

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) . Int. Cl.⁷
H04N 5/913

(11) 공개번호 10-2005-0030877
(43) 공개일자 2005년03월31일

(21) 출원번호 10-2004-0077691
(22) 출원일자 2004년09월30일

(30) 우선권주장 60/506,193 2003년09월26일 미국(US)
10/762,680 2004년01월21일 미국(US)

(71) 출원인 제네시스 마이크로칩 인코포레이티드
미국 캘리포니아 95002, 알비소, 2150 골드 스트리트

(72) 발명자 코바야시, 오사무
미국, 캘리포니아 94024, 로스 알토스, 1464 풀른 리프 레인

(74) 대리인 강명구

심사청구 : 없음

(54) 패킷 기반 고 선명 고-대역 디지털 콘텐트 보호

요약

패킷 기반 고 대역 카피 보호 방법은 소스 장치에서 다수의 데이터 패킷들을 형성하고, 암호화 값 세트에 기초한 상기 데이터 패킷들을 암호화 하며, 상기 소스 장치로부터 거기에 연결된 흡수 장치까지 상기 암호화된 데이터 패킷들을 전송하고, 상기 암호화 값에 부분적으로 기초한 상기 암호화된 데이터 패킷들을 복호화 하며 그리고, 상기 흡수 장치에 의해 상기 복호화 된 데이터 패킷들에 액세스 하는 단계를 포함하여 설명된다.

대표도

도 1

명세서

도면의 간단한 설명

도 1 은 당해 발명의 어떠한 실시예에서의 사용에 적합한 디지털 비디오 디스플레이 인터페이스에 기반을 둔 교차 플랫폼의 일반화된 표현이다.

도 2는 도 1 과 관련하여 설명된 시스템에서 사용에 적합한 암호화 오디오/비디오 컨텐트를 위한 암호화 시스템을 도시한다.

도 3 은 당해 발명의 실시예에 따라 암호화된 데이터 흐름의 표현을 도시한다.

도 4는 당해 발명을 구현하기 위해 이용하는 시스템을 설명한다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

관련 출원

당해 발명은 코바야시에 의해 2003년 9월 26일 출원된 미국 특허 출원 번호 60/506,193, 명칭 "PROVIDING HIGH DEFINITION COPY PROTECTION IN A PACKET BASED DATA STREAM"를 여기서 참고 자료로서 통합한다.

당해 발명은 디스플레이 장치에 관한 것이다. 보다 상세히, 당해 발명은 패킷 기반 정송 환경에서 오디오/비디오 데이터의 로버스트 암호화를 제공할 수 있는 방법 및 장치에 대하여 설명한다.

디지털 컨텐트의 지적 보호가 특히, 고 화질(HD), 고-대역 장치가 중요한 고려 대상이 되고 있다. 특히, HD의 경우에 있어 중요한 것은, 고-대역 장치들, 컨텐트 보호는 디지털화된 컨텐트의 소유자가 그들의 독점적 컨텐트의 비인가 사용 및 복제로부터 보호되는 것의 확신을 제공하는 것이다. HDCP로 일반적으로 간주되는 Santa Clara CA 인텔 회사에 의해 개발된 인기 있는 고-대역 디지털-컨텐트 보호 구조가 널리 구현되어 왔다. 최근에 구현된 것으로써, 이 특별한 HDCP 프로토콜은 특히 Digital Visual Interface(DVI) 및 고-화질 멀티미디어 인터페이스(HDMI) 기반 환경에서의 사용을 위해 특별히 제작되었다.

일반적으로, HDCP는 PC, DVD 플레이어 또는 셋-톱 박스와 같은 비디오 소스 또는 송신기 그리고 모니터, 텔레비전 또는 프로젝터와 같은 디지털 디스플레이 또는 수신기 간의 디지털 컨텐트의 전송을 암호화 한다. 이런 방식으로, HDCP는 디지털 컨텐트의 복사 또는 기록을 방지하기 위해 디자인되고 그것에 의해 그것이 전송되고 있는 것과 같은 컨텐트의 보전을 보호한다. 예를 들어, 인증화 단계 동안, 설명된 HDCP 프로토콜에 의해 요구되는 것과 같이, 리시버는 단지 일단 컨텐트와 함께 제공될 것이고, 그것은 비밀값의 계산을 통해 트랜스시버가 입증하는 인증화 키의 인식을 설명할 것이다. 더구나, 데이터의 도청 및 도난을 방지하기 위해, 상기 트랜스미터 및 리시버는 전송을 통해 일관적으로 체크되는 분배된 비밀값을 발생할 것이다. 일단 인증화가 설립되면, 상기 트랜스미터는 상기 데이터를 암호화하고 그리고 그것은 복호화를 위해 리시버에 전송한다.

