캔들로어 등의 특허출원, 시리얼 번호 10/037,914; 및 명칭이 "부분적 암호화 및 PID 맵핑"이고 서류 번호 SNY-R4646.04인 운거 등의 특허출원, 시리얼 번호 10/037,499와 동시에 출원되었다. 이들 동시에 출원된 특허 출원은 본 명세서에 참조로 통합된다.

배 경 기 술

[0004] 텔레비젼은 엔터테인먼트 및 교육을 뷰어들에게 전달하는데 이용된다. 소스 재료(오디오, 비디오, 등)는 나중에 캐리어를 변조하는데 이용되는 결합 신호(combined signal)로 멀티플렉스된다. 이 캐리어는 일반적으로 채널로서 알려져 있다. (통상적인 채널은 하나의 아날로그 프로그램, 하나 이상의 고선명도(HD) 디지털 프로그램 또는 여러 개의(예를 들어 9개의) 표준 선명도 디지털 프로그램들을 운반할 수 있다. 지상 시스템에서 이들 채널들은 정부가 할당해 준 주파수들에 대응하며 공중에 배포된다. 이 프로그램은 공중으로부터 신호를 끌어당겨 복조기에 전달해주는 튜너를 가지고 있는 수신기에 전달되고, 이후 수신기는 비디오를 디스플레이에 오디오를 스피커에 제공한다. 케이블 시스템에서, 변조된 채널들은 케이블로 운반된다. 어떤 프로그램이 이용가능한지를 나타내는 프로그램 가이드의 대역내 또는 대역외 공급(in-band or out-of-band feed)이 있을 수 있다. 케이블 채널 수는 유한이고 장비/케이블 대역폭에 의해 제한된다. 케이블 분배 시스템은 상당한 케이블 투자를 요하며 업그레이드하는데 비용이 많이 든다.

[0005] 텔레비젼 콘텐트 대부분은 그의 프로듀서에게 귀중한 것이므로 판권 소유자는 억세스를 제어하여 카피를 제한하기를 원한다. 통상적으로 보호받는 재료의 예들은 극장 필름, 스포츠 이벤트 및, 성인 프로그래밍을 포함하고 있다. 조건적 억세스(CA) 시스템은 케이블 시스템과 같은 콘텐트 전달 시스템에서 프로그래밍의 이용을 제어하는데 사용된다. CA 시스템은 매칭된 세트로서 형성된다: 한 파트는 케이블 시스템 헤드엔드내에 합체되어 프리

미엄 콘텐트를 암호화하고 다른 파트는 암호해독을 제공하며 이용자의 가정에 설치된 셋톱 박스(STB)내에 설치된다. NDS(캘리포니아 뉴포트 비치), 모토로라(일리노이 샤움버그) 및 사이언티픽 애틀랜타(조지아 애틀랜타)가 제공하고 있는 것을 포함해서 여러 개의 CA 시스템이 케이블 산업에 이용되고 있다. 앞서 언급한 CA 시스템의 매칭된 세트 상황은 "레거시" 벤더가 부가의 STB 공급자로서 고착되는 효과를 가지고 있다. 조건적 억세스에 대한 다양한 기술(이들은 종종 소유권이 형성되어 있음)이 상호 호환되지 않기 때문에, 임의의 새로운 잠재적 공급자는 레거시 CA를 라이센스해야만 한다. 그래서, 기술 소유권자가 종종 협조하기를 원치않거나 합리적인 라이센스료 지불도 꺼리기 때문에 케이블 오퍼레이터는 다른 셋톱 박스 제조업자로부터 새로운 기술 또는 경쟁력있는 기술을 습득할 수 없다는 것을 스스로 알게 된다. 이러한 비유연성은 이종의 CA 시스템을 가지고 있는 케이블 회사들이 합병하고자 할 때 특히 장애가 될 수 있다. 서비스 제공자들은 몇 가지 이유로 인해 STB에 대해 하나 이상의 소스를 원할 것이다.

[0006] 케이블 오퍼레이터가 일단 암호 스킴을 선택하면, 백워드 호환가능 디코딩 디바이스(예를 들어, 셋톱박스)를 삽입하지 않고는 콘텐트 암호 시스템을 교체하거나 갱신하기가 어렵다. 멀티플 암호해독 능력을 제공하는 기술이 STB 벤더가 이용가능하다는 가정하에, 멀티플 암호화 시스템을 처리하기 위해 새로운 셋톱박스에 다양한 모드 능력을 제공하고자 하면 임의의 새로운 셋톱박스에 상당한 비용을 부가해야만 할 것이다.

[0007] 레거시 벤더에 의한 지배(도매 대체 수단의 부족)를 피하기 위한 공지된 현 옵션은 "풀 듀얼 캐리지(full dual carriage)"를 이용하는 것이다. 풀 듀얼 캐리지는 이용될 CA 암호화의 각 종류에 대해 한번씩 각각의 암호화된 프로그램에 대해 전송이 중복된다는 것을 의미한다. 풀 듀얼 캐리지를 제공하기 위해서 헤드엔드가 CA의 각 형태를 동시에 제공하도록 강화되어 있다. 레거시 STB는 충돌되어서는 안되며 어떤 변화에도 불구하고 그들의 기능을 연속 수행하여야 한다. 그러나, 풀 듀얼 캐리지는 종종 대역폭 충돌 때문에 불합리한 가격대를 형성함으로써, 이용가능한 고유의 프로그램 수가 감소된다. 일반적으로, 프리미엄 채널의 수로 인해 뷰어가 이용가능한 옵션의 수가 제한되고 케이블 오퍼레이터가 제공할 수 있는 가격이 제약을 받게될 수 있다.

[0008] 종래의 케이블 시스템 배열이 도 1에 도시되어 있다. 그러한 시스템에서, 케이블 오퍼레이터는 케이블 시스템-헤드엔드(22)에서 시스템 A에 따르는 CA 암호화 장비(18)를 이용하는 제조업자 A(시스템 A)로부터의 CA 기술을 갖춘 오디오/비디오(A/V) 콘텐트(14)를 소유하고 있다. 시스템 정보(SI)(26) 및 프로그램 특정 정보(PSI)(27)와 함께 암호화된 A/V 콘텐트는 함께 멀티플렉스되어 케이블 시스템(32)을 통해서 이용자의 STB(36)로 전송된다. STB(36)는 A/V 콘텐트를 해독하는 시스템 A(제조업자 A)로부터의 암호해독 CA 장비를 탑재하고 있다. 암호해독된 A/V 콘텐트는 이용자가 볼 수 있도록 텔레비젼 세트(44)에 제공될 수 있다.

[0009] 도 1과 같은 케이블 시스템에 있어서, 디지털 프로그램 스트림은 전송을 위한 패킷들로 나뉘어 진다. 프로그램(비디오, 오디오, 보조 데이타, 등)의 각 컴포넌트에 대한 패킷들에는 패킷 식별자 또는 PID가 태크된다. 한 채널내에서 운반된 모든 프로그램의 각 컴포넌트에 대한 이들 패킷 스트림들이 모여서 하나의 복합(composite) 스트림이된다. 또한 암호해독 키 및 다른 오버헤드 정보를 제공하기 위한 부가의 패킷들이 포함되어 있다. 반면에, 사용되지 않은 대역폭은 널 패킷(null packets)으로 채워진다. 대역폭 버짓(budgets)은 통상 이용가능한 채널 대역폭의 약 95%를 이용하도록 조정된다.

[0010] 오버헤드 정보는 일반적으로 어떤 프로그램이 이용가능한지 그리고 관련된 채널 및 컴포넌트를 찾는 방법을 설명해 주는 가이드 데이타를 포함하고 있다. 이 가이드 데이타는 또한 시스템 정보 또는 SI로서 알려져 있다. SI는 STB 대역내(한 채널내에서 인코딩된 데이타 부분) 또는 대역외(이 목적을 위해 할당된 특정 채널을 이용함)에 전달될 수 있다. 전자적으로 전달된 SI는 부가의 전통적인 형태 즉 신문이나 잡지에 실린 그리드(grid)로 부분적으로 복제될 수 있다.

[0011] 뷰어가 만족스런 텔레비젼 경험을 얻기 위해서는, 일반적으로 뷰어가 오디오 및 비디오 콘텐트에 클리어하게 억세스하는 것이 바람직하다. 어떤 아날로그 케이블 시스템들은 승인받지 않은 뷰어가 돈을 지급하지 않고 프로그래밍을 수신하는 것을 방지하기 위해 비디오를 흐리게 하는 다양한 필터링 기술을 이용해 왔다. 그러한 시스템에서, 아날로그 오디오는 종종 클리어하게 전송된다. C-밴드 위성 전송에 이용된 모토로라 비디오사이퍼 2 플러스 시스템(Motorola Video Ciper 2 Plus System)에서는, 강한 디지털 오디오 암호화가 (동기 반전을 이용하는) 아날로그 비디오의 비교적 약한 보호와 연계되어 이용된다. 비행중의 항공기 무비 시스템에서는, 지불하는 고객에게만 풀 오디오 및 비디오를 제공하기 위해 헤드폰의 렌탈을 통해서만 오디오를 이용할 수 있게 하는 것이 이용되어 왔다.

발명의 내용

발명의 실시를 위한 구체적인 내용

[0012] 본 발명이 많은 다양한 형태로 구현가능하지만 본 명세서가 본 발명의 원리에 대한 예로서 간주되며 도시되어 있고 이하 설명되는 특정 실시예들에 본 발명을 한정하고자 함이 아니라는 이해를 바탕으로 본 발명의 특정 실시예들에 대해 상세히 설명하고자 한다. 이하의 설명에서 동일한 참조 번호는 몇 개의 도면에서 동일하거나 유사하거나 대응하는 부분을 기술하는데 이용된다. 용어 "스크램블" 및 "암호화" 및 이들의 변형은 본 명세서에서 동일한 의미로 이용된다. 또한 용어 "텔레비젼 프로그램" 및 유사한 용어들은 텔레비젼 세트 또는 유사한 모니터 디바이스상에 표시될 수 있는 A/V의 임의의 단편을 의미함은 물론이고 일반적인 대화체 의미로 해석될 수 있다.

[0013] 개요

[0014] 근래의 디지털 케이블 네트워크는 일반적으로 적절하게 가입한 사람을 제외하고는 프로그램에 억세스하지 못하도록 디지털 비디오 및 오디오를 완전하게 암호화하는 CA 시스템을 이용한다. 그러한 암호화는 해커 및 비가입자가 돈을 지불하지 않은 프로그램밍을 수신하지 못하도록 설계되어 있다. 그러나, 케이블 오퍼레이터들이 그들의 가입자들에게 임의의 여러 제조업자가 생산한 셋톱 박스를 제공하고자 해도, 이들은 각 STB 제조업자의 CA 시스템과 상응하는 멀티플 암호화 기술로 암호화된 싱글 프로그램의 멀티플 카피를 전송해야할 필요성 때문에 좌절하게 된다.

[0015] 이와 같이 프로그래밍의 다수의 사본을 운반해야하는 필요성(소위 "풀 듀얼 캐리지"라고 불리고 있음)을 충족하려면 뷰어에게 부가의 프로그래밍 콘텐트를 제공하는데 이용될 수 있는 귀중한 대역폭을 완전히 이용해야한다. 본 발명의 특정 실시예들은 멀티플 캐리지에 상당하는 것을 제공하기 위한 대역폭 필요조건이 최소화되는 문제를 다루고 있다. 이 결과는 풀 대역폭 비용 없이도 풀 듀얼 캐리지의 장점들이 제공되기 때문에 "버추얼 듀얼 캐리지"로 기술될 수 있다. 본 명세서에 제시되는 본 발명의 몇몇 실시예들은 효과적인 부분적 스크램블링을 달성한다. 이들 실시예들은 암호화를 위한 부분을 선택하는데 이용된 기준(criteria)에 따라 다르다. 이후 선택된 부분은 부가의 대역폭 필요조건 및 암호화의 유효에 영향을 준다. 본 발명의 실시예들과 상응하는 방식들과 연계해서 하나의 암호화 처리 또는 몇 개의 처리를 이용하는 것이 바람직할 수 있다.

[0016] 여기서 설명되는 부분적 이중 암호화의 구현들 중 어떤 것은 각각의 복제된 컴포넌트에 대해 부가의 (2차) PID를 이용한다. 이들 2차 PID는 부가의 암호화 방법으로 복제된 콘텐트를 운반하는 패킷을 태그하는데 이용된다. 삽입된 PID가 레거시 STB에 의해서는 무시되지만 새로운 STB에 의해서 쉽게 추출되는 식으로 이들 새로운 PID의 존재에 대한 정보를 전송하는 PSI가 강화되어 있다.

[0017] 부분적 이중 암호화의 일부 구현들은 소정의 PID로 태그된 특정 패킷들만을 복제하는 것을 포함한다. 암호화한 패킷들을 선택하는 방법이 이하 상세히 설명된다. 오리지널(즉, 레거시) PID는 클리어하게 전송된 패킷들은 물론이고 레거시 암호화로 암호화된 패킷들을 계속해서 태그한다. 새로운 PID는 제2 암호화 방법에 의해 암호화된 패킷들을 태그하는데 이용된다. 2차 PID를 가지고 있는 패킷들은 1차 PID로 태그된 암호화된 패킷들을 따라다닌다(shadow). 암호화된 쌍들을 구성하는 패킷들은 순차적으로 나타날 수 있으나 양호한 실시예에서는 PID 스트림의 클리어 부분을 갖고 있는 시퀀스를 유지한다. 1차 및 2차 PID를 이용함으로써, 셋톱박스내에 위치한 디코더는 셋톱박스에 관련된 암호해독 방법을 이용하여 어느 패킷이 암호해독되어야 하는지를 쉽게 결정할 수 있다. 이는 다음의 설명을 고려해 보면 명백히 알 수 있을 것이다. PID를 다루는데 이용되는 처리들은 나중에 상세히 설명하기로 한다.

[0018] 여기서 설명되는 암호화 기술은 3개의 기본 변화로 (한 분류화에 따라서) 크게 분류할 수 있다: 메이저 부분(즉, 오디오)만 암호화, SI만 암호화, 및 단지 선택된 패킷들만 암호화. 일반적으로, 여기서 설명되는 실시예들에 이용된 암호화 기술들 각각은 대역폭을 보존하기 위해서 클리어하게 A/V 신호 또는 관련된 정보의 부분들을 암호화하고 A/V 신호의 다른 부분은 남겨두는 것을 추구한다. 동일한 클리어 부분이 다양한 모든 셋톱박스에 전송될 수 있기 때문에 대역폭이 보존될 수 있다. 암호화될 정보의 부분들을 선택하는데 다양한 방법이 이용된다. 이렇게 함으로써, 본 발명의 다양한 실시예들은 하나의 특정 스크램블링 스킴으로 전체 콘텐트를 암호화하는 종래의 "브루트-포스(brute-force)" 기술을 무시한다. 이와 같은 종래의 기술에서는 교번적인 스크램블링 스킴이 요구되는 경우 대역폭의 중복 이용이 예측된다. 또한, 여기서 설명되는 부분적 이중 암호화 스킴 각각은 본 발명의 실시예들로부터 벗어남이 없이 싱글 부분 암호화 스킴으로서 이용될 수 있다.

[0019] 본 발명의 다양한 실시예들은 콘텐트를 올바르게 재생하는데 요구되는 단지 작은 양의 정보를 암호화하면서 콘텐트의 실질적인 부분을 명료하게 전송하기 위해 여러 개의 처리를 단독으로 또는 조합으로 이용한다. 그러므

로, 특정 스크램블링 스킴으로 고유하게 암호화되는 전송된 정보량은 각각의 원하는 프로그램 스트림의 전체 복제에 비해서 콘텐트의 작은 퍼센티지를 차지한다. 이 명세서의 예시적인 시스템의 목적 달성을 위해서, 암호화 시스템 A가 레거시 시스템 전체에 고려될 것이다. 앞서 언급한 몇 개의 암호화 기술 각각은 이하 상세히 설명될 것이다.

[0020] 본 발명의 다양한 실시예들은 각각의 참여 CA 시스템이 독립적으로 동작될 수 있게 해준다. 각각은 다른 것에 오소고널(orthogonal)하다. 헤드엔드 내의 키 공유는 각 시스템이 그 자신의 패킷들을 암호화하기 때문에 요구되지 않는다. 서로 다른 키 에포치(epoch)는 각각의 CA 시스템에 의해 이용될 수 있다. 예를 들어, 모토로라의 소유인 암호화 방식으로 암호화된 패킷들은 내장된 보안 ASIC를 이용하는 빠른 변환 암호화 키를 이용할 수 있는 한편, NDS 스마트 카드 기반 시스템으로 암호화된 패킷들은 약간 더 느린 변환 키를 이용한다. 이 실시예는 사이언티픽 애틀랜타 및 모토로라 레거시 암호화에도 동일하게 잘 적용된다.

[0021] 암호화된 엘리멘터리 스트림

[0022] 도 2를 보면, 멀티플 캐리지를 제공하기 위한 부가의 대역폭을 감소시키기 위한 시스템의 한 실시예가 시스템(100)으로 도시되어 있다. 이 실시예에서, 이 시스템은 오디오없이 텔레비젼 프로그래밍를 보는 것은 일반적으로 바람직하지 않다는 사실의 장점을 취하고 있다. 예외(예를 들어, 성인 프로그램밍, 일부 스포팅 이벤트, 등)가 있을 지라도, 통상적인 뷰어들은 오디오를 듣지 않으면서 텔레비젼 프로그래밍의 틀에 박힌 보기는 원치 않을 것이다. 그래서, 헤드엔드(122)에서, 케이블 네트워크를 통한 방송을 위해 비디오 신호(104)는 클리어하게(비암호화된) 제공되나 클리어 오디오(106)는 멀티플 CA 시스템에 제공된다. 예시적인 시스템(100)에서, 클리어 오디오(106)는 암호화 시스템 A(암호화 시스템 A는 이 명세서 전체에 걸쳐서 레거시 시스템으로 고려된다)를 이용하여 오디오 데이타를 암호화하는 암호화 시스템(118)에 제공된다. 동시에, 클리어 오디오(106)는 암호화 시스템 B를 이용하여 오디오 데이타를 암호화하는 암호화 시스템(124)에 제공된다. 이후 클리어 비디오는 118(오디오 A)로부터의 암호화된 오디오 및 124(오디오 B)로부터의 암호화된 오디오, 시스템 정보(128) 및 프로그램 명세 정보(129)와 함께 멀티플렉스된다.

[0023] 케이블 시스템(32)을 통한 분배 후에, 비디오, 시스템 정보, 프로그램 명세 정보, 오디오 A 및 오디오 B는 모두 셋톱박스(36 및 136)에 전달된다. 레거시 STB(36)에서, 비디오는 디스플레이되고 암호화된 오디오는 텔레비젼 세트(44)에서의 재생을 위해 CA 시스템 A(40)에서 암호해독된다. 유사하게, 새로운 STB(136)에서, 비디오는 디스플레이되고 암호화된 오디오는 텔레비젼 세트(144)에서의 재생을 위해 CA 시스템 B(140)에서 암호해독된다.

[0024] 오디오는 완전한 A/V 프로그램(또는 단지 비디오 부분)에 비해서 비교적 낮은 대역폭 필요조건을 가지고 있다. 384 Kb/초인 스테레오 오디오를 위한 현행 최대 비트 레이트는 3.8 Mb/초 텔레비젼 프로그램의 대략 10%이다. 그래서, 256 QAM(구형 진폭 변조)으로 운반되는 10개의 채널을 가지고 있는 시스템에서 암호화된 오디오(비디오는 클리어하게 전송됨)만의 듀얼 캐리지를 위해서는, 단지 약 1 채널분의 대역폭 손실이 따를 것이다. 그러므로, 대략 9개의 채널이 운반될 수 있다. 이는 모든 채널을 이중 암호화해야 하는 필요성 - 이는 이용가능한 채널을 10개에서 5개로 감소시키는 결과를 초래한다 - 에 비해 획기적인 발전이다. 예를 들어, 스포팅 이벤트, 페이 퍼 뷰, 성인용 프로그래밍, 등과 같이 필요하다고 간주 되면 오디오 및 비디오의 이중 암호화를 실행할 수도 있다.

[0025] 레거시 및 새로운 셋톱박스는 비디오를 클리어하게 수신하고 암호화된 A/V 콘텐트를 완전히 해독하는데 이용된 것과 같은 식으로 오디오를 암호해독하는 노멀한 식으로 기능할 수 있다. 이용자가 상기 스킴에 따라서 암호화된 프로그래밍에 가입하지 않았다면, 이용자는 오디오는 듣지 못하고 기껏해야 비디오만을 볼 수 있다. 비디오에 대한 보안을 강화하기 위해서, 나중에 설명될 본 발명의 다른 실시예들을 이용할 수 있다. (예를 들어, SI는 승인되지 않은 셋톱박스가 프로그램의 비디오 부분에 동조하는 것을 좀 더 어렵게 만들어 주기 위해 스크램블될 수 있다.) 해커에 의해 수정되지 않은 비승인된 셋톱박스는 암호화된 오디오의 수신 결과로서 비디오는 텅 비울(blank) 것이다.

[0026] 승인된 셋톱박스는 억세스 기준 및 디스크램블링 키를 얻는데 이용되는 엔타이틀먼트 콘트롤 메시지(ECM; Entitlement Control Messages)를 수신한다. 이 셋톱박스는 이 키를 오디오는 물론이고 비디오에 적용하기 위해 시도한다. 비디오가 스크램블되어 있지 않기 때문에, 셋톱박스의 디스크램블러를 통해서 그대로 간단히 통과한다. 셋톱박스는 비디오가 클리어 상태라는 것에 개의치 않는다. 수정이 없고 가입되지 않은 셋톱박스는 클리어 비디오는 물론이고 스크램블된 오디오에 대해 비승인된 것으로 작동한다. 실제로 스크램블된 오디오는 물론이고 비디오는 텅비게 된다. 뷰어에게 프로그래밍에 가입할 필요성이 있음을 알리는 온-스크린 디스플레이가 TV상에 나타날 것이다. 이는 뜨내기(casual) 뷰어가 콘텐트를 보고 듣는 것을 바람직하게 완전히 차단한다.

[0027] 본 발명의 한 실시예에서, 암호화된 오디오는 A/V 채널을 통해 디지털 패킷으로 전송된다. 2개(또는 이 이상)의 오디오 스트림들은 시스템의 셋톱박스가 이용하는 2개의(또는 이 이상) 암호화 시스템에 따라서 암호화되어 전송된다. 두개의(또는 이 이상의) STB가 그들의 각 오디오 스트림들을 적절히 암호해독해서 디코딩하도록 하기 위해서, SI(시스템 정보) 데이타는 오디오를 찾기 위한 전송된 서비스 식별자를 이용하여 오디오가 발견될 수 있는 특정 채널을 식별하는 케이블 시스템의 헤드엔드(122)로부터 전송된다. 이는 시스템 A에 대한 오디오에는 제1 패킷 식별자(PID)를 할당해주고 시스템 B에 대한 오디오에는 제2 패킷 식별자(PID)를 할당해 줌으로써 달성된다. 예로서, 다음의 프로그램 명세 정보(PSI)는 두 시스템(하나는 NDS 조건적 억세스를 이용하고, 다른 하나는 모토로라 조건적 억세스를 이용함)에 대한 오디오의 위치를 식별하기 위해 전송될 수 있다. 본 기술 분야에 숙련된 자이면 이 정보를 후에 설명될 부분적 암호화의 다른 실시예들에 어떻게 적용할 수 있는지를 이해할 것이다.

[0028] SI는 레거시 및 비-레거시 셋톱박스 모두에 개별적으로 전달될 수 있다. 레거시 및 비-레거시 셋톱박스가 근본적으로 간섭없이 동작할 수 있도록 SI 정보를 전송하는 것이 가능하다. 레거시 셋톱박스에 전달된 SI에 있어서, VCT(가상 채널 테이블)는 원하는 프로그램, 예를 들어, 프로그램 번호 1로서 참조된 HBO는 서비스 ID "1"에 있고 VCT 억세스 제어 비트는 설정되어 있음을 말하고 있다. 네트워크 정보 테이블(NIT)은 서비스 ID "1"이 주파수=1234에 있음을 나타낸다. 비-레거시 셋톱박스에 전달된 SI에 있어서, VCT는 원하는 프로그램, 예를 들어, 프로그램 번호 1001로서 참조된 HBO가 서비스 ID "1001"에 있고 VCT 억세스 제어 비트는 설정되어 있음을 나타낸다. 비-레거시 STB에 전달된 네트워크 정보 테이블은 서비스 ID "1001"가 주파수 1234에 있음을 가리킨다. 다음의 예시적인 프로그램 관련 테이블 PSI 데이타는 (MPEG 데이타 구조 포맷으로) 레거시 및 비-레거시 셋톱박스에 전송된다.

[0029]

PID=0×0000으로 전송된 PAT

PAT 0×0000
-전송 스트림 ID
-PAT 버전
-프로그램 번호 1
 -PMT 0×0010
-프로그램 번호 2
 -PMT 0×0020
-프로그램 번호 3
 -PMT 0×0030
-프로그램 번호 4
 -PMT 0×0040
-프로그램 번호 5
 -PMT 0×0050
-프로그램 번호 6
 -PMT 0×0060
-프로그램 번호 7
 -PMT 0×0070
-프로그램 번호 8
 -PMT 0×0080
-프로그램 번호 9
 -PMT 0×0090
-프로그램 번호 1001
 -PMT 0×1010
-프로그램 번호 1002
 -PMT 0×1020
-프로그램 번호 1003
 -PMT 0×1030
-프로그램 번호 1004
 -PMT 0×1040
-프로그램 번호 1005
 -PMT 0×1050
-프로그램 번호 1006
 -PMT 0×1060
-프로그램 번호 1007
 -PMT 0×1070
-프로그램 번호 1008
 -PMT 0×1080
-프로그램 번호 1009
 -PMT 0×1090

[0030] 다음의 예시적인 프로그램 맵 테이블 PSI 데이타는 레거시 및 비-레거시 셋톱박스(MPEG 데이타 구조 포맷으로)에 의해 선택적으로 수신된다:

[0031]

PID=0×0010으로 전송된 PMT

PMT 0×0010
- PMT 프로그램 번호 1
- PMT 섹션 버전 10
- PCR PID 0×0011
- 엘리멘터리 스트림
  - 스트림 유형(비디오 0×02 또는 0×80)
  - 엘리멘터리 PID(0×0011)
  - 디스크립터
  - CA 제공자 #1에 대한 CA 디스크립터(ECM)
- 엘리멘터리 스트림
  - 스트림 유형(오디오 0×81)
  - 엘리멘터리 PID(0×0012)
  - 디스크립터
  - CA 제공자 #1에 대한 CA 디스크립터(ECM)

PID=0×1010으로 전송된 PMT

PMT 0×1010
- PMT 프로그램 번호 1010
- PMT 섹션 버전 10
- PCR PID 0×0011
- 엘리멘터리 스트림
  - 스트림 유형(비디오 0×02 또는 0×80)
  - 엘리멘터리 PID(0×0011)
  - 디스크립터
  - CA 제공자 #2에 대한 CA 디스크립터(ECM)
- 엘리멘터리 스트림
  - 스트림 유형(오디오 0×81)
  - 엘리멘터리 PID(0×0013)
  - 디스크립터
  - CA 제공자 #2에 대한 CA 디스크립터(ECM)

[0032] NDS CA는 물론이고 모토로라 또는 사이언티픽 애틀랜타를 이용하는 시스템에서 프로그래밍을 전달하는 것이 바람직한 예를 고려해 보면, 상기 통신은 단지 사소한 변경을 제외하고는 그들의 CA 시스템 내의 모토로라 및 사이언티픽 애틀랜타에 의해 전달된 PSI와 일치한다. 프로그램 관련 테이블(PAT)는 각 프로그램에 대한 부가의 프로그램 맵 테이블(PMT)을 참조하도록 변경된다. 이 실시예에서의 각 프로그램은 PAT내에 2개의 프로그램 번호를 가지고 있다. 상기 테이블에서, 프로그램 번호 1 및 프로그램 번호 1001은 이들이 다른 오디오 PID 및 CA 디스크립터를 참조한다는 것을 제외하고는 동일한 프로그램이다. 멀티플 PMT를 생성하고 데이타 스트림으로 새로운 PAT 및 PMT를 멀티플렉스하기 위한 시스템 내의 변경은 케이블 시스템 헤드엔드 장비를 적절히 수정하여 달성할 수 있다. 다시, 본 기술분야에서 숙련된 자이면 이들 메시지를 여기서 설명된 다른 부분적 암호화 스킴에 어떻게 적응시켜야하는지를 이해할 것이다. 이러한 접근법의 장점은 헤드엔드 또는 레거시 및 비-레거시 셋톱박스가 이 스킴을 이용하여 암호화된 레거시 및 비-레거시인 오디오를 전달하는데 특별한 하드웨어나 소프트웨어가 요구되지 않는다는 것이다.

[0033] 이 기술은 이용자가 지불되지 않은 프리미엄 프로그래밍을 듣지 못하게 하여 이의 이용을 저지하지만 해커는 비디오를 동조하려는 시도를 할 수 있다. 이를 퇴치하기 위해, 본 발명에 상응하는 다른 암호화 기술들(후에 설명될 것임)에 이용된 메카니즘들은 원하는 경우 동시에 이용될 수도 있다. 클로즈드 캡셔닝(closed captioning)은 일반적으로 비디오 데이타의 일부로서 전송되기 때문에, 이용자는 클리어 비디오와 연관해서 판독가능한 오디오 정보를 얻을 수 있다. 그래서, 어떤 애플리케이션들에는 적절할지라도, 현 기술 단독으로는 모든 시나리오에서 적절한 보호를 제공할 수 없다. 다른 실시예에서, 유료의 일부로서의 클로즈드 캡셔닝 정보

를 포함하고 있는 비디오 패킷들은 부가적으로 스크램블할 수 있다.

[0034] 대안 실시예에서는 비디오만이 암호화된 비디오의 각 세트에 할당된 개별 PID로 듀얼(dual) 암호화될 수 있다. 이는 (비디오가 오디오 보다 더 중요할 수 있기 때문에) 일반적인 프로그래밍에 대한 보안 암호화를 제공할 수 있지만, 단지 오디오만이 거의 모든 셋톱박스들에 공유되어 있기 때문에 풀 듀얼 캐리지와 비교할 때 대역폭 절약 양은 대략 10%에 불과하다. 그러나, 이 접근법은 특정 콘텐트, 예를 들어, 성인용 및 스포츠용으로 이용될 수 있으며 이 콘텐트에 대한 대역폭 오버헤드를 감소시킬 수 있는 한편 오디오 암호화 접근법은 다른 콘텐트 유형에 이용될 수 있다. DirecTV™ 서비스에 이용된 디지털 위성 서비스(DSS) 전송 표준에서, 암호화를 위한 오디오 패킷들은 동등한 것으로 간주되는 서비스 채널 식별자(SCID)의 이용에 의해 식별될 수 있다.

[0035] 타임 슬라이싱(TIME SLICING)

[0036] 본 발명에 상응하는 다른 실시예는 여기서 타임 슬라이싱이라 칭하고 도 3에 시스템(200)으로 도시되어 있다. 이 실시예에서, 각 프로그램의 일부는 이용자가 프로그래밍에 돈을 지불하지 않은 경우 이 프로그램의 보기를 방해하는 식으로 타임 종속 기반으로 암호화된다. 본 발명의 이 실시예는 부분적으로 암호화된 비디오 및 오디오, 클리어 비디오 및 부분적으로 암호화된 오디오 또는 부분적으로 암호화된 비디오 및 오디오로서 구현될 수 있다. 전체 시간의 백분율로 취해진 암호화되는 타임 슬라이스의 기간은 대역폭 이용과 해커에 대한 보안의 적절한 균형에 부합하게 선택될 수 있다. 일반적으로, 여기서 설명된 실시예들 중 임의 실시예에서는, 콘텐트의 100% 미만이 암호화되어 원하는 부분적 암호화가 이루어진다. 다음의 예는 부분적으로 암호화된 비디오 및 오디오를 설명하고 있다.

[0037] 예로서, 이 예시적인 실시예에 따라 듀얼 부분 암호화되는 9개의 프로그램을 갖고 있는 시스템을 고려하기로 한다. 이들 9개의 채널은 멀티플렉스된 패킷들의 스트림으로서 케이블 헤드엔드에 공급되고 9개의 프로그램중 특정한 하나의 프로그램에 관련된 패킷들을 식별하기 위한 디지털 식별자(PID)를 이용하여 디지털식으로 인코드된다. 이 예에서, 이들 9개의 프로그램들이 번호 101-109가 부여된 비디오 PID 및 번호 201-209가 부여된 PID를 가지고 있는 것으로 가정한다. 이 실시예에 따른 부분적 암호화는 싱글 프로그램으로부터의 패킷들만이 임의의 소정 시간에 암호화되도록 프로그램들 사이에서 타임 멀티플렉스된다. 이 방법은 콘텐트를 알고 있어야할 필요는 없다.

[0038] 아래 표 1을 참조로 해서, 본 발명의 실시예에 상응하는 타임 슬라이스 이중 암호화 스킴의 예시적인 실시예가 도시되어 있다. 1차 비디오 PID 101 및 1차 오디오 PID 201를 가지고 있는 프로그램 1의 경우, 제1 타임 기간 동안, PID 101 및 PID 201를 가지고 있는 패킷들은 암호화 시스템 A를 이용하여 암호화되는 한편, 다른 프로그램들을 나타내는 다른 것들은 클리어하게 전송된다. 이 실시예에서, 2차 PID는 또한 비디오 및 오디오에 할당된다. 2차 PID들은 각각 프로그램 1에 대한 비디오 PID 111 및 오디오 PID 211이다. 2차 PID를 가지고 있는 패킷들은 제1 타임 기간 동안 암호화 시스템 B를 이용하여 암호화된다. 다음의 8 타임 기간들은 클리어하게 전송된다. 이후, 타임 기간 10 동안 4개의 PID중 임의의 것을 가지고 있는 패킷들은 다시 암호화되고, 뒤이어 다음의 8 타임 기간이 클리어하게 전송된다. 유사한 방식으로, 제2 기간 동안 1차 비디오 PID 102 및 1차 오디오 PID 202를 가지고 있는 프로그램 2는 암호화 시스템 A를 이용하여 암호화되고 이들과 관련된 2차 PID를 가지고 있는 패킷들은 암호화 시스템 B를 이용하여 암호화되며, 다음의 8 타임 기간 동안에는 클리어하게 전송되는 등의 동작을 수행한다. 이 패턴은 표 1에서 처음 9개 행을 검사해 보면 명확하게 알 수 있다. 본 발명의 범위를 벗어남이 없이 오디오 및 비디오 패킷, 또는 오디오만 또는 비디오만 이 기술에 따라서 암호화될 수 있다. 또한 오디오 및 비디오는 그들 자신의 개별적인 암호화 시퀀스를 가질 수 있다. 표 1에서, P1은 타임 기간 번호 1을 가리키고, P2는 타임 기간 번호 2를 가리키는 등의 동작을 수행한다. EA는 정보가 CA 시스템 A를 이용하여 암호화됨을 가리키며, EB는 정보가 CA 암호화 시스템 B를 이용하여 암호화되는 것을 가리킨다.

표 1

[0039]

프로그램	비디오 PID	오디오 PID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	...
1	PID 101	PID 201	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	클리어	...
2	PID 102	PID 202	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	...
3	PID 103	PID 203	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	...
4	PID 104	PID 204	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
5	PID 105	PID 205	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
6	PID 106	PID 206	클리어	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	...
7	PID 107	PID 207	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	...
8	PID 108	PID 208	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	...
9	PID 109	PID 209	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	...
1	PID 111	PID 211	EB									EB			...
2	PID 112	PID 212		EB									EB		...
3	PID 113	PID 213			EB									EB	...
4	PID 114	PID 214				EB									...
5	PID 115	PID 215					EB								...
6	PID 116	PID 216						EB							...
7	PID 117	PID 217							EB						...
8	PID 118	PID 218								EB					...
9	PID 119	PID 219									EB				...

[0040] 설치된 레거시 암호화 시스템(암호화 시스템 A)과의 호환성을 유지하기 위하여, 1 내지 9의 프로그램들 각각에 대한 암호화된 기간들은 암호화 시스템 A를 이용하여 암호화된다. 레거시 STB 장비는 그렇게 부분 암호화된 A/V 데이타 스트림을 수용해서 암호화되지 않은 패킷은 통과시키고 암호화된 패킷은 투명하게 암호해독한다. 그러나, 암호화 시스템 A 및 암호화 시스템 B 둘 다를 이용하여 이중 암호화를 얻는 것이 바람직하다. 이를 달성하기 위해서, 명기된 프로그램에는 소정의 프리미엄 채널에 대한 엘리멘터리 데이타 스트림을 운반하기 위한 1차 PID(예를 들어, 프로그램 1에 대해, 비디오 PID 101 및 오디오 PID 201) 및 2차 PID(예를 들어, 프로그램 1에 대해 비디오 PID 111 및 오디오 PID 211)가 할당된다.

[0041] 도 3을 참조해 보면, 시스템(200)은 헤드엔드(222)에서 클리어 비디오(208)의 N 채널이 인텔리전트 스위치(216)(이는 프로그램된 처리기의 제어하에 동작함)에 제공된다. 이 스위치는 220에서 1차 PID가 할당되는 클리어로 전송되는 패킷들의 경로를 정해준다. 암호화될 패킷들은 조건적 억세스 시스템 A 암호기(218) 및 조건적 억세스 시스템 B 암호기(224)로 방향이 전해진다. 일단 암호화되면, 218 및 224부로부터 암호화된 패킷들에는 220에서 각각 1차 또는 2차 PID가 할당된다. 228로부터의 시스템 정보와 229로부터의 PSI는 멀티플렉스되거나, 케이블 시스템(32)을 통해 클리어 패킷, 시스템 A 암호화된 패킷과 시스템 B 암호화된 패킷 및 방송과 결합된다.

[0042] 논의의 목적으로, 타임 슬라이스의 기간이 100 밀리초이면 표 1에 도시된 바와 같이, 평균해서 하나와 단편 암호화된 기간들이 있으며, 이들을 모두 합하면 모든 9개의 프로그램에 대해 초마다 111밀리 초이다. 기간이 50 밀리초이면, 평균해서 두개와 단편 암호화된 기간들이 있고, 이들은 합해서 111 밀리초이다. 비디오를 동조하고자 시도하는 비-가입 박스는 임의의 종류의 이미지 록(lock)이 유지될 수 있고 오디오가 왜곡(garble)된다면 매우 나쁜 이미지를 얻을 것이다.

[0043] 부분적으로 스크램블된 스트림에 대한 PSI는 상기 이중 암호화 예와는 약간 다르게 처리된다. 근본적으로, 동일한 SI 및 PAT PSI 정보가 레거시 및 비-레거시 셋톱박스에 전송될 수 있다. 차이는 PMT PSI 정보에 있다. 레거시 셋톱박스는 PMT PSI를 해부해서 이전과 같이 1차 오디오 및 비디오 PID를 얻는다. 비-레거시 셋톱박스는 레거시 셋톱박스와 같은 1차 PID를 얻지만, 스트림이 부분적으로 스크램블되어 있는지를 알기 위해서 PMT PSI내의 CA 디스크립터를 조사해야만 한다. 2차 PID는 특정 CA 제공자에 대해 명시적으로 스크램블되고, 그 결과 PID에게 신호를 보내는데 특정 CA 제공자에게 특정한 CA 디스크립터를 이용할 수 있다. 본 발명은 하나 이상의 2차 PID를 허용해줌으로써 2 이상의 CA 제공자가 공존할 수 있게 해준다. 2차 PID는 특정 CA 제공자에게 고유한 것이어야 한다. 셋톱박스는 가지고 있는 CA에 대한 CA ID를 알고 있으므로 그에 관련된 모든 CA 디스크립터를 체크할 수 있다.

[0044] ECM용으로 이용된 동일한 CA 디스크립터로 개인용 데이타로서 2차 PID 데이타를 전송하는 것이 가능할지라도 양호한 실시예는 개별적인 CA 디스크립터를 이용한다. 2차 PID는 CA PID 필드에 배치된다. 이는 CA 디스크립터의 개인용 데이타 필드를 분석할 필요없이 헤드엔드 처리 장비가 PID를 "찾을 수" 있게 해준다. ECM과 2차 PID

CA 디스크립터 간의 차이를 알려 주기 위해 더미 개인용 데이타 값이 전송될 수 있다.