상기 DVI 표준의 구현은 10 비트 전송 프로토콜에 기초한 정의된 문자 세트의 이용을 요구한다. 예를 들어, 최근에 구현된 것과 같이, 4개의 문자들이 hsync 및 vsync와 같이 정확한 제어 신호로써 사용되는 동안 데이터를 위한 리시버에 의해 사용된다. 이 배열에서, 어떠한 시간에서도 상기 리시버는 수신하고 그리고 데이터를 표현하는 미리 지정된 문자들 중의 하나를 인식한다. 함축적으로 수신된 것은 액티브로서 데이터 가능 신호(DE)를 정의하며, 그것에 의해 수신된 데이터가 트루(true) 데이터라는 것을 표시한다. 4개의 제어 문자들 중의 하나가 리시버에 의해 수신될 때마다, 데이터 가능(DE)이 비활성화라는 암시적 가정이 이루어진다.

HDCP 프로토콜은 그것의 상태 기계를 진척시키기 위해 DE의 상태, Hsync, Vsync, 그리고 CNTL3라 불리는 또 다른 제어 신호를 이용한다. 상기 DE, Hsync, Vsync 신호들은 "흐름" 방식에서 발송되는 레스터 비디오와 관련된 시간 신호들이다. 흐름 전송에서, 픽셀 데이터는 픽셀 비율에서 전송되고 그리고 데이터 구간으로의 블랭킹 구간의 비율이 보존된다. 패킷 전송의 경우에서, 이러한 타이밍 신호들은 표현되지 않는다. 타이밍 정보가 다른 방식으로 통신되는 동안, 단지 픽셀 데이터는 패킷 흐름 내에서 전송된다. 따라서 요구되는 것은 패킷 전송 모드에서 작동하는 링크에 대한 HDCP 또는 전송 매체와 같은 고 화질 저작 보호 프로토콜과 호환하는 고-화질 저작 보호를 지원하는 것이다.

발명이 이루고자 하는 기술적 과제

제공되는 것은, 따라서, 패킷-기반 디지털 전송 매체 및 HDCP와 같은 고 화질 저작 보호 프로토콜과 뒤에서 호환하는 고-화질 저작 보호를 지원하는 프로토콜이다.

당해 발명의 일 실시예에서, 패킷 기반 고 대역 저작 보호 방법은 다음의 작동을 포함하여 설명된다. 소스 장치에서 다수의 데이터 패킷들을 형성하는 것, 암호화 값 세트에 기초한 데이터 패킷들을 암호화 하는 것, 소스 장치로부터 거기에 결합된 흡수 장치까지 암호화된 데이터를 전송하는 것, 암호화 값에 부분적으로 기초한 암호화된 데이터 패킷들을 복호화 하는 것, 그리고 상기 흡수 장치에 의한 복호화 된 데이터 패킷들에 액세스 하는 작동이다.

또 다른 실시예에서, 데이터 흐름으로 패킷 기반 고 대역 저작 보호를 제공하기 위한 시스템이 설명되며, 이는 다수의 데이터 패킷들을 제공하기 위해 배열되는 소스 유닛, 상기 소스 유닛으로부터 데이터 패킷들을 수신하기 위해 배열된 소스 유닛에 결합된 흡수 유닛, 상기 소스 유닛으로부터 상기 싱크 유닛까지 전송된 데이터 패킷들을 암호화하기 위해 배열된 상기 소스 유닛에 결합된 암호화 유닛, 상기 적합한 데이터 패킷들을 암호화 및 복호화 하기 위해 사용되는 암호화/복호화 값들의 세트를 제공하기 위해 배열되는 암호화/복호화 값들 및 암호화된 데이터 패킷을 복호화 하기 위해 배열된 흡수 유닛에 결합된 복호화 유닛을 포함한다.

또 다른 실시예에서, 고 대역 저작 보호에 기초한 패킷을 제공하기 위한 컴퓨터 프로그램 장치가 설명되었으며, 이 장치는 소스 장치에서 다수의 데이터 패킷들을 형성하기 위한 컴퓨터 코드, 암호화 값 세트에 기초한 데이터 패킷들을 암호화하기 위한 컴퓨터 코드, 상기 소스 장치로부터 거기에 결합된 흡수 장치까지 암호화된 데이터 패킷들을 전송하기 위한 컴퓨터 코드, 상기 암호화 값에 부분적으로 기초한 암호화된 데이터 패킷들을 복호화 하기 위한 컴퓨터 코드, 상기 흡수 장치에 의해 복호화 된 데이터 패킷들에 액세스하기 위한 컴퓨터 코드, 상기 컴퓨터 코드를 저장하기 위한 컴퓨터 판독형 매체를 포함한다.

발명의 구성 및 작용

최근에 구현되는 것과 같이, HDCP는 디스플레이 장치가 보호된 컨텐트를 수신하기 위해 라이선스 되고 그리고 일단 설립되었다는 것을 확인하기 위해 보호 채널을 설치하고, 상기 보호된 컨텐트의 "도난"을 방지하기 위해 호스트 측면에서 상기 데이터를 암호화하고 그리고 디스플레이 장치에서 복호화 한다. 게다가, 비인증된 또는 포함된 장치들을 확인하기 위해, HDCP는 인증화 그리고 키 교환, 컨텐트 암호화 및 장치 재생 화에 의존한다.

보다 바람직하게, HDCP는 비디오 소스와 디지털 디스플레이(리시버) 간의 전송을 암호화함으로써 디지털 비디오 인터페이스(DVI) 내의 판권으로 보호된 디지털 연예 컨텐트를 보호한다. 상기 비디오 소스는 PC, 셋-톱 박스, DVD 플레이어 등일 수 있으며, 상기 디지털 디스플레이는 LCD, 텔레비전, 플라즈마 패널, 또는 프로젝터일 수 있으며,

이러한 인증화 된 장치들은 주어진 유일한 보호 장치 키들의 세트이다. 인증화 과정동안, 상기 리시버는 상기 보호된 컨텐트가 정송되기 이전에 다수의 보호 장치키의 지식을 설명해야만 한다. 상기 리시버가 상기 키들을 인식한 이후에, 장치들(센더 및 리시버)은 상기 컨텐트의 도난으로부터 도청을 방지하기 위해 제작된 분배된 보호값을 생성한다. 인증화 이후, 상기 컨텐트는 암호화 되고 그리고 그것을 차례로 복호화 하는 리시버로 전송된다.

인증화는 디스플레이 장치가 보호된 컨텐트를 수시하기 위해 인증되는 것을 확인하기 위한 암호 과정이다. 상기 인증화 된 호스트 및 디스플레이 장치는 모두 40개의 56비트 보호 장치키의 배열 및 대응하는 40-비트 이진 키 선택 벡터(KSV)로 구성되는 보호 키 세트의 인식을 지닌다. 상기 호스트는 그것의 키 선택 벡터, AKSV 및 64-비트 값 An 을 포함하는 초기화 메시지를 전송함으로써 인증화를 시작한다. 상기 디스플레이 장치는 그것의 키 선택 벡터, BKSV를 포함하는 응답 메시지를 전송함으로써 응답한다. 호스트는 수신된 KSV 가 철회되지 않는 것을 확실히 한다. 이 지점에서, 상기 두 개의 장치들은 분배된 값을 계산할 수 있고, 이는 양 장치들이 유효한 키 세트 값을 지닐 경우 같아질 것이다. 이 분배된 값은 인증화가 설치되기 때문에 상기 보호된 컨텐트의 암호화 및 복호화에서 사용될 것이다.

제-인증화는 링크의 계속된 보호를 확실히 하기 위해 약 매 2초의 비율에서 지속된다. 상기 분배된 값의 균등이 솔루션되는 경우, 예를 들어, 디스플레이 장치 그리고/또는 비합법적 복사 장치의 연결에 의한 것과 같은 경우, 상기 호스트는 DVI 링크가 비인증화 되었고, 보호된 컨텐트의 전송이 끝났다고 생각할 것이다.