[0045]

PID=0×0010으로 전송된 PMT

PMT 0×0010
- PMT 프로그램 번호 1
- PMT 섹션 버전 10
- PCR PID 0×0011
- 엘리멘터리 스트림
  - 스트림 타입(비디오 0×02 또는 0×80)
  - 엘리멘터리 PID(0×0011)
  - 디스크립터
  - CA 제공자 #1에 대한 CA 디스크립터 (ECM)
  - CA 제공자 #2에 대한 CA 디스크립터 (ECM)
  - CA 제공자 #2에 대한 CA 디스크립터 (2차 PID)
- 엘리멘터리 스트림
  - 스트림 타입(오디오 0×81)
  - 엘리멘터리 PID(0×0012)
  - 디스크립터
  - CA 제공자 #1에 대한 CA 디스크립터 (ECM)
  - CA 제공자 #2에 대한 CA 디스크립터 (ECM)
  - CA 제공자 #2에 대한 CA 디스크립터 (2차 PID)

[0046] CA 제공자 #2(ECM)에 대한 CA 디스크립터

[0047]

디스크립터
- 태그:조건적 억세스(0×09)
- 길이: 4 바이트
- 데이타
  - CA 시스템 ID:0×0942(제2 CA 제공자)
  - CA PID(0×0015)

[0048] CA 제공자 #2(2차 PID)에 대한 CA 디스크립터

[0049]

디스크립터
- 태그:조건적 억세스(0×09)
- 길이: 5 바이트
- 데이타
  - CA 시스템 ID:0×1234(제2 CA 제공자)
  - CA PID(0×0016)
  - 개인용 데이타

[0050] CA 시스템 A하에서 동작하는 레거시 STB(36)는, 데이타는 수신하고, 2차 PID는 무시하고, CA 시스템 A하에서 암호화된 패킷은 암호해독하여 프로그램을 텔레비젼 세트(44)에 제공한다. 새로운 또는 비-레거시 STB(236)은 SI(228)을 수신한다. 이는 PSI(229)를 수신하고 보여줄 프로그램에 관련된 제2 CA 디스크립터내에 소집된 1차 및 2차 PID를 식별하는데 PMT를 이용한다. CA 시스템 A하에서 암호화된 패킷들은 버려지고 2차 PID를 갖고 있는 CA 시스템 B하에서 암호화된 패킷들은 CA 시스템 B(240)에 의해 암호해독되어 디코딩을 위한 클리어 데이타

스트림내로 삽입된 후 텔레비젼 세트(244)에 디스플레이된다.

[0051] 도 4는 CA 시스템 A가 레거시 시스템이고 CA 시스템 B가 소개될 새로운 시스템인 본 발명의 실시예를 구현하는데 이용될 수 있는 케이블 시스템 헤드엔드에서 인코딩을 위한 한 처리를 보여주고 있다. 클리어 패킷이 주어진 프로그램에 대한 250에서 수신될 때, 이 패킷(또는 프레임)이 암호화되는 것이 아니면(즉, 이 프로그램을 위한 암호화용 현행 타임 슬라이스가 아니면) 클리어 패킷(C)은 통과되어 254에서 출력 스트림내로 삽입된다. 현행 패킷이 암호화 타임 슬라이스의 일부인 현행 패킷에 의해서 암호화되는 것이면, 이 패킷은 암호화를 위해 패킷 암호화 처리 A(258) 및 패킷 암호화 처리 B(262) 모두를 통과한다. 258(EA)에서 암호화 처리 A로부터의 암호화된 패킷은 254로 가서 출력 스트림내로 삽입된다. 262(EB)에서의 암호화 처리 B로부터의 암호화된 패킷에는 264에서 2차 PID가 할당된 후 254에서 출력 스트림내로 삽입된다. 이는 프로그램 내의 모든 패킷에 대해서 반복된다.

[0052] 도 5는 설명한 바와 같이 1차 및 2차 PID를 갖고 있는 C, EA 및 EB 패킷을 포함하는 수신된 데이타 스트림을 암호해독 및 디코딩을 위해 새로 도입된 CA 시스템 B를 갖고 있는 STB(236)에서 이용되는 처리를 보여주고 있다. 패킷이 272에서 수신되면, 그것이 당해 1차 PID를 가지고 있는지 여부를 알기 위해 조사된다. 가지고 있지 않다면, 이 패킷은 274에서 당해 2차 PID를 가지고 있는지 여부가 검사된다. 패킷이 1차 PID도 아니고 2차 PID도 아니라면, 278에서 무시되거나 탈락된다. 1차 PID도 2차 PID도 아닌 EA 및 EB 패킷들 사이에 개재된 패킷들은 버려진다. 디코더가 대체 매칭된 EA 또는 EB 패킷을 수신하기 전에 멀티플 EA 또는 EB를 행으로 수신할 수 있는지에 대한 버퍼링 이슈가 있다. 또한, 1차 패킷 후가 아닌 1차 패킷 전에 오는 2차 패킷을 검출하는 것은 쉽다. 또한, 2차 패킷이 1차 패킷 전 또는 후에 오게 할 수 있는 회로를 설계하는 것도 가능하다. 이 패킷이 당해 1차 PID를 가지고 있다면, 284에서 이 패킷이 암호화되어 있는지를 결정하기 위해 검사된다. 가지고 있지 않다면, 패킷(C)은 디코딩을 위해 288에서 직접 디코더로 통과된다. 284에서 이 패킷이 암호화되어 있다면, EA 패킷인 것으로 간주되어 278에서 탈락되거나 무시된다. 어떤 구현에서는, 1차 패킷의 암호화가 284에서 체크되지 않는다. 오히려, 284에서는 그것이 대체용인지를 식별하기 위해 2차 패킷에 비해 1차 패킷의 간단한 위치가 체크된다.

[0053] 274에서 이 패킷이 2차 PID를 가지고 있다면, 이 PID는 292에서 1차 PID에 다시 맵핑된다(또는 동등하게 1차 PID가 2차 PID 값에 다시 맵핑된다). 이후 패킷은 296에서 암호해독되어 디코딩을 위해 288에서 패킷 디코더에 전송된다. 물론, 본 기술 분야에 숙련된 자이면 본 발명의 범위를 벗어나지 않고 다양한 변화가 가능함을 인식하고 있을 것이다: 변화의 예로는 292 및 296의 순서 또는 272 및 274의 순서를 바꿀 수 있다는 것이 있다. 초기에 언급한 바와 같이, 284는 2차 패킷에 대한 1차 패킷 위치의 체크로 대체될 수 있다. 다른 변화도 본 기술 분야에 숙련된 자에게는 가능하다.

[0054] 암호화 시스템 A하에서 동작하는 레거시 STB(36)는 2차 PID 패킷을 완전히 무시한다. 1차 PID를 가지고 있는 패킷들은 필요하다면 암호화되고, 이들이 클리어 패킷이면 암호해독없이 디코더에 전달된다. 그래서 암호화 시스템 A하에서 동작하는 소위 말하는 "레거시" STB는 1차 PID에 관련된 부분 암호화된 데이타 스트림을 암호해독하고 디코드하며 2차 PID는 수정없이 무시한다. 암호화 시스템 B하에서 동작하는 STB는 1차 PID에 관련된 모든 암호화된 패킷은 무시하고 특정 채널에 관련된 2차 PID로 전송된 암호화된 패킷은 이용하도록 프로그램된다.

[0055] 그래서, 각각의 듀얼 부분 암호화된 프로그램은 그들과 연관된 2 세트의 PID를 가지고 있다. 설명한 바와 같이, 적절한 타임 슬라이스 간격을 갖는 것으로 도시된 시스템의 경우 암호화가 기간 단위(period-by-period basis)로 실행된다면, 암호해독을 하더라도 STB로 픽처를 볼 수 없을 것이다.

[0056] 도 6의 헤드엔드(322) 내의 이 시스템을 구현하기 위해서 SI 및 PSI는 제2 세트의 CA 디스크립터 정보를 포함하도록 수정될 수 있다. 레거시 셋톱박스는 알려지지 않은 CA 디스크립터를 취급할 수 없다. 결과적으로, 셋톱박스에서 대안으로 콘텐트 PID 및/또는 SI/PSI에 대한 레거시 CA PID와 ECM PID로부터의 오프셋을 "하드 코드"하는 것은 가능할 수 있다. 대안으로, 병렬 PSI도 전송될 수 있다. 예를 들어, 보조 PAT는 비-레거시 셋톱박스에 대해 PID 0 대신에 PID 1000으로 전달될 수 있다. 레거시 PAT내에서 발견되지 않은 보조 PMT를 참조할 수 있다. 보조 PMT는 비-레거시 CA 디스크립터를 포함할 수 있다. 보조 PMT는 레거시 셋톱박스에 알려지지 않았기 때문에 임의의 보간 이슈가 없을 것이다.

[0057] 시스템 A가 모토로라 또는 사이언티픽 애틀랜타에서 제작한 레거시 셋톱박스에 대응하는 경우의 시스템에서, STB에 대한 수정이 필요치 않다. 여기서 설명된 바와 같은 부분 암호화된 프로그램의 듀얼 캐리지에 대한 시스템 B 컴플라이언트 STB의 경우, 비디오 및 오디오 디코더는 단지 하나의 PID 대신에 2개의 PID 각각(1차 및 2차 PID)을 들을 수 있도록 적응되어 있다. 이용되는 비-레거시 CA 시스템의 수에 따라서 하나 이상의 2차 섀도우

(shadow) PID일 수 있지만, 특정 셋톱박스는 특정 STB에 의해 이용되는 CA 방법용으로 적절한 것으로 2차 PID들 중 하나를 들을 수 있다. 또한, 거의 클리어한 비디오 또는 오디오를 운반하는 PID로부터의 암호화된 패킷은 이상적으로 무시된다. "배드 패킷"(그 자체로 쉽게 디코드될 수 없는 것)을 무시하는 것은 많은 디코더들이 실행하는 기능일 수 있기 때문에, 수정이 요구되지 않는다. 배드 패킷을 무시하지 않는 디코더를 가지고 있는 시스템의 경우에, 필터링 기능이 이용될 수 있다. 타임 슬라이스 기술이 단지 비디오 및 오디오에만 적용될 수 있다는 것은 이해되어야 한다. 또한, 초기의 실시예에서와 같이 비디오는 타임 슬라이스 암호화될 수 있고 오디오는 이중 암호화된다. 타임 슬라이스 기술은 동시에 멀티플 프로그램들에 적용될 수 있다. 시간 간격 동안 암호화된 프로그램들의 수는 주소 대역폭 할당의 이슈이고, 본 예에서 한번 싱글 프로그램을 스크램블링하는 것에 대해 논의하고 있을지라도, 본 발명이 이에 의해 제한되는 것은 아니다. 이 명세서에서 설명된 암호화 기술들의 다른 조합도 본 기술 분야에 숙련된 자이면 가능할 것이다.

[0058] M번째 및 N 패킷 암호화

[0059] 본 발명에 상응하는 다른 실시예는 M번째 및 N 패킷 암호화라 칭하기로 한다. 이는 시스템(200)으로 도 3에 도시된 실시예의 변형이다. 이 실시예에서, 한 프로그램을 나타내는 각 PID의 패킷들은 이용자가 프로그램에 대한 돈을 지불하지 않은 경우는 프로그램의 보기를 방해하는 식으로 암호화된다. 이 실시예에서, M은 암호화 이벤트의 개시 간의 패킷 수를 나타낸다. N은 일단 암호화가 시작되면 행으로 암호화되는 패킷수를 나타낸다. N은 M 보다 작다. M=9이고 N=1이면, 9개의 패킷마다 암호화 이벤트 래스팅 1 패킷이 있다. M=16이고 N=2이면, 16개의 패킷마다 암호화 이벤트 래스팅 2 패킷이 있다. 듀얼 부분 암호화되는 각 패킷은 앞서의 실시예에서와 같이 CA 시스템 A(218) 및 CA 시스템 B(224)를 이용하여 복제되고 처리된다. 이 실시예와 앞서의 타임 슬라이스 기술 간의 동작에 있어서의 차이는 프로그램된 처리기의 제어하에 암호화를 위한 패킷의 선택을 실행하기 위한 스위치(216)의 동작에 있다.

[0060] 예로서, 이 예시적인 실시예에 따른 이중 암호화되는 프로그래밍의 9 채널을 가지고 있는 시스템을 고려하기로 한다. 이들 9개의 채널들은 9개의 프로그램중 특정한 하나에 연관된 패킷들을 식별하기 위해 패킷 식별자(PID)를 이용하여 디지털식으로 인코딩된다. 이 예에서, 이들 9개의 프로그램이 101-109 번호가 부여된 비디오 PID와 201-209 번호가 부여된 오디오 PID를 가지고 있다고 가정한다. 이 실시예에 따른 암호화는 다른 프로그램들로부터의 패킷들이 동시에 암호화될 수 있도록 랜덤한 프로그램 대 프로그램이다. 이는 아래의 표 2에 도시되어 있으며, 여기서 M=6이며 N=2이고 단지 비디오만이 암호화되나 이에 제한되는 것은 아니다. 이 방법은 콘텐트를 알고 있어야 할 필요는 없다. 표 2에서 PK1은 패킷 번호 1을 가리키고 PK2는 패킷 번호 2를 가리킨다.

표 2

프로그램	비디오	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
1	PID 101	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	...
2	PID 102	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	...
3	PID 103	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	...
4	PID 104	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	...
5	PID 105	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	...
6	PID 106	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	...
7	PID 107	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	...
8	PID 108	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	...
9	PID 109	EA	클리어	클리어	클리어	클리어	EA	EA	클리어	클리어	클리어	클리어	EA	...
1	PID 111	EB	EB					EB	EB					...
2	PID 112				EB	EB					EB	EB		...
3	PID 113			EB	EB					EB	EB			...
4	PID 114				EB	EB					EB	EB		...
5	PID 115			EB	EB					EB	EB			...
6	PID 116	EB					EB	EB					EB	...
7	PID 117	EB	EB					EB	EB					...
8	PID 118		EB	EB					EB	EB				...
9	PID 19	EB					EB	EB					EB	...

[0061]

[0062] 표 2의 예에서, 각 프로그램은 M=6 및 N=2 암호화 스킴을 이용하는 다른 것들과는 완전히 독립적으로 암호화된

다. 다시, 도시된 예는 단지 비디오만을 암호화하지만, 오디오 역시 이 배열 또는 다른 배열에 따라서 암호화될 수 있다. 비디오에만 적용한다면, 오디오는 이전 실시예에서와 같이 듀얼 스크램블되거나 타임 슬라이스 암호화될 수 있다. 대안적으로, 오디오에만 적용한다면, 비디오는 이전 실시예에서와 같이 타임 슬라이스될 수 있다.

[0063] 본 기술 분야에 숙련된 자이면 여기서 설명된 부분적 스크램블링 개념에 일치하게 이 기술에 대한 다른 많은 변형을 고안할 수 있을 것이다. 예를 들어, 5개의 클리어 그 다음은 2개의 암호화, 그 다음은 2개의 클리어, 그 다음은 하나의 암호화와 같은 패턴(CCCCCEECCECCCCCEECCE...)은 부분적 암호화 개념의 변형과 일치하며, M 및 N에 대한 램덤, 의사-램덤 및 세미-램덤 값들은 암호화를 위한 패킷들의 선택을 위해 이용될 수 있다. 패킷들의 랜덤, 의사-랜덤 또는 세미-램덤(여기서는 모두 "랜덤"이라 칭한다) 선택은 해커가 스크램블된 기록 콘텐트를 복구하려는 사후 처리 시도시 패킷을 알고리즘식으로 재구성하는 것을 어렵게 해준다. 본 기술 분야에 숙련된 자이면 후에 설명되는 부분적 암호화의 다른 실시예에 이 정보를 적용하는 방법을 이해할 것이다. 실시예들 중 어떤 것들은 콘텐트를 보다 효과적으로 보안하는 조합으로 이용될 수도 있다.

[0064] 데이타 구조 암호화

[0065] 본 발명의 실시예들에 상응하는 다른 부분적 암호화 방법은 암호화를 위한 기준으로서 데이타 구조를 이용한다. 예로서, 암호화에 이용하기에 편리한 하나의 데이타 구조는 MPEG 비디오 프레임이다. 이는 아래 표 3에 도시되어 있다(비디오전용으로). 이 표에서, 10개의 비디오 프레임 마다 암호화된다. 이 실시예에서, 각 프로그램의 10 프레임 암호화 사이클은 다른 채널과 구별되지만, 이 개념에 제한되는 것은 아니다. 이 개념은 M=10 및 N=1를 가지고 있는 예시적인 실시예에서 비디오 또는 오디오 프레임(또는 어떤 다른 데이타 구조)을 기반한 타임 슬라이스 또는 M번째 및 N 부분적 암호화 배열(또는 다른 패턴)의 변형으로 볼 수 있다. 물론, M 및 N의 다른 값들은 유사한 실시예에서 이용될 수 있다. 표 3에서, F1은 프레임 번호 1을 가리키며, F2는 프레임 번호 2를 가리킨다.

표 3

프로그램	비디오	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
1	PID 101	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	...
2	PID 102	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
3	PID 103	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
4	PID 104	클리어	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
5	PID 105	클리어	클리어	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	...
6	PID 106	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	...
7	PID 107	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	...
8	PID 108	클리어	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	...
9	PID 109	EA	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	클리어	EA	클리어	...
1	PID 111	EB										EB		...
2	PID 112				EB									...
3	PID 113			EB										...
4	PID 114					EB								...
5	PID 115				EB									...
6	PID 116	EB										EB		...
7	PID 117		EB										EB	...
8	PID 118		EB										EB	...
9	PID 119	EB										EB		...

[0066]

[0067] 그래서, 각각의 암호화된 프로그램은 그와 관련된 2 세트의 PID를 가지고 있다. 설명된 바와 같이, 암호화가 기간 단위로 실행된다면, 도시된 시스템의 경우 픽쳐는 근본적으로 볼 수 없게 된다. 도시된 바와 같이 초당 30 프레임인 9개의 프로그램 시스템의 경우 대략 초당 3 프레임이 암호화될 것이다. 프로그램을 볼 수 있는 자격을 부여받지 않은 뷰어들의 경우, 그들의 STB는 일정하게 동기 및 복원을 시도하기 때문에 STB는 임시의 고정 프레임(occasional frozen frame) 보다 많은 것을 획득할 수 없을 것이다. 프로그래밍에 가입한 뷰어들은 프로그래밍을 쉽게 볼 수 있을 것이다. 그러한 암호화 배열에 대한 대역폭 비용은 암호화에 적용되는 주파수(frequency)에 따른다. 상기 예에서, 데이타의 1/9 엑스트라 팩터(extra factor)는 각 프로그램에 대해 전송된

다. 이 예에서, 대략 한 프로그램에 상당하는 대역폭이 이용된다. 프로그램의 수가 많으면 많을 수록 프로그램당 암호화되는 패킷 수는 작아지게되고, 암호화 시스템의 보안은 다소 열화될 수 있다. 랜덤식 M 및 N 방법에 있어서와 같이, 랜덤 프레임들이 선택될 수 있다. 비디오의 경우에 랜덤 프레임을 선택하게 되면 모든 프레임 종류 즉, 내부 코딩된 프레임(I 프레임), 예측 코딩된(P 프레임), 양방향 코딩된(B 프레임) 및 DC 프레임이 영향받는다는 것은 당연하다.

[0068] 본 발명의 변형에 있어서, 허용가능한 보안 레벨을 달성하기 위해 적은 패킷을 암호화하는 것도 가능할 수 있다. 즉, 9 프로그램의 시스템의 경우에 허용가능한 보안 레벨을 달성하는데는 초당 1프레임만을 암호화해도 좋다. 그러한 시스템에서, 오버헤드는 프로그램 마다 초당 하나의 암호화된 기간이 되거나 오버헤드로 전송된 데이타의 대략 1/30이 된다. 이러한 레벨의 오버헤드는 2개의 암호화 시스템하에서 암호화의 풀 듀얼 캐리지에 관련된 대역폭의 50% 손실에 비해 상당히 개선된 것이다. 본 발명의 다른 변형에 있어서, 허용가능한 보안 레벨을 달성하기 위해 단지 특정 비디오 프레임만을 암호화하는 것도 가능하다. 예를 들어, MPEG 콘텐트의 경우, 대역폭 오버헤드는 더 줄이고 허용가능한 보안 레벨을 그대로 유지하기 위해 단지 내부 코딩된 프레임(I 프레임)만을 스크램블할 수 있다. 이들은 풀 듀얼 캐리지에 요구되는 대역폭에 비해 상당한 개선을 제공한다.

[0069] 크리티컬 패킷 암호화

[0070] 대역폭 이용에 있어서의 실질적인 효율은 선택적 패킷 단위 이중 암호화 기술(a selective packet-by-packet dual encryption technique)을 이용하여 달성할 수 있다. 이 기술에서는, 프로그램 콘텐트의 오디오 및/또는 비디오의 적절한 디코딩에 대한 중요성에 기초하여 암호화를 위한 패킷이 선택된다.