컨텐트는 만들어지는 것으로부터 전송된 컨텐트의 이용 가능한, 비인증화 복제물들을 방지하기 위해 암호화 된다. 암호화는 암호라 불리는 알고리듬의 장치이며, 그것은 컨텐트를 전환한다. 상기 컨텐트를 복구하기 위해, 상기 디스플레이 장치는 정확한 복호키의 인식에 의해 상기 컨텐트를 복호화 한다. 상기 HDCP 암호는 혼합 블락/흐름 암호이다. 상기 블락 암호는 인증화 프로토콜 동안 작동한다. 컨텐트 암호화 및 복호화를 위해, HDCP 는 암호화가 비트와 이즈(bitwise) 배제적-OR 작동을 통해 전송된 컨텐트와 함께 HDCP 암호에 의해 발생되는 데이터 흐름을 결합함으로써 성취되는 곳에서 흐름 암호를 이용한다. 이런 방식으로, 상기 컨텐트는 광 셀 단위로 보호된다. 복호화 없이 디스플레이 장치 상에 보이는 암호화된 내용은 분간할 수 없는 컨텐트를 지닌 랜덤 노이즈로 보인다. 위에서 설명한 것과 같이, 현재 이용할 수 있는 HDCP 프로토콜들은 DVI 타입 커넥터를 이용하여 구현되어야 한다.

당해 발명은 패킷 기반 전송 매체에서 이용에 적합한 고 화질 고 대역 저작 보호 프로토콜을 제공하며, 이는 고 화질 카피 보호 프로토콜과 뒤에서 호환하는 고 화질 카피 보호를 지원하는 로버스트 디지털 저작권 보호를 제공한다. 당해 발명의 한 실시예에서, HDCP 프로토콜은 패킷 시반 고 대역 카피 보호 방법으로서 수행되며, 상기 방법은 소스 장치에서 다수의 데이터 패킷을 형성하는 것, 암호화 값 세트에 기초한 데이터 패킷들의 선택된 하나를 암호화 하는 것, 상기 소스 장치로부터 거기에 연결된 흡수 장치까지 암호화된 데이터 패킷들을 전송하는 것, 상기 암호화 값을 통해 부분적으로 기초한 암호화된 데이터 패킷들을 복호화 하는 것, 그리고 상기 흡수 장치에 의해 암호화된 데이터 패킷들에 액세스 하는 것을 포함한다.

매우 잘 적합화 된 패킷 기반 전송 시스템이 당해 발명의 어떠한 실시예에도 적합한 교차 플랫폼 패킷 기반 디지털 비디오 디스플레이 인터페이스(100)의 일반화된 구현을 도시하는 도 1과 관련하여 설명되었다. 상기 인터페이스(100)는 트랜스미터(102)를 링크(106, 또한 파이프로서 언급되는)를 경유하여 리시버(104)에 연결한다. 설명된 실시예에서, 다수의 데이터 흐름들(108-112)은 트랜스미터(102)에서 수신되고, 필요한 경우, 각각을 대응하는 다수의 데이터 패킷(114)들로 패킷화 한다. 이러한 데이터 패킷들은 그 후 리시버(104)로 관련된 가상 파이프(116-120)를 통해 패스하는 것의 각각 대응하는 데이터 흐름으로 형성된다. 주의할 것은 상기 데이터 흐름들(108-112)은 비디오, 그래픽, 오디오 등과 같은 다수의 형태를 취할 수 있다는 점이다.

특히, 상기 소스가 비디오 소스인 경우, 상기 데이터 흐름들(108-112)은 혼합 비디오, 직렬 디지털, 병렬 디지털, RGB 또는 소비자 디지털 비디오와 같은 잘 -알려진 포맷의 타입을 지닐 수 있는 다양한 비디오 신호들을 포함한다. 상기 비디오 신호는 소스(102)에 의해 제공되는 아날로그 비디오 신호가 될 수 있으며, 이는 예를 들어, 아날로그 텔레비전, 스틸 카메라, 아날로그 VCR, DVD 플레이어, 캠코더, 레이저 디스크 플레이어, TV 티비, 셋톱 박스(위성 DSS 또는 케이블 신호를 지닌) 등과 같은 아날로그 비디오 소스의 일부 형태를 포함한다. 상기 소스(102)는 또한 디지털 텔레비전(DTV), 디지털 스틸 카메라 등과 같은 디지털 이미지 소스를 포함할 수 있다. 상기 디지털 비디오 신호는 표준 480 프로그레시브 스캔 비디오와 마찬가지로 SMPTE 274M-1995(1920*1080 해상도, 프로그레시브 또는 인터레이스 스캔), SMPTE 296M-1997(1280*720 해상도, 프로그레시브 스캔)과 같은 잘 알려진 디지털 포맷 타입이 될 수 있다.