[0071] 이 실시예는 패킷들중 적은 단편만을 스크램블하여 암호화된 콘텐트의 풀 듀얼 캐리지에 비교해서 대역폭 요구조건을 감소시킬 수 있다. 클리어 패킷들은 두개의(또는 그 이상의) 듀얼 캐리지 PID 간에 공유된다. 한 양호한 실시예에서, 이하 설명되듯이, 전체 콘텐트 대역폭의 약 1 퍼센트가 덜 이용된다. 레거시 암호화 스킴을 갖고 있는 시스템의 경우, 클리어 프로그램 콘텐트 패킷들은 레거시 및 새로운 셋톱박스에 의해 수신된다. 앞서 언급한 바와 같이, 암호화된 패킷들은 적절한 CA를 갖고 있는 각각의 셋톱박스에 의해 듀얼 운반되어 처리된다. 각 CA 시스템은 오소고널(orthogonal)이다. 키 공유는 요구되지 않으며 다양한 키 에포치(epoch)는 각 CA 시스템에 의해 이용될 수 있다. 예를 들어, 모토로라 소유인 암호화를 갖는 시스템은 내장된 보안 ASIC를 이용하여 빠른 변경 암호화 키를 생성하는 한편, NDS 스마트 카드 기반 시스템은 약간 느린 변경 키를 생성한다. 이 실시예는 사이언티픽 애틀랜타 및 모토로라 레거시 암호화에도 동일하게 잘 작동된다.

[0072] 도 6을 참조해 보면, 프로그래밍의 부분들이 패킷단위로 이중 암호화되는 본 발명의 한 실시예에 상응하는 시스템의 블록도는 시스템(300)으로 도시되어 있다. 이 시스템에서, 각 프로그램의 패킷들은 예를 들어 레거시 CA 시스템 A 및 새로운 CA 시스템 B를 이용하여 이중 암호화한다. 암호화되는 패킷들은 비디오 및/또는 오디오 스트림의 적절한 디코딩에 대한 중요성에 따라서 선택된다.

[0073] 도 6에 도시된 시스템에서, 케이블 시스템 헤드엔드(322)는 암호화를 위한 패킷 선택기(316)에서 A/V 콘텐트(304) 패킷을 선택한다. 암호화를 위해 선택된 패킷들은 프로그램의 실시간 디코딩 및 기록 콘텐트의 임의 가능한 후 처리(post processing)에 심각한 영향을 끼칠 것이다. 즉, 크리티컬 패킷들만이 암호화된다. 비디오 및 오디오에 대해서, 이는 PES(패킷화된 엘리멘터리 스트림) 헤더 및 페이로드의 일부로서의 다른 헤더를 포함하고 있는 "프레임의 스타트" 전송 스트림 패킷들을 암호화함으로써 달성되며, 이 정보 없이는 STB 디코더가 MPEG 압축된 데이타를 압축해제할 수 없다. MPEG2 스트림은 전송헤더 내에 "패킷 유닛 스타트 인디케이터"를 가지고 있는 "프레임의 스타트" 패킷들을 식별한다. 일반적으로, 한 그룹의 픽쳐 헤더 또는 비디오 시퀀스 헤더를 포함하고 있는 페이로드를 운반하는 패킷들은 본 스크램블링 기술을 실시하는데 이용될 수 있다.

[0074] MPEG(동화상 전문가 그룹) 컴플라이언트 압축된 비디오는 엘리멘터리 데이타 스트림을 약간 조정가능한 188 바이트 데이타의 페이로드인 전송 스트림으로 다시 패키지한다. 이와 같이, PES 헤더를 포함하고 있는 전송 스트림 패킷들은 선택기(316)에서 암호화를 위해 선택되어 CA 시스템 A 암호화기(318) 및 CA 시스템 B 암호화기(324)에 의해 이중 암호화된다. 듀얼 부분 암호화되는 패킷들은 복제되고 암호화기(324)에 의해서 암호화된 복제 패킷들의 PID는 330에서 이전 실시예에서와 같이 2차 PID에 다시 맵핑된다. 나머지 패킷들은 클리어하게 통과된다. 클리어 패킷들, 시스템 A 암호화된 패킷들, 시스템 B 암호화된 패킷들, 시스템 정보(328) 및 329로부터의 PSI는 케이블 시스템(32)를 통해 방송될 수 있게 멀티플렉스된다.

[0075] 이전 시스템에서와 같이, 레거시 STB(36)은 클리어 데이타 및 CA 암호화 시스템 A에 의해 암호화된 데이타를 수신하고, CA 암호해독 A(40)에 의해 암호해독된 데이타와 결합된 암호화되지 않은 데이타를 그의 디코더로 투명

하게 통과시킨다. 새로운 STB(336)에서, 프로그램은 1차 및 2차 PID에 할당된다. 1차 PID를 가지고 있는 클리어 패킷은 수신되어 디코더로 전달된다. 1차 PID를 가지고 있는 암호화된 패킷은 버려진다. 2차 PID를 가지고 있는 암호화된 패킷은 암호해제되고 디코딩을 위해 (예를 들어 패킷을 1차 PID에 리맵핑함으로써) 데이타 스트림과 재결합된다.

[0076] 예로서 비디오가 이용되는 경우, 각 샘플은 프레임으로 알려져 있고 이 샘플 레이트는 통상 초당 30 프레임이다. 샘플들이 3.8 Mbps로 맞추어지도록 인코딩되면, 각 프레임은 127K 비트의 대역폭을 차지할 것이다. 이 데이타는 프레임 데이타의 바디를 처리하라는 명령들에 이용되는 헤더를 포함하는 각 프레임의 제1 패킷(들)을 가지고 있는 188 바이트의 패킷으로 MPEG 전송을 위해 슬라이스된다. 제1 헤더 패킷(1504 부가 비트)을 이중 암호화하는 것은 단지 1.2%(1504/127K)의 부가적인 대역폭을 요구한다. 고해상도(19 Mbps) 스트림의 경우, 퍼센티지가 더 작아진다.

[0077] 앞서 설명한 바와 같이, PES 헤더를 포함하는 전송 스트림 패킷들은 본 발명에 따른 암호화를 위한 우선 목표이다. 이들 패킷들은 시퀀스 헤더, 시퀀스 신장 헤더, 픽쳐 헤더, 동일 패킷 내에 속하는 양자화 및 다른 디코드 표를 포함하고 있다. 이들 패킷들이 디코드될 수 없다면(즉 가입 요금을 지불함이 없이 승인되지 않은 프로그램을 보기 위해 시도하는 해커에 의해서도 디코드될 수 없다면), 이 프로그램의 작은 부분 조차도 볼 수 없을 것이다. 일반적으로, 공지된 디코더 집적회로는 비디오 및 오디오와 같은 엘리멘터리 스트림에 실시간으로 동기시키기 위해 PES 헤더를 이용하기 때문에 이 프로그램에 동조하려는 어떠한 시도도 오디오 없는 블랭크 스크린과 마주치게 될 것이다. PES 헤더를 암호화함으로써, 비승인된 셋톱박스내의 디코딩 엔진은 시작조차할 수 없다. 예를 들어, 저장된 콘텐트에 대한 후 처리 공격도 PES 헤더를 포함하는 패킷 내의 정보를 동적으로 변경함으로써 퇴치된다. 본 기술 분야에 숙련된 자이면 본 발명의 이 실시예의 구현을 위해 본 발명을 벗어나지 않고도 비승인된 보기를 금지시킬 수 있는 암호화에 대한 다른 크리티컬 또는 중요한 패킷 또는 콘텐트 요소들이 식별될 수 있다는 것은 이해하고 있을 것이다. 예를 들어, MPEG 내부 코딩 또는 I 프레임 픽쳐 패킷들은 이 프로그램의 비디오 부분의 보기를 금지하기 위해 암호화될 수 있다. 본 발명의 실시예들은 예를 들어 랜덤, M번째 및 N은 물론이고 PES 헤더를 포함하는 패킷을 스크램블링하는 것 또는 다른 패킷들의 데이타 구조 암호화와 같은 다른 실시예와의 임의 조합으로 이용될 수 있다. 크리티컬 패킷 암호화는 비디오 암호화에 적용할 수 있는 한편 다른 방법은 오디오에 적용할 수 있다. 오디오는 예를 들어 이중 암호화될 수 있다. 본 발명의 범위내의 다른 변형들은 본 기술 분야에 숙련된 자이면 충분히 실행할 수 있을 것이다.

[0078] 도 7은 도 6의 헤더(322)에서 이용될 수 있는 것과 같은 예시적인 인코딩 처리를 보여주는 흐름도이다. 전송 스트림 패킷이 350에서 수신될 때, 패킷이 암호화를 위한 선택 기준에 부합하는지 여부를 알기 위해 패킷을 검사한다. 양호한 실시예에서, 이러한 선택 기준은 패킷 페이로드의 일부로서의 PES 헤더의 존재이다. 패킷이 이 기준에 부합하지 않으면, 패킷은 354에서 출력 데이타 스트림내로의 삽입을 위해 캐리어 암호화되지 않은 패킷(C)으로서 통과된다. 패킷이 이 기준에 부합하면, 358에서 CA 암호화 시스템 A하에서 암호화되어 암호화된 패킷 EA가 생성된다. 이 패킷은 또한 362에서 CA 시스템 B하에서 복제되고 암호화되어 암호화된 패킷이 생성된다. 암호화된 패킷은 366에서 2차 PID에 맵핑되어 암호화된 패킷 EB가 생성된다. 암호화된 패킷 EA 및 EB는 354에서 클리어 패킷 C와 함께 출력 데이타 스트림내로 삽입된다. 양호하게는 EA 및 EB 패킷은 데이타의 시퀀스가 거의 동일하게 유지되도록 싱글 오리지널 패킷이 얻어진 데이타 스트림 내의 위치에 삽입된다.

[0079] 354로부터의 출력 데이타 스트림은 도 6의 336과 같은 CA 암호화 시스템 B에 따른 STB에서 수신될 때, 도 8의 처리와 같은 (도 5의 처리와 유사한) 처리는 프로그램을 암호해독 및 디코드하는데 이용될 수 있다. 370에서 1차 또는 2차 PID를 가지고 있는 패킷이 수신될 때, 이 패킷이 클리어(C)인지 또는 370에서 시스템 A(EA)하에서 암호화된 것인지 또는 374에서 시스템 B(EA)하에서 암호화된 것이지 여부에 대한 결정이 이루어진다. 패킷이 클리어이면, 직접 디코더(378)로 통과된다. 어떤 실시예에서는, 2차 패킷의 전 또는 후의 1차 패킷의 상대 위치가 스트림내의 대체를 위한 1차 패킷을 신호하는데 이용될 수 있다. 1차 패킷의 스크램블링 상태의 체크는 명시적으로 요구되지 않는다. 패킷이 EA 패킷이면, 380에서 드롭된다. 패킷이 EB 패킷이면, 384에서 암호해독된다. 이 때, 2차 PID 패킷 및/또는 1차 PID 패킷은 388에서 동일한 PID에 다시 맵핑된다. 암호해독된 패킷 및 클리어 패킷은 378에서 디코딩된다.

[0080] 앞서 설명한 듀얼 부분적 암호화 배열은 풀 듀얼 캐리지를 위해 요구되는 것에 비해서 대역폭 필요조건을 상당히 감소시켜준다. PES 헤더 정보를 암호화하는 것은 비디오 및 오디오를 안전하게 유지하는데 효과적이면서도 2 이상의 CA 시스템들이 동일 케이블 시스템 상에 독립적으로 "공존"할 수 있게 해준다. 레거시 시스템 A 셋톱박스는 영향받지 않으며, 시스템 B 셋톱박스는 각각 비디오 및 오디오용인 두개의 PID에 대한 청취를 위해서는 단지 마이너 하드웨어, 펌웨어 또는 소프트웨어 강화만을 필요로 한다. 각 유형의 STB, 레거시 및 비-레거시는

그의 고유 CA 방법을 보유하고 있다. 헤드엔드 수정은 암호화를 위한 콘텐트를 선택하는데, 제2 암호화기를 도입하고 합성 출력 스트림내로의 결합을 믹스하기 위한 수단을 제공하는데 제한되어 있다.

[0081] 한 실시예에서, 헤드엔드 장비는 크리티컬 PES 헤더만이 아니고 대역폭이 허용하는 만큼 콘텐트를 상황에 맞게 스크램블링하도록 구성된다. 이들 부가의 스크램블된 패킷은 비디오/오디오 프레임 전체를 통해 PES 페이로드 또는 다른 패킷 내에 존재하게 되므로 콘텐트의 좀 더 나은 보안이 제공된다.

[0082] SI 암호화

[0083] 도 9를 보면, 부가 대역폭을 최소화하는 시스템의 한 실시예가 시스템(400)으로 도시되어 있다. 이 실시예에서, 시스템은 셋톱박스가 프로그래밍을 동조하는데 시스템 정보(SI)(428)가 요구된다는 장점을 취하고 있다. 케이블 시스템에서, SI는 노멀한 뷰잉 채널에서 벗어난(set aisde) 주파수에서 대역외(out-of-band) 전송된다. 이것을 대역 내로 전송하는 것도 가능하다. 대역 내로 전송된다면, SI(428)는 복제되고 각 스트림으로 전송된다. 논의를 위해, 이전의 제조업자로부터의 "레거시" 셋톱박스에 전달된 SI가 STB(436)과 같은 새로운 제조업자로부터의 셋톱박스에 전달된 SI와 분리된다고 가정하기로 한다. 결과적으로, SI의 각 버전은 조건적 억세스 시스템 A(418) 및 조건적 억세스 시스템 B(424)를 이용하여 도시된 바와 같이 독립적으로 스크램블될 수 있다. 클리어 비디오(404) 및 클리어 오디오(406)는 클리어로 전달되지만, 이들을 어떻게 찾아야 하는지를 이해하기 위해서는 SI 정보(428)가 필요하다.

[0084] SI는 채널 이름에 대한 정보, 및 각 채널에 대한 주파수 동조 정보는 물론이고 프로그램명 및 시작 시간 등과 같은 프로그램 가이드 정보를 전달한다. 디지털 채널들은 함께 멀티플렉스되어 특정 주파수로 전달된다. 본 발명의 실시예에서, SI 정보는 암호화되어 승인된 셋톱박스만이 이용할 수 있다. 모든 A/V 주파수의 위치를 알려주는 SI 정보가 수신되지 않으면 동조가 이루어지지 않는다.

[0085] 셋톱박스를 프로그램할 수 있는 해커가 주파수를 스캔하는 것을 저지하기 위해서 채널에 대한 주파수는 표준 주파수로부터 오프셋될 수 있다. 또한, 주파수는 매일, 매주 또는 다른 주기나 랜덤 기반으로 동적으로 변경될 수 있다. 통상적인 케이블 헤드엔드는 대략 30개의 주파수를 이용할 수 있다. 각 주파수는 통상적으로 서로, 다른 것들 간에, 지상 방송 신호들 간에 그리고 수신 장비의 클럭에 의해 이용되는 주파수들 간에 간섭이 생기지 않게 선택된다. 각 채널은 이용되는 경우 간섭이 생기지 않게 하거나 이웃 채널들의 주파수가 변경되게 하지 않는 적어도 하나의 독립적 교번 주파수를 가지고 있다. 실제로 가능한 주파수 맵은 2^{30} 또는 1.07×10^{9} 이다. 그러나 해커는 30개 정도의 채널 각각에 대한 주파수에 간단하고 신속하게 동조시도를 할 수 있다. 콘텐트를 가지고 있는 주파수를 찾는데 성공한 경우, 해커의 셋톱박스는 프로그램을 구성하는 각 PID에 대해 알기 위하여 PSI(429)를 분석할 수 있다. 해커는 "프로그램 1"은 "CNN" "프로그램 2"는 "TNN", 등 이라는 것을 아는데 어려움을 가지고 있을 것이다. 이 정보는 SI와 함께 전송되고, 이는 앞서 설명한 바와 같이 스크램블되어 있어 비-승인된 셋톱박스에 이용할 수 없다. 그러나, 끈질긴 해커는 각각을 선택해서 전달된 콘텐트를 검사하여 이들을 알아낼 수도 있다. 그래서 채널들의 식별을 좌절시키기 위해 싱글 스트림내에 한 프로그램의 할당을 예를 들어 "프로그램 1"이 "TNN"이고 "프로그램 5가 "CNN"이 되도록 상기 예에서 교환된 프로그램 2 및 프로그램 5 주위로 이용할 수 있다. 또한, 프로그램을 완전히 새로운 프로그램 그룹핑을 가지고 있는 완전히 다른 스트림으로 이동시키는 것이 가능하다. 통상의 디지털 케이블 헤드엔드는 뮤직을 포함해서 250개의 콘텐트 프로그램을 전달할 수 있다. 각각은 고유하게 동조된다. 재순서화를 위한 가능한 조합은 250!(팩토리얼)이다. 전달된 SI 또는 해커에 의해 제공된 콘텐트의 맵없이는, 이용자는 프로그램이 흥미있는 것인지 여부를 알기 위해 스트림내의 각 프로그램을 랜덤하게 선택하게 된다.

[0086] 그래서, 헤드엔드(422)에서는 비디오 신호(404) 및 오디오 신호(406)가 클리어(암호화됨이 없이)하게 제공되는 한편 SI(428)는 케이블 네트워크를 통한 전달을 위해 CA 시스템에 제공된다. 그래서, 예시적인 시스템(400)에서는 클리어 SI(428)가 암호화 시스템 A를 이용하여 SI 데이타를 암호화하는 암호화 시스템(418)에 제공된다. 동시에, 클리어 SI(428)는 암호화 시스템 B를 이용하여 SI 데이타를 암호화하는 암호화 시스템(424)에 제공된다. 클리어 비디오(404), 오디오(406), 및 PSI(429)는 이후 대역외 시스템 정보(428)를 대체하기 위해 418(SI A)로부터 암호화된 SI와 424(SI B)로부터 암호화된 SI와 함께 멀티플렉스된다.

[0087] 케이블 시스템(32)을 통한 분배 후에, 비디오, 오디오, PSI, 시스템 정보 A 및 시스템 정보 B는 모두 셋톱박스(36 및 436)에 전달된다. STB(36)에서, 암호화된 SI는 CA 시스템 A(40)에서 암호해독되어 동조 정보가 셋톱박스에 제공된다. 셋톱박스는 특정 프로그램을 동조시켜 텔레비젼 세트(44)에 디스플레이되게 해준다. 유사하게, STB(436)에서, 암호화된 SI는 CA 시스템 B(440)에서 암호해독되어 동조 정보가 셋톱박스에 제공되어

특정 프로그램이 동조되어 텔레비젼 세트(444)에 디스플레이될 수 있게 한다.

[0088] 이러한 접근법의 장점은 콘텐트 전달 시스템, 예를 들어, 케이블 시스템에 부가의 A/V 대역폭이 요구되지 않는다는 것이다. SI만이 듀얼 운반된다. 특정 하드웨어가 요구되지 않는다. 표준 주파수로부터의 임의 오프셋 주파수는 대부분의 튜너에 의해 용이하게 수용될 수 있다. SI 암호해독은 소프트웨어로 수행될 수 있거나 하드웨어에 의해 지원될 수 있다. 예를 들어, 레거시 모토로라 셋톱박스는 디코더 IC 칩에 내장된 하드웨어 암호해독기를 이용하여 모토로라 대역외로 전달된 SI를 암호해독하는 능력을 가지고 있다.

[0089] 결단성있는 해커는 A/V 채널이 위치한 곳을 알아내기 위해 동축 케이블에 대해 스펙트럼 분석기를 이용할 수도 있을 것이다. 또한, 해커가 비교적 느린 처리로 A/V 채널들이 위치해 있는 곳을 알아내기 위해 주파수를 자동-스캔하기 위한 셋톱박스를 프로그램하는 것도 가능할 것이다. A/V 채널 주파수가 동적으로 변경된다면, 이는 해커가 대역을 일정하게 분석하거나 스캔해야하기 때문에 해커를 좌절시킬 수 있다. 또한, 프로그램 번호와 할당된 PID는 변할 수 있다. 그러나, 주파수, 프로그램 번호 및 PID를 동적으로 변경시키면 서비스 제공자, 예를 들어, 케이블 오퍼레이터가 연산 어려움에 직면하게 될 수 있다.

[0090] 일반화된 표현

[0091] 상기 기술들 각각은 일반적으로 도 10의 시스템(500)으로 표현될 수 있다. 시스템(500)은 케이블 시스템 헤드엔드(522)를 가지고 있고, 이 헤드엔드는 클리어 비디오(504), 클리어 오디오(506), SI(528), 및 PSI(529)를 포함하며, 이들은 인텔리전트 처리기 제어 스위치(518)를 통해서 선택적으로 스위치되며, 이 스위치(518)은 (PID 할당 또는 재할당을 요구하는 실시예에서) PID를 조건적 억세스 시스템 A(520) 또는 조건적 억세스 시스템 B(524)에 할당하거나 또는 케이블 시스템(32)에 클리어로 통과시키는 역할을 한다. 앞서와 같이, 레거시 CA 시스템 A에 따라서 암호화된 프로그램 또는 SI는 STB(36)에 의해서 적절하게 디코드될 수 있다. CA 시스템 B 암호화된 정보는 앞서 설명한 바와 같이 STB(536)에 의해 이해된 후 암호해독되고 디코드된다.

[0092] PID 맵핑 고려

[0093] 앞서 설명된 PID 맵핑 개념들은 필요에 따라서 본 명세서에 설명된 듀얼 부분적 암호화 기술들에 일반적으로 적용할 수 있다. 케이블 헤드엔드에서, 일반적인 개념은 암호화를 위해 선택된 패킷들이 복제되도록 패킷들의 데이타 스트림이 조정된다는 것이다. 이 패킷들은 2개의 개별 암호화 방법하에 복제되고 암호화된다. 복제된 패킷들에는 개별 PID(이들 중 하나는 클리어 콘텐트를 위해 이용된 레거시 CA PID를 매치시킨다)가 할당되고, 케이블 시스템을 통한 전송을 위한 데이타 스트림으로 오리지널 선택된 패킷의 위치에 다시 삽입된다. 케이블 시스템 헤드엔드의 출력에서, 레거시 암호화된 패킷과 동일 PID를 가지고 있는 클리어 패킷을 갖고 있는 패킷 스트림이 나타난다. 2차 PID는 새로운 암호화 시스템하에서 암호화된 패킷을 식별한다. 헤드엔드에서 발생하는 PID 맵핑이외에도, MPEG 패킷들은 패킷들의 적절한 시퀀스가 유지되도록 연속 카운터를 이용한다. 적절한 디코딩이 보장되도록 하기 위해, 이러한 연속 카운터가 헤드엔드에서 패킷화된 데이타 스트림의 생성 동안 적절하게 유지돼야만 한다. 이는 각 PID를 가지고 있는 패킷들이 노멀한 식으로 순차적으로 연속 카운터들에 할당되게 함으로써 달성된다. 그래서 2차 PID를 가지고 있는 패킷들은 1차 PID의 패킷들로부터의 개별적인 연속 카운터를 운반한다. 이는 아래에 간단한 형식으로 보여주고 있으며, 여기서 PID 025는 1차 PID이고 PID 125는 2차 PID이며, E는 암호화된 패킷을 나타내고, C는 클리어 패킷을 나타내며, 마지막 번호는 연속 카운터를 나타낸다.

[0094]

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

[0095] 이러한 예시적인 패킷의 세그먼트에서, PID 025를 가지고 있는 패킷들은 그 자신의 연속 카운터 (04, 05, 06, 07, 08, 09,...) 시퀀스를 가지고 있다. 유사하게, 2차 PID 125를 가지고 있는 패킷들은 또한 그 자신의 연속 카운터 (11, 12,...)의 시퀀스를 가지고 있다.

[0096] STB에서, PID들은 2차 PID를 가지고 있는 패킷들을 올바른 프로그램에 바르게 관련시키기 위한 여러 방식으로 조정될 수 있다. 한 구현예에서, 아래 예시된 입력 스트림 세그먼트의 패킷 헤더:

[0097]

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

[0098] 는 다음과 같은 출력 스트림 세그먼트가 생성되도록 조정된다:

[0099]

125C04	025E11	125E05	125C06	125C07	125C08	125C09	025E12	125E10

[0100] 출력 스트림내의 1차 PID(025)는 클리어 패킷(C)에 대한 2차 PID(125)로 대체된다. 암호화된 패킷의 경우, 1차 PID와 2차 PID는 유지되지만 연속 카운터는 교환된다. 그래서, 2차 PID를 이용하는 패킷들의 스트림은 연속성의 손실에 의한 에러 발생없이 적절하게 암호화되어 디코드된다. PID를 조정하는 다른 방법들, 예를 들어, 스크램블된 레거시 패킷에 대한 PID(125)를 NOP PID(모든 PID) 또는 디코딩되지 않은 다른 PID 값에 맵핑하는 방법이 이용될 수 있고, 연속 카운터들 또한 본 발명에 따른 실시예들에 이용될 수 있다.

[0101] 1차 및 2차 PID는 프로그램 특정 정보(PSI) 데이타 스트림의 일부로서 전송된 프로그램 맵 테이블(PMT)로 STB들에 전달된다. 2차 PID의 존재는 CA 암호화 시스템 A("레거시" 시스템)하에서 동작하는 STB에 의해 무시되도록 설정될 수 있지만, CA 암호화 시스템 B하에서 동작하는 새로운 STB는 1차 PID에 연관된 프로그램의 암호화된 부분을 전달하는데 2차 PID가 이용되어 있음을 인식할 수 있게 프로그램되어 있다. 이러함 암호화 스킴이 PMT의 "루프용" 오디오 엘리멘터리 PID내에 CA 디스크립터의 존재에 의해서 이러함 암호화 스킴이 이용되고 있다는 사실이 셋톱박스에 알려지게 된다. 통상적으로 "루프용" 비디오 엘리멘터리 PID내의 CA 디스크립터와 "루프용" 오디오 엘리멘터리 PID내의 다른 CA 디스크립터가 있다. CA 디스크립터는 CA_PID를 ECM PID 또는 부분적 스크램블링에 이용되는 2차 PID를 식별하는데 개인용 데이타 바이트를 이용하고, 싱글 프로그램에 관련된 1차 및 2차 PID를 찾기 위해 시스템 B하에서 STB 동작이 설정된다. 전송 헤드내의 PID 필드는 길이가 13 비트이므로, 2^{13} 또는 8,192 PID가 이용가능하며, 필요에 따라 2차 PID용으로 스페어 PID가 이용될 수 있다.

[0102] 각각의 프로그램 컴포넌트 또는 그의 선택된 부분에 대한 PID의 할당 이외에도, 새로운 PID는 2차 암호화 기술에 이용된 태그 ECM 데이타에 할당될 수 있다. 할당된 각각의 PID 번호는 레거시 STB의 방해 동작을 방지하기 위해 사용자 정의된 스트림 타입으로서 표기될 수 있다. MPEG는 사용자 정의된 데이타 스트림 타입들에 대한 그러한 번호들의 예비된 블록을 정의한다.

[0103] 개념적으로는 케이블 헤드엔드에서의 PID 맵핑은 간단한 동작인 반면, 실제로 케이블 헤드엔드 장비는 종종 미리 설치되어 있으므로, 설치된 케이블 시스템에 대한 분열을 최소화하면서 효율적인 비용으로 이 임무를 달성하도록 수정된다. 그래서, 케이블 시스템 헤드엔드내의 실제 구현의 세부사항은 어느 정도는 헤드엔드내에 존재하는 실제 레거시 하드웨어에 의존한다. 이의 예는 이하 좀 더 상세히 설명하기로 한다.

[0104] 헤드엔드 구현

[0105] 본 기술 분야에 숙련된 자이면 도 2, 3, 6, 9 및 10에 관련된 상기 설명들이 성격에 있어서 약간은 개념적이며 본 발명의 다양한 실시예에 관련된 전반적인 아이디어와 개념을 설명하기 위해 이용되는 있다는 것을 이해할 것이다. 본 발명의 실제 구현을 이해하는데 있어서, 본 기술 분야에 숙련된 자이면 중요한 실제 경쟁 이슈가 설치된 케이블 사업자측에서 기존의 레거시 헤드엔드 장비내에 다양한 부분적 암호화의 비용에 있어서 효율적인 구현을 제공하는 것이라는 사실을 알고 있을 것이다. 예로서 두개의 1차 레거시 케이블 시스템을 취해서 케이블 헤드엔드에서 상기 기술들이 어떻게 구현될 수 있는지를 이하 설명하기로 한다.

[0106] 먼저, 모토로라 브랜드인 조건적 억세스 시스템을 이용하는 케이블 시스템 헤드엔드를 고려하기로 한다. 그러한 시스템에서, 도 11에 도시된 수정들은 부분적 이중 암호화 구현을 위해 비용에 있어서 효과적인 메카니즘을 제공하기 위해 실행될 수 있다. 통상의 모토로라 시스템에서, HIT(스카이 내의 헤드엔드) 또는 유사한 데이타 피드가 위성으로부터 제공된다. 이 피드는 케이블 제공자에게 제공되어, 모토로라 집적 수신기 트랜스코더(IRT) 모델 IRT 1000 및 IRT 2000, 및 모토로라 모듈러 처리 시스템(MPS)과 같은 수신기/디스크램블러/스크램블러 시스템(604)에 의해 수신되는 집합된 디지털 콘텐트를 제공한다. 디지털 텔레비젼 데이타의 클리어 스트림은 수신기/디스크램블러/스크램블러 시스템(604)의 위성 디스크램블러 기능 블록(606)으로부터 얻어질 수 있다. 이러한 클리어 스트림은 패킷 선택기/듀플리케이터(610)로 도시된 새로운 기능 블럭에 의해 조정될 수 있다. 이러한 새로운 블록(610)은 프로그램된 처리기로서 구현될 수 있거나 또는 하드웨어, 소프트웨어, 또는 이들의 조합으로 구현될 수도 있다.

[0107] 패킷 선택기/듀플리케이터(610)는 상기 부분 이중 암호화 방법중 임의의 방법하에서 이중 암호화될 수 있다. 이후 이들 패킷은 이들이 후에 암호화를 위해 식별될 수 있도록 새로운 PID로 복제된다. 예를 들어, 특정 프로그램에 관련된 610의 입력에서 패킷들이 PID A를 가지고 있다면, 패킷 선택기/듀플리케이터(610)는 암호화될 패킷들을 식별하고 이들 패킷을 복제한 후에 이들을 PID B 및 C에 각각 리맵핑한다. 그 결과 이들은 후에 두개의 서로 다른 시스템하에서 암호화를 위해 식별될 수 있다. 양호하게는, 복제 패킷들은 이들이 (하나의 패킷이 데이타 스트림내에 이전에 상주해 있는 두개의 패킷을 제외하고) 원래 제공되어 있는 것과 동일한 순서로 유지되

도록 PID B 및 C를 가지고 있는 원래 복제된 패킷의 위치에 서로 인접한 데이타 스트림내로 삽입된다. 부가될 새로운 CA 시스템이 NDS이 암호화라고 가정하기로 한다. 이 경우에, PID A는 클리어 패킷을 나타내고, PID B는 NDS 암호화된 패킷을 나타내며, PID C는 모토로라 암호화된 패킷을 나타낼 것이다. PID B를 가지고 있는 패킷들은 610내의 포인트에서 NDS 암호화하에서 암호화되거나 후에 암호화될 수 있다.

[0108] PID B 및 C를 가지고 있는 패킷들은 시스템(604)에 복귀하고, 이 시스템에서는 PID C를 가지고 있는 패킷이 모토로라 장비에 관련된 제어 시스템(614)이 지시한대로 케이블 스크램블러(612)에서 모토로라 암호화하에 암호화된다. 케이블 스크램블러(612)로부터의 출력 스트림은 다른 새로운 디바이스 즉 PID 리맵퍼 및 스크램블러(620)로 진행하고, 이 스크램블러(620)는 612로부터 출력 스트림을 수신하고 PID A 내지 PID C를 가지고 있는 나머지 패킷들을 리맵핑하고 제어 시스템(624)의 제어하게 NDS 암호화 알고리즘하에서 PID B 패킷을 암호화한다. 626에서 출력 스트림은 PID C를 가지고 있는 클리어 암호해독된 패킷과 PID B를 가지고 있는 NDS 암호화 시스템하에서 암호화된 패킷과 함께 PID C를 가지고 있는 모토로라 암호화 시스템하에서 복제되고 암호화된다. 이 스트림은 628에서 케이블 시스템을 통한 분배를 위해 변조된다(예를 들어, 구형 진폭 변조 및 RF 변조). 양호한 실시예는 레거시 프로그램 특정 정보(PSI)내에서 호출된 오디오 및 비디오 PID가 가는 방향이 정확하기 때문에 PID C에 대한 스크램블된 패킷들을 매칭시키기 위해 PID A에 대한 암호화되지 않은 패킷들을 맵핑한다. 제어 컴퓨터, 스크램블러, 및 레거시 셋톱박스만이 PID C에 대해 알고있다. 대안적으로, PID C에 대한 스크램블된 패킷들은 다시 PID A에 맵핑될 수 있지만, 이는 PID 리맵퍼 및 스크램블러(620)에서 PID C로부터의 PID 번호를 PID A에 맵핑하기 위해 자동으로 발생된 PSI를 편집하는 것을 의미할 것이다.

[0109] 상기 예에서, PID 리맵퍼 및 스크램블러(620)은 또한 PSI 정보를 디멀티플렉스하여 (PMT내의 CA 디스크립터의 이용을 통해) NDS 암호화의 부가를 반영하기 위해 수정하고, 수정된 PSI 정보를 다시 데이타 스트림으로 멀티플렉스한다. NDS 암호화를 지원하는 ECM도 PID 리맵퍼 및 스크램블러(620)에서 데이타 스트림내로 삽입될 수 있다(또는 패킷 선택기/듀플리케이터(610)에 의해 삽입될 수도 있다).

[0110] 그래서, 모토로라 장비를 이용하여 NDS 암호화(또는 다른 암호화 시스템)를 케이블 시스템 헤드엔드에 부가하기 위하여, 패킷들이 위성 디스크램블러로부터의 데이타 스트림으로 다시 맵핑된다. 다시 맵핑된 PID는 이후 각 CA 시스템하에서 스크램블되는 패킷들을 식별하는데 이용된다. 일단 레거시 시스템 암호화가 실행되면, 클리어 PID는 이후 레거시 시스템내의 클리어 및 암호화된 패킷들이 동일 PID(또는 PID들)을 공유하도록 다시 맵핑된다. 620에서와 같은 PID 리맵핑 및 610에서와 같은 패킷 복제 선택 및 복제는 애플리케이션 특정 집적회로 또는 프로그램가능 로직 디바이스 또는 필드 프로그램가능 게이트 어레이와 같은 주문형 또는 반주문형 집적회로, 또는 프로그램된 처리기를 이용하여 구현될 수 있다. 다른 구현들도 본 발명을 벗어남이 없이도 가능하다.

[0111] 도 12는 사이언티픽 애틀랜타 기반의 케이블 헤드엔드에서 본 발명의 부분적 이중 암호화를 구현하는데 이용된 것과 같은 유사한 장비 구성을 도시하고 있다. 이 실시예에서, HIT 피드 또는 유사한 것은 위성 디스크램블러(706)를 내장하고 있는 IRD(704)에서 수신된다. 이는 단지 위성 디스크램블러 기능만이 이용가능한 모토로라 IRT 또는 MPS일 수 있다. 위성 디스크램블러(706)의 출력은 다시 암호화될 패킷들을 선택하는 새로운 선택기/듀플리케이터(710)에 의해 조정될 수 있는 클리어 데이타 스트림을 제공하고, 이들을 복제한 후 복제 패킷들의 PID를 새로운 PID에 맵핑한다. 다시, 예를 들어, 클리어로 유지하기 위한 패킷들에는 PID A가 할당되고, 새로운 시스템(예를 들어, NDS)하에서 암호화될 패킷들에는 PID B가 할당되고, 사이언티픽 애틀랜타 암호화 시스템하에서 암호화될 패킷들에는 PID C가 할당된다. PID B를 가지고 있는 패킷들은 이때 NDS 암호화 시스템하에서 암호화될 수 있다.

[0112] 패킷들의 스트림은 이후 멀티플렉서(712)(예를 들어, 사이언티픽 애틀랜타 멀티플렉서)에 전송되고, 이 멀티플렉서에서 PID C를 가지고 있는 패킷들이 멀티플렉서(712)에 관련된 제어 시스템(718)의 제어하에 사이언티픽 애틀랜타 암호화 시스템(714)에 의해 암호화된다. 데이타 스트림은 이후 멀티플렉서(712)내의 QAM 복조기(720)에 제공된다. 이들 패킷을 적절하게 리맵핑하기 위하여, 멀티플렉서(712)의 출력에서 QAM 변조된 신호는 새로운 처리기 시스템(724)에 제공되고, 이 시스템에서는 QAM 변조된 신호가 QAM 복조기(730)에서 복조되고, 클리어 PID A 패킷들은 제어 시스템(738)의 제어하에 PID 리맵퍼(734)에서 PID C에 다시 맵핑된다. NDS 암호화 알고리즘에 의한 암호화는 710에서 보다는 오히려 여기서 실행될 수 있다. 리맵핑된 PID 및 듀얼 부분적 암호화를 가지고 있는 데이타 스트림은 이후 케이블 시스템을 통한 분배를 위해 742에서 QAM 및 RF 변조된다.

[0113] 상기 예에서, PID 리맵퍼 및 스크램블러(734)는 또한 PSI 정보를 복조하고, NDS 암호화의 부가(CA 디스크립터를 PMT에 부가하는 것)를 반영하기 위해 복조된 정보를 수정하고 수정된 PSI 정보를 다시 데이타 스트림으로 멀티

플렉스한다. NDS 암호화를 지원하는 ESM은 또한 PID 리맵퍼 및 스크램블러(734)에서 데이타 스트림내로 삽입될 수 있다(또는 패킷 선택기/듀플리케이터(710)에 의해 삽입될 수도 있다). 734에서와 같은 PID 리맵핑 및/또는 734에서와 같은 스크램블링, 각각 730 및 742에서와 같은 QAM 복조 및 QAM 변조, 그리고 710에서와 같은 패킷 선택 및 복제는 프로그램된 처리기를 이용하거나 또는 특정 애플리케이션 집적 회로 또는 프로그램가능 로직 디바이스 또는 필드 프로그램가능 게이트 어레이와 같은 주문형 또는 반주문형 집적회로를 이용하여 구현할 수 있다. 다른 구현들도 본 발명을 벗어남이 없이 가능하다.

[0114] 본 발명의 상기 실시예는 레거시 스크램블링 장비가 원하는 패킷만을 전체 엘리멘터리 스트림 대신 엘리멘터리 스트림으로 스크램블할 수 있게 해준다. 엘리멘터리 스트림의 특정 패킷의 스크램블링은 스크램블되지 않을 패킷 예를 들어 PID A에 대해 PID 번호를 이용함으로써 달성된다. 스크램블될 패킷은 PID C에 배치될 것이다. 스크램블링 장비는 PID C상의 패킷들(스크램블링을 위해 선택된 것들)을 스크램블한다. 스크램블링이 실행된 후에, 스크램블되지 않은 패킷들은 스크램블된 패킷과 동일한 것에 맵핑된 PID 번호를 갖는다. 즉 PID A는 PID C가 된다. 레거시 셋톱박스는 스크램블된 패킷과 스크램블되지 않은 패킷을 가지고 있는 엘리멘터리 스트림을 수신한다.

[0115] 이들 실시예에서의 패킷들은 스트림으로 처리된다. 전체 스트림은 스크램블링을 위해 레거시 스크램블링 장비에 전송된다. 이는 패킷들 모두를 정확한 타임 동기 순서로 유지한다. 패킷들이 스트림으로부터 추출되어 레거시 스크램블링 장비에 전송되었다면, 타임 지터(jitter)가 도입될 수 있다. 본 실시예는 모든 패킷을 스트림으로 유지시킴으로써 이 문제를 해결한다. 이 실시예는 이 장비가 PID A로부터 PID C까지의 패킷들의 리맵핑에 관련되어 있지 않기 때문에 레거시 스램블링 장비 제공자의 협조를 요하지 않는다. 이러한 리맵핑은 레거시 스크램블링 시스템에 의해 생성된 PSI로부터 호출된 PID가 변경될 필요가 없기 때문에 바람직하다. 레거시 시스템은 PID C에 대해서 알고 있지만 PID A에 대해서는 모른다. 레거시 스크램블링 장비에 의해 스크램블될 전체 엘리멘터리 스트림은 스크램블링 시스템이 스크램블하도록 지시받은 싱글 PID로 발견된다.

[0116] 상기 예에서, 제2 암호화 시스템으로서의 NDS의 이용은 제한적인 것으로 간주되어서는 안된다. 더욱이, 두개의 널리 사용되는 모토로라 및 사이언티픽 애틀랜타의 시스템은 예로 든 것이고 PID 리맵핑 및 듀얼 부분적 암호화를 허용하는 레거시 시스템에 대한 수정이 이용될 수도 있다. 일반적으로, 앞서 설명된 기술은 도 13에 800으로 기술된 처리를 포함한다. 피드는 806에서 수신되고 이는 810에서 디스크램블되어 패킷들의 클리어 데이타 스트림이 생성된다. 814에서는 원하는 부분적 이중 암호화 기술에 따라서 패킷들(예를 들어, 단지 오디오만, PES 헤더를 포함하고 있는 패킷, 등)이 선택된다. 818에서는 선택된 패킷들이 복제되고 복제 쌍들이 두개의 새로운 PID(예를 들어, PID B 및 PID C)에 다시 맵핑된다. 복제된 패킷들은 이후 822에서 PID를 기반으로 암호화된다(즉, PID C는 레거시 암호화에 따라 암호화되고 PID B는 새로운 암호화 시스템에 따라서 암호화된다). 클리어 패킷들(예를 들어, PID A)은 이후 826에서 레거시 암호화된 PID(PID C)와 동일한 PID에 다시 맵핑된다.