소스(102)가 아날로그 이미지 신호를 제공하는 경우에 있어서, 아날로그-디지털 컨버터(A/D)는 아날로그 전압 또는 전류 신호를 디지털 프로세싱에 적합한 적절한 디지털 이미지를 형성하는 과정에서 디지털 적으로 인코드된 숫자들(신호)의 분리된 일련으로 전환한다. 다양한 A/D 컨버터들 어느 것이라도 사용될 수 있다. 실시예에 따라, 다른 A/D 컨버터들은, 예를 들어, Philips, Texas Instrument, Analog Devices, Brooktree 그리고 다른 것들에 의해 제조되는 것을 포함한다.

예를 들어, 데이터 흐름(110)이 아날로그 타입 신호인 경우, 트랜스미터(102) 내에 포함된 또는 그것에 결합된 상기 아날로그 디지털 컨버터(도시 안남)는 아날로그 데이터를 디지털화 하고, 이때, 상기 아날로그 데이터는 그 후 가상 링크(116)를 경유하여 상기 리시버(104)로 전송될 각각의 다수의 데이터 패킷들로 디지털화 된 데이터 흐름(110)을 전환하는 패킷타이저(paketizer)에 의해 패킷화 된다. 상기 리시버(104)는 그 후 상기 데이터 패킷들(114)을 그들의 원 포맷으로 적합하게 재결합함으로써 상기 데이터 흐름(110)을 재구성할 것이다.

도 2는 도 1과 관련하여 설명된 시스템(100)과 함께 사용에 적합한 오디오/비디오 컨텐트를 암호화하기 위한 암호화 시스템(200)을 도시한다. 도 2에 도시되는 바와 같이, 비디오 소스(202)는 데이터 흐름(110,112)과 같은 다수의 데이터 흐름들을 제공하기 위해 배열된다. 다수의 데이터 흐름을 이용함으로써, 상기 시스템(200)은 비디오 데이터를 전송할 수 있으며, 예를 들어, 동시에 다수의 비디오 포맷들과 일치한다. 예를 들어, 상기 데이터 흐름(110)은 60Hz에서 1024*768 과 일치하는 비디오 데이터로 형성됨에 반하여, 상기 데이터 흐름(112)은 75Hz에서 640*480

과 함께 일치하도록 형성되는 것 등이다. 적합한 포맷에서 비디오를 재구성하기 위해 리시버(204)(모니터와 같은)를 경우, 상기 데이터 흐름들은 부가적으로 적합한 포맷에서 비디오를 재구성하기 위해 리시버에 의해 사용되는 관련 속성 데이터를 포함한다.

따라서 상기 비디오 소스(202)는 다수의 버퍼(206)를 포함하고, 각각은 비디오 데이터 흐름들 중의 관련된 하나를 버퍼하기 위해 사용된다. 상기 버퍼들 각각은, 차례로, 패킷타이저(210)로 전송을 위한 데이터 흐름들 중의 특정 하나를 선택하기 위해 사용되는 멀티플렉서(208)에 결합된다. 패킷 ID를 통합하고, 선택적으로 여러 수정을 수행하며 그리고 시간 스템프 및 리시버(404)에 의해 비디오 래스터를 바르게 재구성하기 위해 중요하거나 또는 필요하다고 여겨지는 특징들 중의 어느 것과 시간 스템프를 부착함으로써 상기 패킷타이저(210)는 관련 다수의 데이터 패킷들로 부수적 데이터 흐름을 분석한다. 암호화 제어 발생기 유닛(212)은 적합한 암호화 알고리듬을 제어 패킷을 삽입하는 것에 의해 데이터 패킷 기반 각각으로 적합한 암호화 알고리듬을 적용하고, 이 때 상기 제어 패킷은 Hsync, Vsync 그리고 암호화된(그리고 역으로 암호화되지 않은) 그러한 데이터 패킷들) 그러한 데이터 패킷들을 플래그(flag)하기 위해 사용되는 특정 제어 문자 CNTL3와 같은 신호들을 전달한다.