[0117] 도 13의 처리의 요소들중 어떤 요소들이 실행되는 순서는 이용될 특정의 이중 암호화 배열을 수용하도록 수정되는 특정 레거시 시스템에 따라서 변할 수 있다. 예를 들어, 새로운 암호화 시스템 하에서의 암호화는 도 11 및 12에 도시된 바와 같이 복제시에 실행되거나 또는 레거시 패킷들의 리맵핑시에 실행될 수 있다. 부가적으로, 다양한 복조 및 변조 동작들은 특정 레거시 시스템을 즉시 수용하기 위한 필요에 따라서 실행될 수 있다(도 13에는 도시안됨).

[0118] 셋톱박스 구현

[0119] 여러 개의 셋톱박스 구현은 본 발명의 범위내에서 가능하다. 암호화를 위한 패킷들을 선택하기 위해 헤드엔드에서 이용된 방법은 STB와는 무관하다.

[0120] 그러한 하나의 구현이 도 14에 도시되어 있다. 이 실시예에서, 튜너 및 복조기(904)로부터의 패킷들은 디코더 회로(908)의 디멀티플렉서(910)에 제공된다. 이들 패킷은 (예로, 일정한 메모리 아키텍처를 이용하여) 메모리(912)내로 버퍼되어 ROM 메모리(920)내에 저장된 소프트웨어를 이용하는 STB의 메인 CPU(916)에 의해 처리된다.

[0121] 선택된 PID는 PVR(Personal Video Recorder) 애플리케이션에서 HDD(hard disk drive)로의 전송을 준비하기 위해 요구되는 초기 처리와 유사하게 STB의 PID 필터를 통한 인입 전송으로부터 분리되어 암호해독된 후 SDRAM(Synchronous Dynamic Random Access Memory)에 버퍼된다. 호스트 CPU(916)는 이후 불필요한 PID를 포함하고 있는 패킷들의 제거를 위해 SDRAM내에 버퍼된 데이타를 "매뉴얼식으로" 거른다. 이러한 처리에는 몇 몇 분명한 부작용이 있다.

[0122] 호스트 오버헤드는 CPU 대역폭의 약 1%인 것으로 평가된다. 최악의 경우에, 이는 15 Mbit/S 비디오 스트림에

대한 40 K 바이트/S와 같다. 이러한 감소는 기껏해야 각 패킷의 4 바이트가 평가되고 위치가 188 바이트 간격에 있어서 간섭 데이타가 고려되지 않기 때문에 가능하다. 그러므로, SDRAM내의 각 패킷 헤더는 간단한 메모리 포인터 조정을 통해서 직접 억세스될 수 있다. 부가적으로, 패킷들은 블록으로 캐시(cache)되고 덩어리로 평가되므로 호스트의 태스크 스위칭이 감소된다. 이는 각각의 새로운 패킷의 수신시에 다른 태스크에 대한 방해를 제거할 것이다. 이는 캐시를 채우기 위한 시간을 허용하는 채널 변경시 스트림의 디코드를 시작하기 위한 대기 시간을 증가시켜준다. 이는 할당된 SDRAM 캐시 버퍼 사이즈에 따라 무시될 수 있다.

[0123] SDRAM 버퍼에서 호스트 필터된 패킷들은 기존의 하드웨어 DMA 처리를 통해서 A/V 큐에 전송되고 이는 PVR 구현과 유사하다. 필터된 패킷들은 이후 디코딩을 위한 디코더(922)에 제공된다.

[0124] 셋톱박스내의 제2 구현 기술은 도 15에 도시되어 있다. 디코더 회로(930)내의 RISC 처리기 A/V 디코더 모듈(934)은 부분적 전송 PID 및 디코드를 위한 스트라이프/컨케티네이트(concatenate)를 처리하기 때문에, 디코더 IC(930)내의 펌웨어는 각 패킷 헤더내의 기준에 근거해 부분적 전송 스트림내의 개별 패킷들이 배제되도록 변경될 수 있다. 대안적으로, 디멀티플렉서(910)는 패킷들을 배제하도록 설계될 수 있다. 레거시 스크램블된 패킷(들)은 암호화된 CA 모듈을 통해서 통과한다. 레거시 스크램블된 패킷들을 제거하기 위해 디코더 IC(930)를 이용하고, 새로운 암호화 알고리즘(예를 들어, NDS)으로 암호화된 패킷들이 레거시 암호화된 패킷에 아주 인접해(또는 적어도 차기의 1차 스트림 비디오 패킷 전에) 있다고 가정할 때 효과적으로 레거시 패킷을 제거하면 싱글 클리어 스트림을 헤더 스트립 및 비디오 큐내로 합체하는 것이 달성된다.

[0125] 셋톱박스내의 부분적 암호해독의 제3 구현 기술은 도 16에 도시되어 있다. 이 실시예에서, PID 맵핑은 ASIC(Application Specific Integrated Circuit), 필드 프로그램가능 게이트 어레이(FPGA)와 같은 회로내에서 또는 튜너 및 복조기(904)와 디코더 IC(908)간에 배치된 프로그램가능 로직 디바이스(PLD)(938) 또는 다른 주문형 설계 회로내에서 실행될 수 있다. 이 실시예에 대한 변형에서, 디코더 IC(908)은 디멀티플렉서(940)내의 PID 리맵핑을 구현하기 위해 수정될 수 있다. 어느 경우에도, 레거시 암호화된 패킷들은 드롭되고, 비-레거시 패킷들은 회로(938) 또는 디멀티플렉서(940)에서 리맵핑된다.

[0126] 이러한 제3 기술은 도 17에 도시된 PLD를 이용하는 한 실시예에서 구현될 수 있다. 이 구현은 행으로 나타나는 특정 PID의 하나 이상의 암호화된 패킷이 없다는 것을 가정하며, 그러한 가정하에서 이 구현은 앞서 설명한 M 및 N번째 암호화 배열을 가지고 있는 것과 같은 암호화 패킷의 버스트를 수용하도록 수정될 수 있다(이는 나중에 설명될 것이다). 입력 스트림은 PID를 근거로 입력 스트림을 멀티플렉스하는 PID 식별자(950)을 통해 통과한다. 1차 PID 패킷은 958에서 연속 클럭된다. 연속 에러가 검출되면, 이 에러는 메모되고 카운터는 960에서 리셋된다.

[0127] 오리지널 입력 패킷 스트림은 많은 PID로 태그된 패킷들을 포함하고 있다. PID 식별자(950)는 모든 다른 패킷들로부터 당해 두개의 PID(1차 및 2차 PID)을 갖고 있는 패킷들을 분리한다. 이 능력은 멀티플 PID 쌍들을 처리할 수 있도록 나누어질 수 있다. 이들 다른 패킷들은 수정된 출력 스트림으로 직접 바이패스된다. 이러한 처리에는 3 또는 4 바이트의 클럭킹 지연이 따른다.

[0128] 2차 PID를 갖고 있는 패킷들은 PID 식별자(950)에 의해서 연속 카운트 체커(954)로 루트되고, 이 체커는 이 PID를 위한 시퀀스 보전을 확증해준다. 임의 에러는 956에서 메모되지만, 에러에 대한 구체적인 처리는 본 발명을 이해하는데는 관련이 없다. 패킷의 연속 값은 뒤따르는 패킷들의 시퀀스 체킹에 이용을 위해 보존된다. 대응하는 연속 체크(958)는 독립적인 1차 카운터를 이용하여 1차 PID를 갖고 있는 패킷들에 대해 실행되며, 다시 임의 에러가 960에서 메모된다.

[0129] 2차 패킷은 962에서 2차 프래크(flag)에 대해 체크된다. 이러한 불린 인디케이터(Boolean indicator)는 마지막 클리어 패킷 이후로 2차 패킷들이 처리되었는지를 상기하는데 이용된다. 클리어 패킷들간의 하나 이상의 2차 패킷은 이 실시예에서는 에러이고 964에서 메모된다. 2차 패킷의 존재는 966에서 2차 플래그를 설정함으로서 상기된다.

[0130] 2차 패킷의 연속 카운터는 968에서 클리어 패킷들의 시퀀스에 맞추어지도록 변경된다. 이러한 대체를 위한 데이타는 958에서 1차 스트림의 연속성을 입증하는데 이용된 값으로부터 나온다. 개정된 패킷은 968로부터 전송되어 출력 스트림을 형성하는 개정된 스트림내로 합체된다.

[0131] 1차 PID를 갖고 있는 패킷들의 연속성이 958에서 체크된 후에, 이들은 헤더내의 스크램블링 플래그에 의해 970에서 구별된다. 패킷이 스크램블되어 있는지 1차 플래그가 974에서 질의받는다. 이 1차 플래그 불린 인디케이터는 1차 암호화된 패킷이 마지막 클리어 패킷 이후로 처리되었는지를 상기하는데 이용된다. 클리어 패킷들간

의 하나 이상의 암호화된 1차 패킷은 이 실시예에서는 에러이고 976에서 메모된 후에 이 패킷은 978에서 버려진다. 암호화된 1차 패킷의 존재는 980에서 1차 플래그를 설정함으로써 상기된다. 1차 암호화된 패킷에 대한 다운스트림 컨슈머가 없는 경우 978에서 버려질 수 있다. 어떤 경우에 패킷이 연속되는 것이 필요할 수도 있다(이 경우에, 그의 연속 카운터는 버려진 2차 연속 값을 이용할 수 있다).

[0132] 970에서의 1차 PID 스크램블 테스트가 클리어 패킷을 검출하면, 2차 및 1차 플래그의 상태가 984에서 테스트된다. 암호화된 패킷들은 매칭된 쌍들내로 들어가야하기 때문에 유효 조건들이 설정될 수도 설정되지 않을 수도 있다. 하나의 시퀀스는 예외없이 988에서 에러로 메모된다. 그러나, 출현 순서는 이 실시예에서 일관성이 없다. 전송 헤더내의 스크램블링 비트, 예를 들어, 전송_프라이어리티(transport_priority) 비트와는 다른 삭제를 위한 1차 패킷을 플래그하는 다른 방법들이 있을 수 있다. 또한, 대체를 위한 인디케이터로서 2차 패킷 전 또는 후에 임의 비트를 이용하는 것, 예를 들어 1차 패킷의 간단한 위치 정보를 이용하는 것은 전혀 가능하지 않다.

[0133] 1차 PID를 가지고 있는 클리어 패킷들의 PID 값은 개정된 출력 스트림으로 출력되기 전에 2차 PID로 992에서 변경된다. 대안적으로, 2차 PID 패킷들은 1차 PID 값에 리맵핑될 수 있다. 콘텐트를 디코딩하기 위한 올바른 PID(1차 또는 2차 PID)가 디코더에 제공될 때 콘텐트가 디코딩될 수 있다. 클리어 패킷의 존재는 1차 및 2차 불린 플래그를 클리어시킨다.

[0134] 제안된 모든 실시예에서, 2차 패킷은 일련의 1차 패킷들이 대체를 위해 태그될 때 조차도 대체될 1차 패킷에 인접하게 삽입될 수 있다. 그러나, 어떤 경우에는, 멀티플 암호화된 패킷들이 중재 2차 패킷없이 스트림내로 삽입될 수 있다면 헤드엔드 부분적 스크램블링을 실시할 수 있다. (M번째 및 N 부분적 암호화 방법에서와 같이) 다중 연속 암호화된 패킷을 수용하기 위하여, 1차 및 2차 패킷의 이용은 카운터 매칭 테스트 기능으로 대체될 수 있다. 그러므로, 구성 요소 962, 964 및 966 대신에 2차 암호화된 패킷 카운터를 증가시킬 수 있다. 구성 요소 970, 974, 976 및 980 대신에, 1차 암호화된 패킷 카운터를 증가시킬 수 있다. 구성 요소 984는 동일 수의 암호화된 패킷이 1차 및 2차 경로에서 수신되는 것을 공고히 하기 위해 1차 및 2차 암호화된 패킷 카운터의 비교로 대체될 수 있다. 992에서 플래그를 클리어하는 대신에, 카운터들이 클리어된다. 이러한 변형을 이용하여, 멀티플 암호화된 패킷들이 연속해서 수신될 수 있고 수신된 번호는 데이타 스트림의 보전 상태를 모니터하기 위해 비교된다. 다른 변형도 본 기술 분야에서 숙련된 자이면 실행할 수 있을 것이다.

[0135] 도 17을 참조해서 앞서 설명한 기능은 소비자용 셋톱박스에 이용된 상업적으로 구입가능한 브로드컴 시리즈 70xx 또는 71xx 디코더의 기능과 유사한 기능을 하는 A/V 디코더 칩내로 통합될 수 있다. 도 18은 상업화된 칩내에 제공된 기능들이 근본적으로 변경될 수 없는 그러한 디코더 칩에 대한 블록도이다. 일반적으로 상업화된 디코더 칩들은 PID와 프로그램 콤포넌트(예를 들어, 오디오 또는 비디오)들 간에 1대1 대응이 있는 것으로 예상한다.

[0136] 도 18에 도시된 디코더는 1차 및 2차 PID가 메인 오디오, 메인 비디오 및 픽쳐-인-픽쳐(PiP) 기능에 이용된 2차 비디오용으로 다루어지도록 STB 중앙 처리기에 대한 접속을 통해서 멀티플 PID가 디코더내로 프로그램될 수 있게 해준다. 이 실시예에서, 생(raw) 데이타 스트림은 PID를 근거로 패킷들의 스트림을 디멀티플렉스하기 위해 앞서 도 17과 연관해서 설명된 것과 유사한 기능을 제공하는 패킷 소터(1002)에 의해 수신된다. 양호하게는, 도 18의 디코더는 프로그램된 소프트웨어 보다는 하드 와이어 로직 회로를 이용하여 1002의 PID 소팅 기능을 실행한다. 프로그램 가이드 및 스트림 네비게이션 정보는 예를 들어 STB의 메인 처리기가 이용할 수 있게 출력된다. 메인 오디오 프로그램에 관련된 패킷들은 FIFO(1006)내로 버퍼되고, 디스크립터(1010)에서 암호해독된 후에 MPEG 오디오 디코더가 필요할 때마다 검색할 수 있게 1014에서 버퍼된다. 디코딩된 MPEG 오디오는 이후 디코더로부터 출력으로서 제공된다.

[0137] 유사한 방식으로, 메인 비디오 프로그램에 관련된 패킷들은 FIFO(1024)에서 버퍼되고, 디스크립터(1028)에서 암호해독되고, 이후에 MPEG 비디오 디코더(1036)가 필요할 때마다 검색할 수 있게 1032에서 버퍼된다. 메인 채널에 대한 디코딩된 MPEG 비디오는 합성기(1040)에 제공되고 나서 디코더로부터의 출력으로서 제공된다. 유사하게, 픽쳐-인-픽쳐 비디오에 관련된 패킷들은 FIFO(1044)에서 버퍼되고, 디스크립터(1048)에서 암호해독되고 나서 MPEG 비디오 디코더(1056)가 필요할 때마다 검색할 수 있게 1052에서 버퍼된다. 픽쳐-인-픽쳐 채널용의 디코딩된 MPEG 비디오는 컴포지터(1040)에 제공되어 메인 채널 비디오와 결합된후 디코더로부터의 디코딩된 비디오 출력으로서 제공된다. 메인 또는 픽쳐-인-픽쳐 채널에 관련이 없는 다른 패킷들은 버려진다. 물론, 다른 기능들이 본 발명의 실시예들로부터 벗어남이 없이 디코더 칩내에 합체될 수 있거나 또는 삭제될 수 있다.

[0138] 결론

[0139] 앞서 언급한 바와 같이, 끊임없는 해커의 공격을 퇴치하기 위해, 여러 개의 부분적 암호화 배열들을 조합해서 보안을 좀 더 강화시킬 수 있다. 예를 들어, 크 리티컬 패킷 암호화는 보안이 좀 더 강화되도록 SI 암호화, M 번째 및 N, 랜덤 암호화, 타임 슬라이스, 및 다른 기술과의 임의 결합으로 이용될 수 있다. 한 실시예에서, 대역폭이 이용가능한 만큼 많은 패킷들이 암호화될 수 있다. 암호화의 양은 카운터가 레귤러 프로그램인지 또는 프리미엄(예를 들어, 페이-퍼-뷰 또는 VOD)인지에 따라서, 그것이 성인용 프로그램인지 또는 일반적인 무비인지에 따라서, 그리고 다양한 케이블 오퍼레이터가 운영하는 것이 편하다고 느끼는 보안 레벨에 따라서 다를 수 있다. 본 기술 분야에 숙련된 자이면 본 발명을 벗어나지 않고도 암호화의 보안을 강화하기 위해 많은 다른 결합들이 가능하다는 것을 이해할 것이다.

[0140] 본 발명은 앞서 다양한 실시예에서 설명한 바와 같이, MPEG2 코딩을 이용하는 디지털 A/V 시스템의 관점에서 설명되었다. 그래서, 구체적으로 논의된 다양한 패킷 이름들과 프로토콜은 MPEG 2 코딩 및 디코딩에 관련되어 있다. 그러나, 본 기술 분야에 숙련된 자이면 본 명세서에서 개시되고 주장되고 있는 개념들이 제한적으로 해석되어서는 안된다는 것은 이해하고 있을 것이다. MPEG 2 프로토콜에 대한 제한없이 동일하거나 유사한 기술이 임의의 디지털 케이블 시스템에서 사용될 수 있다. 더욱이, 본 기술은 예를 들어 지상 방송 기반의 콘텐트 전달 시스템, 인터넷 기반의 콘텐트 전달, 예로 패키지 미디어(예를 들어, CD 및 DVD)는 물론이고 DirecTV™ 시스템과 같은 위성 기반의 콘텐트 전달 시스템을 포함하는 임의의 적절한 콘텐트 전달 시나리오에 이용될 수 있다. 이들 다양한 대안들은 이 명세서의 목적에 동등한 것으로 간주되며, 예시적인 MPEG 2 케이블 구현은 설명의 목적을 위해 제시된 예시적인 실시예로서 고려되어야만 한다.

[0141] 또한, 본 발명은 텔레비젼 셋톱박스를 이용하는 부분적 암호화된 텔레비젼 프로그램을 디코딩하는 관점에서 설명되었다. 그러나 본 디코딩 메카니즘은 STB 또는 MP3 플레이어와 같은 뮤직 플레이어를 필요로 하지 않고 텔레비젼 수신기내에서 동등하게 구현될 수 있다. 그러한 실시예들은 동등한 것으로 간주된다.

[0142] 또한, 본 발명은 텔레비젼 프로그램의 듀얼 부분적 암호화를 위한 메카니즘을 제공하는데 암호화 기술을 이용하는 관점에서 설명된 한편, 이들 부분적 암호화 기술은 싱글 암호화 기술로서 이용될 수 있거나 또는 제한없이 두개 이상의 암호화 시스템하에서 멀티플 암호화를 위해 이용될 수도 있다. 2 이상의 암호화 시스템은 암호화되는 부가의 복제 패킷을 수용하게 될 것이다. 대안적으로, 복제 패킷들중 하나에 대한 암호화 키는 멀티플 암호화 시스템들 간에 공유될 수 있다. 부가적으로, 텔레비젼 프로그램의 암호화 목적에 대해 구체적으로 설명되었을지라도, 본 발명은 인터넷 또는 다른 네트워크를 통한 다운로드용 콘텐트에 제한없이 뮤직 콘텐트, 패키지 미디어 콘텐트 및 다른 종류의 정보 콘텐트를 포함하는 다른 콘텐트의 싱글 또는 이중 암호화를 위해 이용될 수 있다. 그러한 콘텐트는 본 발명의 범위를 벗어남이 없이도 퍼스널 디지털 어시스턴트(PDA)에 제한됨이 없이 퍼스널 컴퓨터, 퍼스널 뮤직 플레이어, 오디오 시스템, 오디오/비디오 시스템, 등을 포함하는 임의 수의 재생 디바이스에 의해 플레이될 수 있다.

[0143] 본 기술 분야에 숙련된 자이면 본 발명이 프로그램된 처리기의 이용에 의해 실현될 수 있는 예시적인 실시예의 관점에서 설명되었다. 그러나, 본 발명은 설명되고 청구된 발명과 동등한 특정 목적 하드웨어 및/또는 할당된 처리기와 같은 하드웨어 컴포넌트를 이용하여 구현될 수 있기 때문에 본 발명이 앞서의 설명에 제한되는 것은 아니다. 유사하게, 범용 컴퓨터, 마이크로프로세서 기반의 컴퓨터, 광학 컴퓨터, 아날로그 컴퓨터, 할당된 처리기 및/또는 할당된 하드 와이어드 로직은 본 발명의 대안적인 동등한 실시예들을 구성하는데 이용될 수 있다.

[0144] 본 기술 분야에 숙련된 자이면 앞서 언급한 실시예들을 구현하는데 이용된 프로그램 시스템 및 관련 데이타가 본 발명을 벗어남이 없이 예를 들어 판독 전용 메모리(ROM) 디바이스, 랜덤 억세스 메모리(RAM), 광학 저장 요소, 자기 저장 요소, 광자기 저장 요소, 플래시 메모리, 코어 메모리 및/또는 다른 등가의 저장 기술과 같은 다른 유형의 저장장치는 물론이고 디스크 저장장치를 이용하여 구현될 수 있다는 것을 이해할 것이다. 그러한 대안적인 저장 장치들은 동등한 것으로 간주된다.

[0145] 본 명세서에서 설명된 바와 같은 본 발명은 임의 적절한 전자 저장 매체에 저장되거나 임의 적절한 전자 통신 매체를 통해 전송될 수 있는, 앞서 플로우 차트로 설명된, 프로그래밍 명령을 수행하는 프로그램된 처리기를 이용하여 구현될 수 있다. 그러나, 본 기술 분야에 숙련된 자이면 앞서 설명된 처리는 본 발명의 범위를 벗어나지 않는 한 임의 다수의 변형으로 또는 많은 적절한 프로그래밍 언어로 구현될 수 있다는 것을 이해할 것이다. 예를 들어, 실행되는 특정 동작들의 순서는 종종 변할 수 있으며, 부가 동작들이 부가되거나 삭제될 수 있다. 본 발명을 벗어남이 없이 에러 트래핑(trapping)이 부가될 수 있고 및/또는 강화될 수 있으며 이용자 인터페이스 및 정보 표현에서 변경이 있을 수 있다. 그러한 변경들은 등가인 것으로 고려되고 간주된다.

[0146] 본 발명이 특정 실시예를 들어 설명되었을지라도, 본 기술 분야에 숙련된 자이면 앞서의 설명으로부터 많은 대안, 수정, 교환 및 변경을 할 수 있을 것이란 것은 자명하다. 따라서 이러한 대안, 수정 및 변경들은 첨부된 특허청구범위에 속하는 것으로 보아야한다.

도면의 간단한 설명

[0147] 신규한 것으로 간주되는 본 발명의 특징은 특히 첨부된 특허청구범위에 기술되어 있다. 그러나 본 발명의 목적 및 장점과 함께 구조 및 동작 방법에 관한 본 발명 그 자체는 도면을 참조로 기술되어 있으며 특정한 예시적인 실시예를 기술하고 있는 본 발명의 상세한 설명을 참조함으로써 잘 이해할 수 있을 것이다.

[0148] 도 1은 종래의 조건적 억세스 케이블 시스템의 블록도이다.

[0149] 도 2는 이중 암호화된 오디오가 클리어한 비디오와 함께 전송되는 본 발명의 한 실시예에 상응하는 시스템의 블록도이다.

[0150] 도 3은 프로그래밍의 부분들이 타임 슬라이스 메카니즘에 따라서 이중 암호화되는 본 발명의 실시예에 상응하는 시스템의 블록도이다.

[0151] 도 4는 본 발명의 특정 실시예에 상응하는 이중 암호화 처리의 흐름도이다.

[0152] 도 5는 본 발명의 특정 실시예와 상응하는 암호해독 처리의 흐름도이다.

[0153] 도 6은 프로그래밍의 부분들이 패킷 기반으로 이중 암호화되는 본 발명의 실시예에 상응하는 시스템의 블록도이다.

[0154] 도 7은 본 발명의 특정 실시예에 상응하는 이중 암호화 처리의 흐름도이다.

[0155] 도 8은 본 발명의 특정 실시예에 상응하는 암호해독 처리의 흐름도이다.

[0156] 도 9는 시스템 정보가 암호화되고 프로그래밍이 클리어로 전송되는 본 발명의 실시예에 상응하는 시스템의 블록도이다.

[0157] 도 10은 본 발명의 다양한 실시예에 상응하는 일반적 시스템의 블록도이다.

[0158] 도 11은 케이블 시스템 헤드엔드 내의 본 발명의 실시예에 상응하는 암호화 시스템의 제1 구현 실시예의 블록도이다.

[0159] 도 12는 케이블 시스템 헤드엔드 내의 본 발명의 실시예에 상응하는 암호화 시스템의 제2 구현 실시예의 블록도이다.

[0160] 도 13은 케이블 시스템 헤드엔드 내의 본 발명의 특정 실시예들을 구현하는데 이용된 전반적인 암호화 처리의 흐름도이다.

[0161] 도 14는 본 발명의 실시예들에 상응하는 디코딩 시스템의 셋톱박스 구현의 제1 실시예의 블록도이다.

[0162] 도 15는 케이블 시스템 STB내의 본 발명의 실시예들에 상응하는 디코딩 시스템 구현의 제2 실시예의 블록도이다.

[0163] 도 16은 케이블 시스템 STB내의 본 발명의 실시예들에 상응하는 디코딩 시스템 구현의 제3 실시예의 블록도이다.

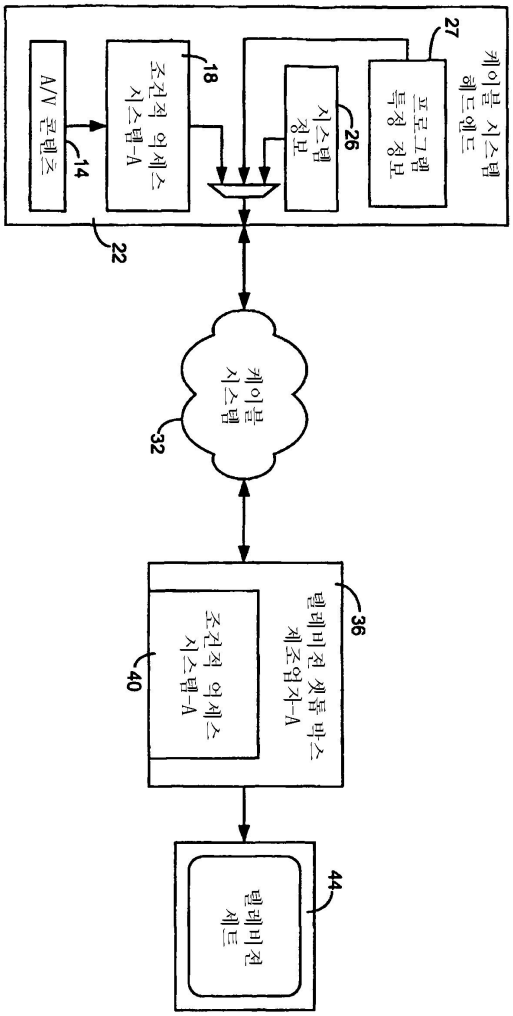
[0164] 도 17은 셋톱박스 PID 리-맵퍼(re-mapper)의 한 실시예에서 실행된 PID 리맵핑 처리를 보여주는 도면이다.

[0165] 도 18은 본 발명에 상응하는 텔레비젼 셋톱 박스에 이용될 수 있는 예시적인 디코더 칩의 블록도이다.

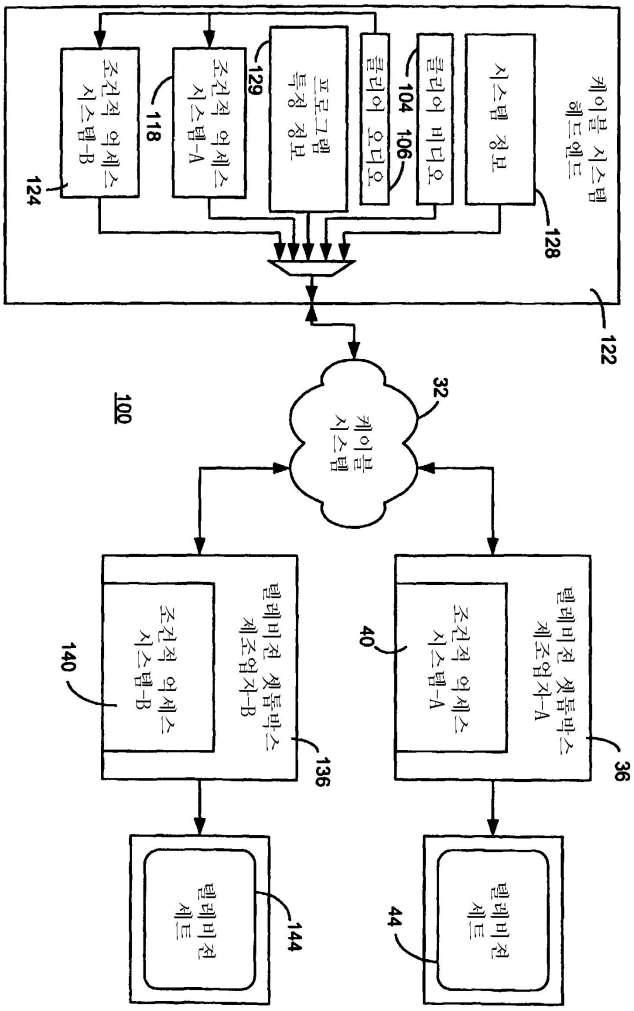
도면

도면1

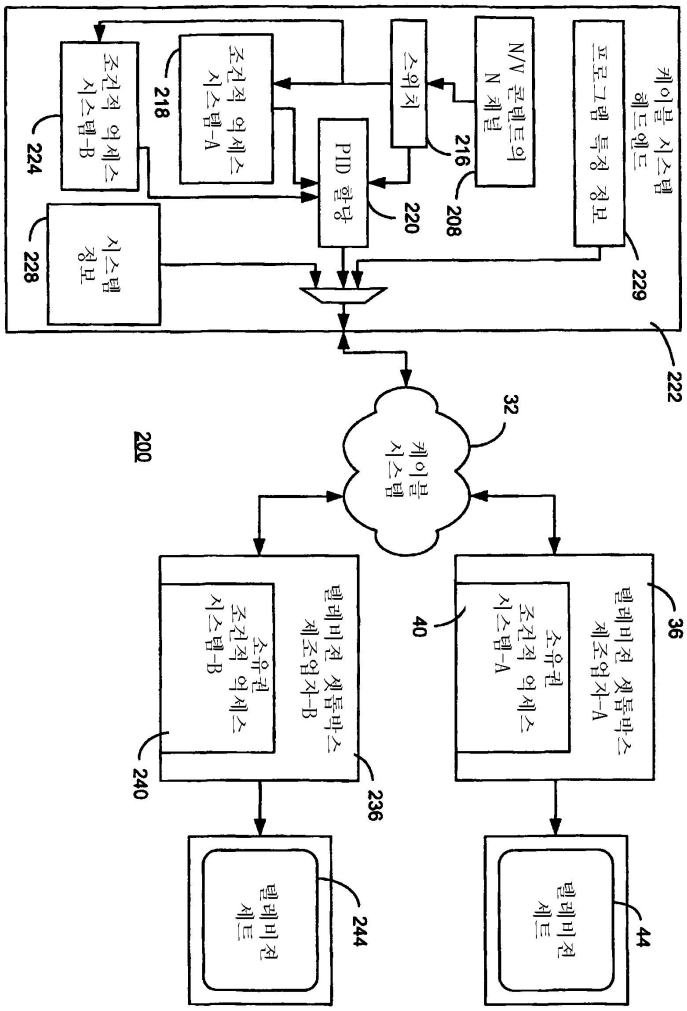
(종래 기술)


케이블 시스템 헤드엔드
27
프로그램 특정 정보
26
시스템 정보
18
조건적 억세스 시스템-A
14
A/V 콘텐츠
22
케이블 시스템
32
텔레비전 셋톱 박스 제조업자-A
36
조건적 억세스 시스템-A
40
텔레비전 세트
44

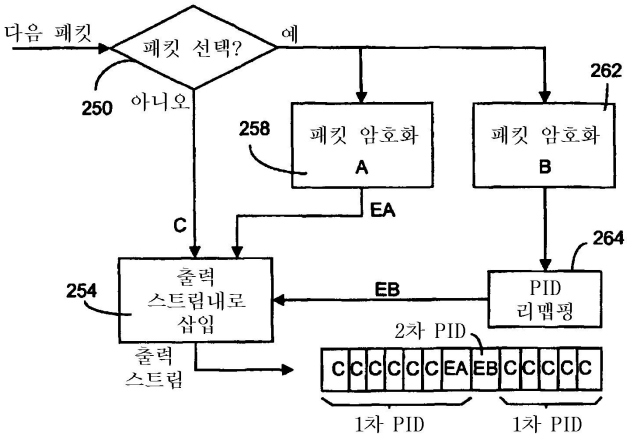
도면2


케이블 시스템 헤드엔드
시스템 정보
128
클리어 비디오
104
클리어 오디오
106
프로그램 특정 정보
조건적 억세스 시스템-A
129
118
조건적 억세스 시스템-B
124
122
100
케이블 시스템
32
텔레비전 셋톱박스 제조업자-A
조건적 억세스 시스템-A
40
36
텔레비전 셋톱박스 제조업자-B
조건적 억세스 시스템-B
140
136
텔레비전 세트
44
텔레비전 세트
144

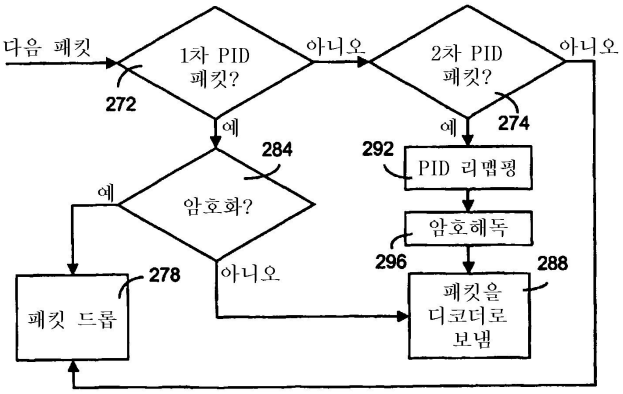
도면3


케이블 시스템 헤드엔드
프로그램 특정 정보
229
N/V 콘텍트의 N 채널
216
208
스위치
PID 할당
220
조건적 억세스 시스템-A
218
조건적 억세스 시스템-B
224
시스템 정보
228
222
200
32
케이블 시스템
텔레비전 셋톱박스 제조업자-A
36
소유권 조건적 억세스 시스템-A
40
텔레비전 셋톱박스 제조업자-B
236
소유권 조건적 억세스 시스템-B
240
텔레비전 세트
44
텔레비전 세트
244

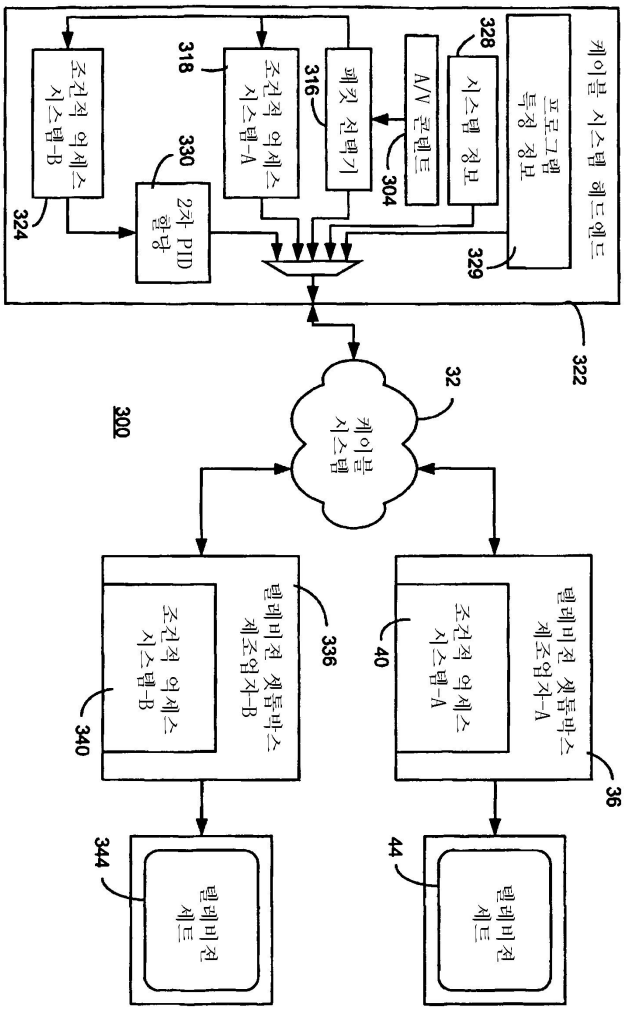
도면4


다음 패킷
패킷 선택?
예
250
아니오
262
258
패킷 암호화 A
패킷 암호화 B
EA
C
264
254
출력 스트림내로 삽입
EB
PID 리맵핑
2차 PID
출력 스트림
C C C C C C EA EB C C C C C
1차 PID
1차 PID

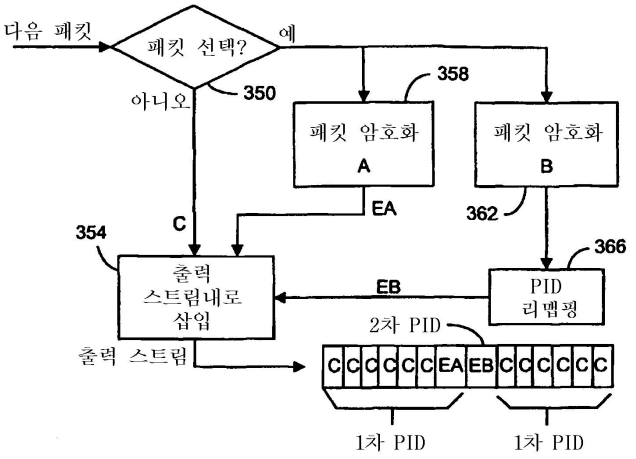
도면5


다음 패킷
1차 PID 패킷?
272
아니오
2차 PID 패킷?
아니오
예
274
292
PID 리맵핑
284
암호화?
예
아니오
암호해독
296
288
278
패킷 드롭
패킷을 디코더로 보냄

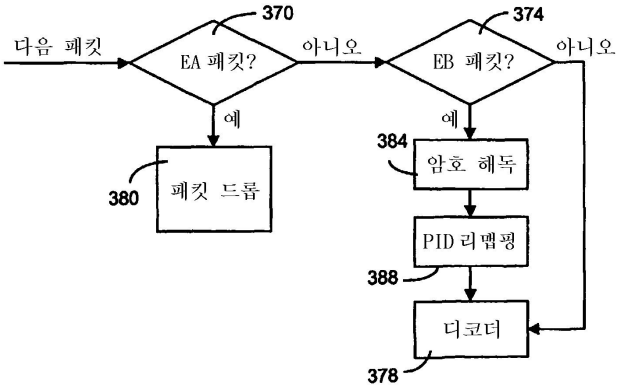
도면6


케이블 시스템 헤드엔드
조건적 억세스 시스템-B
318
조건적 억세스 시스템-A
316
패킷 선택기
A/V 콘텐트
304
328
시스템 정보
프로그램 특정 정보
329
324
330
2차 PID 할당
322
32
300
케이블 시스템
텔레비전 셋톱박스 제조업자-B
336
조건적 억세스 시스템-B
340
텔레비전 셋톱박스 제조업자-A
40
조건적 억세스 시스템-A
36
344
텔레비전 세트
44
텔레비전 세트

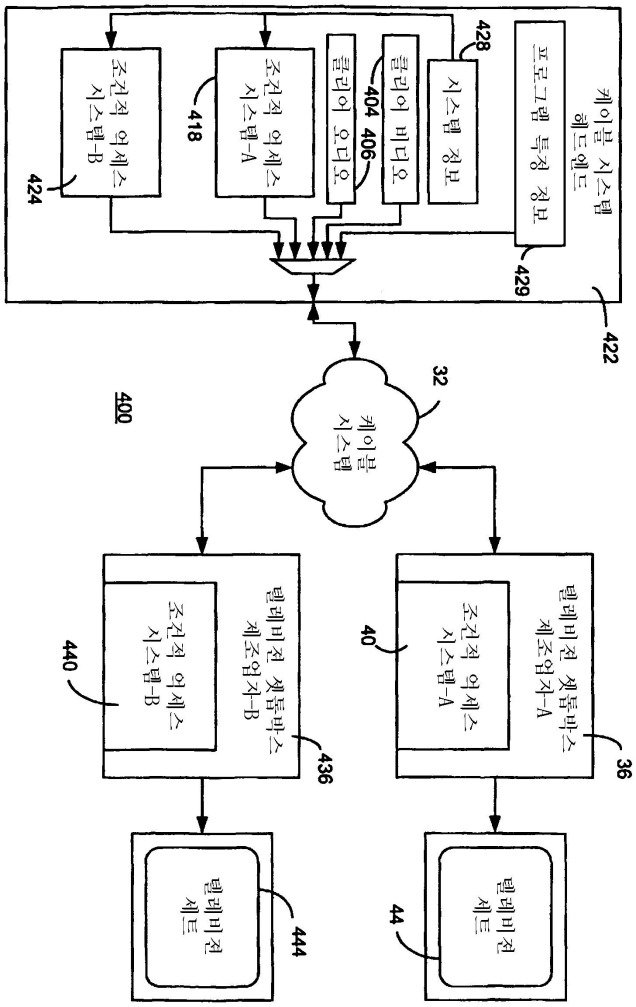
도면7


다음 패킷
패킷 선택?
예
아니오
350
358
패킷 암호화 A
패킷 암호화 B
EA
362
C
354
366
출력 스트림내로 삽입
EB
PID 리맵핑
2차 PID
출력 스트림
C C C C C C EA EB C C C C C C
1차 PID
1차 PID

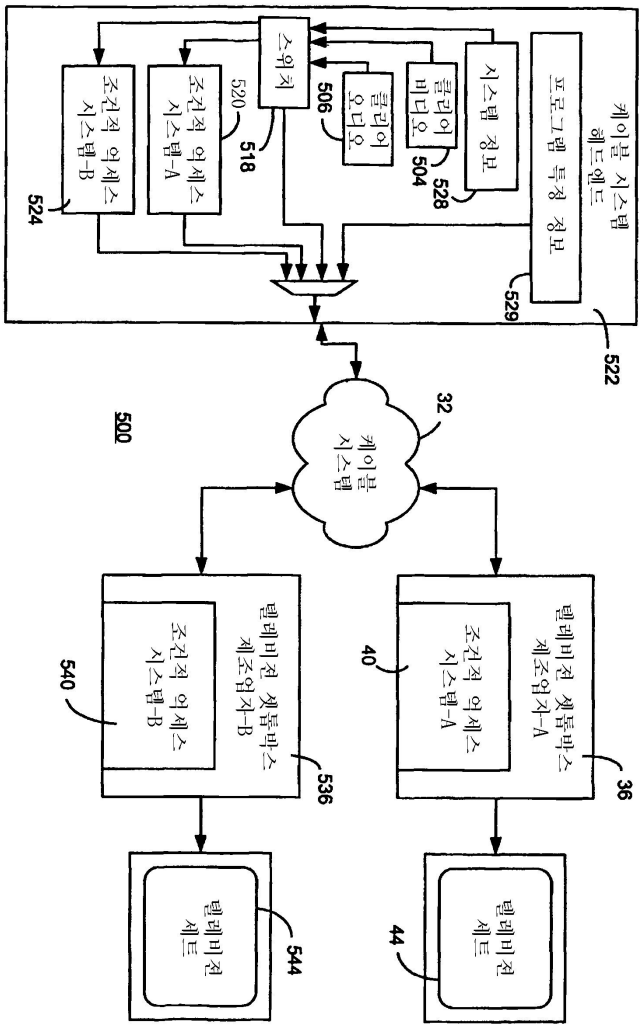
도면8


370
다음 패킷
EA 패킷?
아니오
374
EB 패킷?
아니오
예
예
380
패킷 드롭
384
암호 해독
PID 리맵핑
388
디코더
378

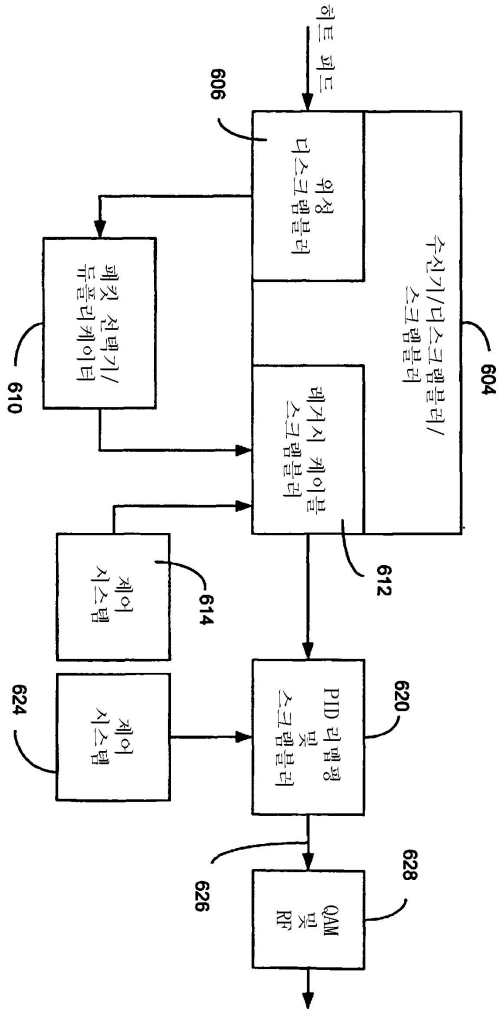
도면9


케이블 시스템 헤드엔드
프로그램 특정 정보
429
422
시스템 정보
428
클리어 비디오
404
클리어 오디오
406
조건적 억세스 시스템-A
418
조건적 억세스 시스템-B
424
400
32
케이블 시스템
텔레비전 셋톱박스 제조업자-A
조건적 억세스 시스템-A
40
36
텔레비전 셋톱박스 제조업자-B
조건적 억세스 시스템-B
440
436
텔레비전 세트
44
텔레비전 세트
444

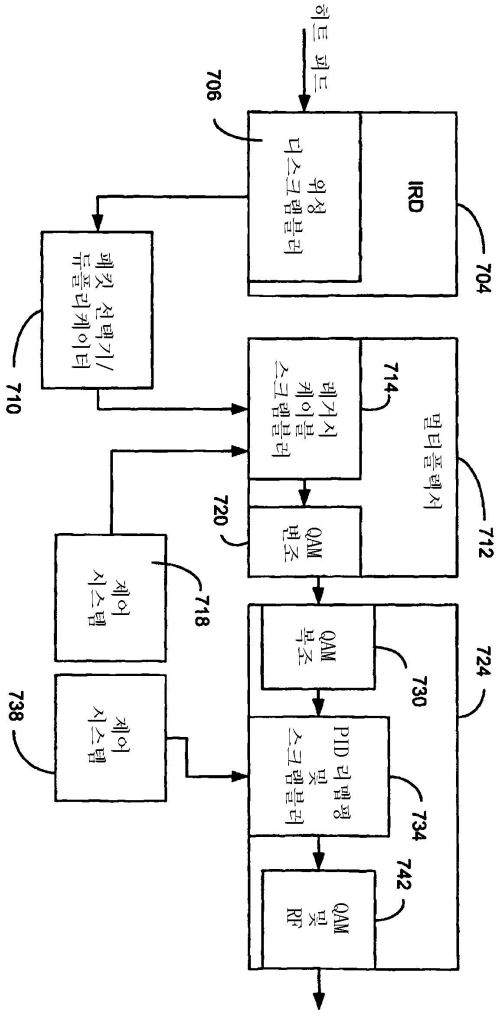
도면10


케이블 시스템 헤드엔드
프로그램 특정 정보
529
522
시스템 정보
클리어 비디오
504
528
클리어 오디오
506
스위치
520
518
조건적 억세스 시스템-A
조건적 억세스 시스템-B
524
500
32
케이블 시스템
텔레비전 셋톱박스 제조업자-A
조건적 억세스 시스템-A
40
36
텔레비전 셋톱박스 제조업자-B
조건적 억세스 시스템-B
540
536
텔레비전 세트
44
544

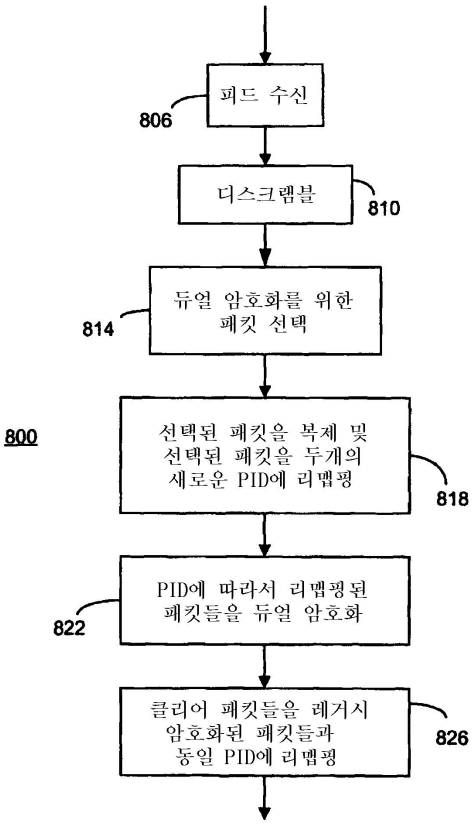
도면11


히트 피드
606
위성 디스크램블러
수신기/디스크램블러/스크램블러
604
페킷 선택기/듀플리케이터
610
레거시 케이블 스크램블러
612
셀 시스템
614
셀 시스템
624
PID 리맵핑 및 스크램블러
620
626
QAM 및 RF
628

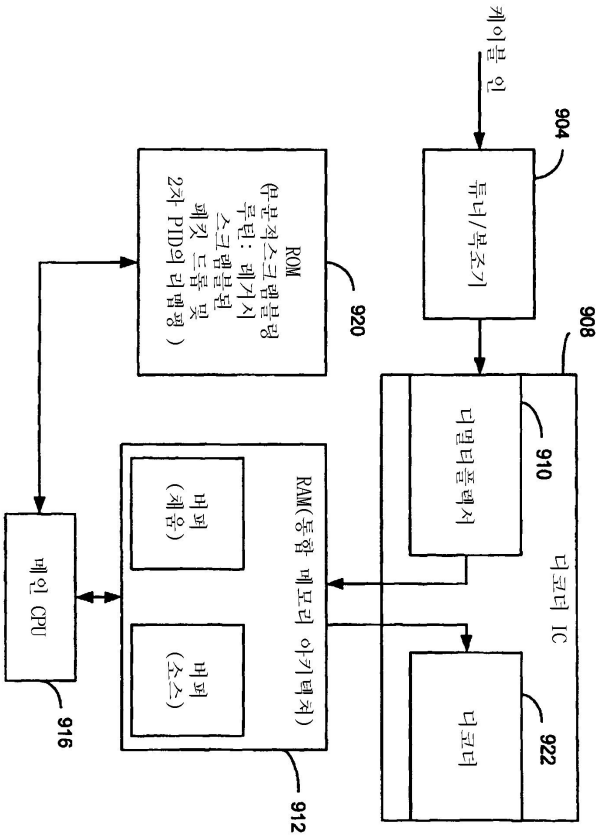
도면12


위성 디스크램블러
IRD
704
706
패킷 선택기/ 듀플리케이터
710
멀티플렉서
712
멕가시 케이블 스크램블러
714
QAM 변조
720
제어 시스템
718
QAM 복조
730
724
PID 리맵핑 및 스크램블러
734
738
제어 시스템
QAM 및 RF
742

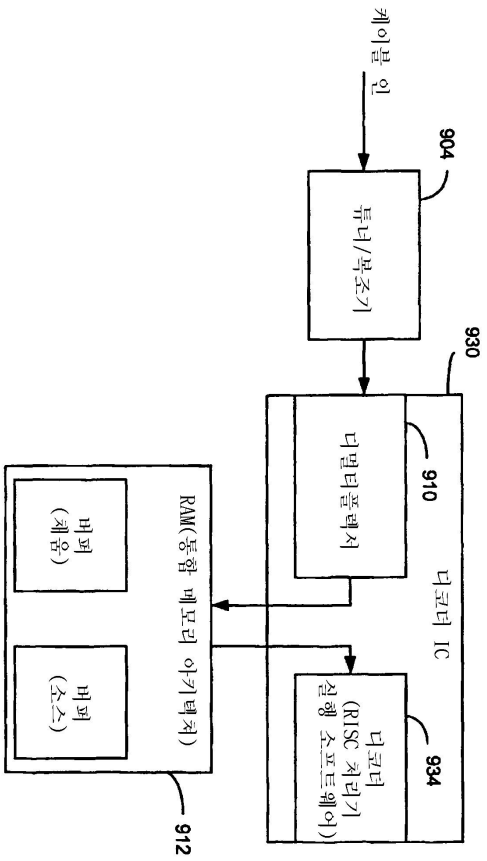
도면13


피드 수신
806
디스크램블
810
듀얼 암호화를 위한
패킷 선택
814
800
선택된 패킷을 복제 및
선택된 패킷을 두개의
새로운 PID에 리맵핑
818
PID에 따라서 리맵핑된
패킷들을 듀얼 암호화
822
클리어 패킷들을 레거시
암호화된 패킷들과
동일 PID에 리맵핑
826

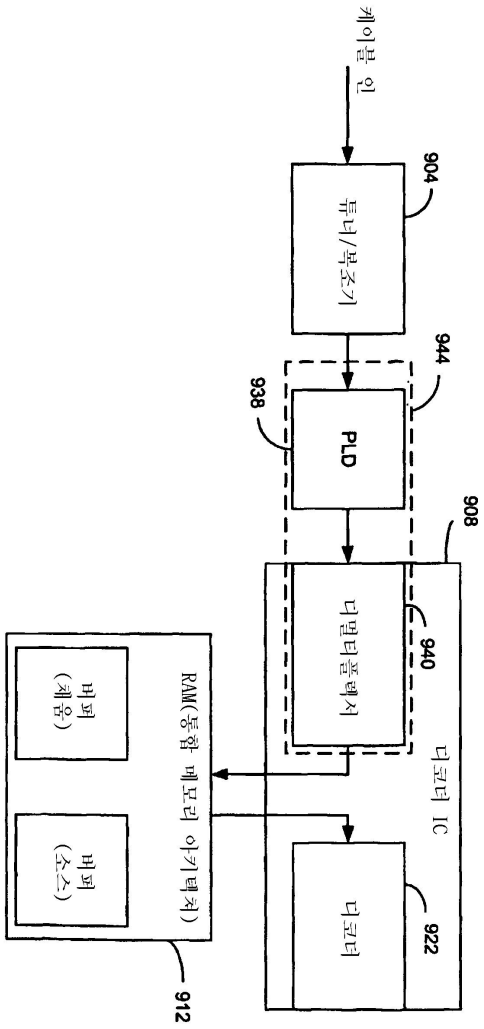
도면14


케이블 인
904
튜너/복조기
908
910
디멀티플렉서
디코더 IC
922
디코더
ROM
(부분적으로 스크램블링 구현: 레거시 스크램블된 패킷 드롭 및 2차 PID의 리맵핑)
920
RAM(동적 메모리 아키텍처)
버퍼 (제어)
버퍼 (소스)
912
메인 CPU
916

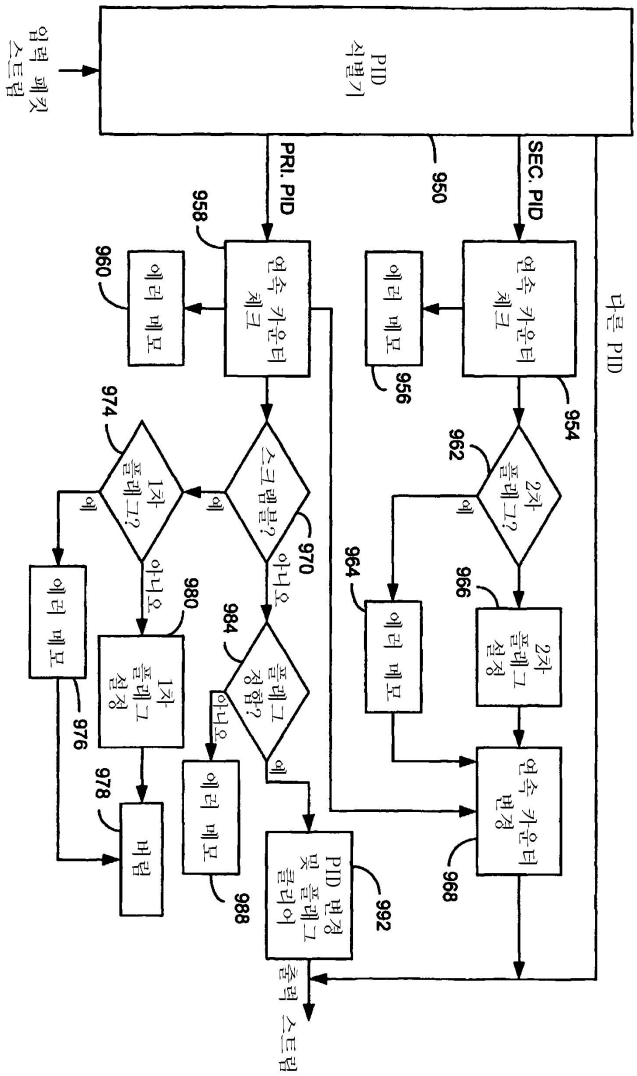
도면15


케이블 인
904
튜너/복조기
930
910
디멀티플렉서
디코더 IC
934
디코더
(RISC 처리기
실행 소프트웨어)
RAM(통합 메모리 아키텍처)
버퍼
(체움)
버퍼
(소스)
912

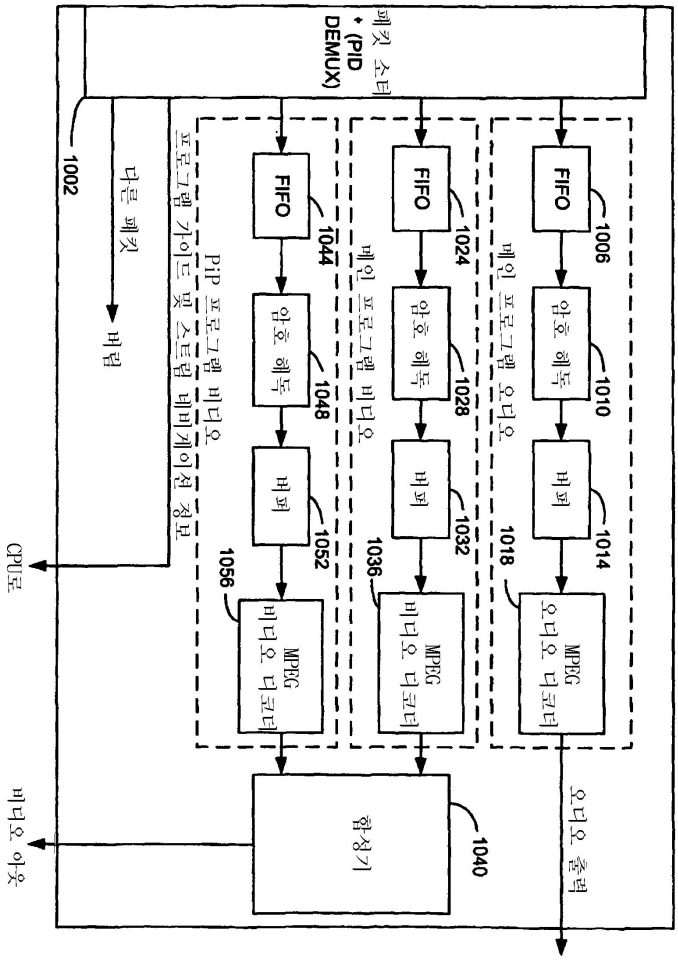
도면16


케이블 인
튜너/복조기
904
944
938
PLD
908
디멀티플렉서
940
디코더 IC
디코더
922
RAM(통합 메모리 아키텍처)
버퍼
(채움)
버퍼
(소스)
912

도면17


입력 패킷 스트림
PID 식별기
950
SEC. PID
PRI. PID
다른 PID
연속 카운터 체크
954
에러 메모
956
2차 플래그?
962
에
2차 플래그 설정
966
에러 메모
964
연속 카운터 변경
968
연속 카운터 체크
958
에러 메모
960
스크램블?
970
아니오
1차 플래그?
974
에
아니오
에러 메모
976
1차 플래그 설정
980
버퍼
978
플래그 정합?
984
아니오
에러 메모
988
에
PID 변경 및 클리어
992
출력 스트림

도면18


패킷 소터
(PID DEMUX)
1002
다른 패킷
버림
CPU로
비디오 아웃
오디오 출력
FIFO
1006
암호 해독
1010
버퍼
1014
MPEG 오디오 디코더
1018
메인 프로그램 오디오
FIFO
1024
암호 해독
1028
버퍼
1032
MPEG 비디오 디코더
1036
메인 프로그램 비디오
FIFO
1044
암호 해독
1048
버퍼
1052
MPEG 비디오 디코더
1056
PiP 프로그램 비디오
프로그램 가이드 및 스트림 네비게이션 정보
합성기
1040