당해 발명의 한 실시예에 따라, 상기 초래되는 암호화 데이터 스트림(214)(데이터 흐름(300)으로서 도 3에 도시되는 것의 특성 실시예)은 다수의 데이터 패킷들로 형성된다. 상기 데이터 흐름(300)은 상기 케이스가 되는 것과 같이 암호화된(또는 암호화 되지 않은) 비디오 데이터 패킷들을 마크하기 위해 사용되는 다수의 제어 패킷들(302)을 포함한다. 각 비디오 패킷은 관련 헤더9304)를 지니고, 상기 헤더는, 부분적으로, 비디오 데이터 패킷(306)과 관련되어 위에서 설명된 데이터를 분배한다. 예를 들어, 도 3에 도시된 경우에서, 상기 데이터 흐름(300)은 데이터 흐름(110)을 위한 데이터 패킷들을 포함하고, 그리고 상기 데이터 흐름(112)은 데이터 흐름(300)으로 결합되고 그 결과 상기 비디오 소스(202) 및 상기 리시버(204) 간의 상기 트래픽은 일정한 링크 환경과 일치한다.

설명된 실시예에서 주의할 것은, 상기 데이터 흐름(300)은 다중 송신 방식의 시간 영역이며, 데이터 흐름(110)과 관련된 그러한 데이터 패킷들은 상기 데이터 흐름(112)과 관련된 것보다 더 긴 구간을 지닌다. 이러한 경우에서, 리시버(204) 내의 시간-기반 회복(TBR) 유닛(216)은 필요한 경우 주된 링크 데이터 패킷들 내에 끼워진 시간 스템프들을 이용하는 흐름의 원 네이티브 비율을 재생산한다. 도 2와 다시 관련하여, 리시버(404)에서, 직렬 변환기(deserializer) 유닛(218)은 입력을 디코더 유닛(220) 및 디패킷타이저(depacketizer)(222)로 제공하는 암호화된 데이터 흐름(300)을 수신한다. 상기 디코더(220)는 제어 패킷을 디코드 하고, 따라서 Hsync, Vsync 및 암호화를 위해 이전에 사용되는 복호화 엔진(228)으로 제공되는 특정 제어 문자 CNTL3을 공급한다.

도 4는 당해 발명을 구현하기 위해 이용되는 시스템(400)을 도시한다. 컴퓨터 시스템(400)은 단지 당해 발명이 구현될 수 있는 그래픽 시스템만의 실시예이다. 시스템(400)은 중앙 처리 유닛(CPU)(410), RAM(420), ROM(425), 하나 이상의 주변 장치(430), 그래픽 제어기(460), 1차 저장 장치(440, 450) 그리고 디지털 디스플레이 유닛(470)을 포함한다. CPU(410)는 또한 하나 이상의 입/출력 장치(490)에 결합되고, 그것은 제한되는 것은 아니라 트랙 볼, 마우스, 키보드, 마이크로폰, 터치-민감형 디스플레이, 애너지 변환 카드 판독기, 마그네틱 또는 페이퍼 데이프 판독기, 타블렛, 스타일러스, 음성 또는 핸드레이팅 인식기 또는 물론, 다른 컴퓨터와 같은 잘-알려진 입력 장치와 같은 장치들을 포함한다. 그래픽 제어기(460)는 아날로그 이미지 데이터 및 대응하는 기준 신호를 생성하고 그리고 둘 모두를 디지털 디스플레이 유닛(470)에 제공한다. 상기 아날로그 이미지 데이터는, 예를 들어, CPU(410) 또는 외부 인코드(도시 안 됨)로부터 수신되는 픽셀 데이터에 기초하여 발생될 수 있다. 한 실시예에서, 상기 아날로그 이미지 데이터는 RGB 포맷 내에서 제공되고 그리고 상기 기준 신호는 당업자에게 잘 알려진 Vsync 및 Hsync 신호들을 포함한다. 그러나 이해하여야 할 것은 당해 발명은 아날로그 이미지, 데이터 및/또는 다른 포맷 내의 기준 신호들과 함께 구현될 수 있다는 점이다. 예를 들어, 아날로그 이미지 데이터는 비디오 신호 데이터를 또한 대응하는 시간 기준 신호와 함께 포함할 수 있다.

당해 발명의 일부 실시예만이 설명되었음에도 불구하고, 당해 발명이 당해 발명의 기술적 사상으로부터 분리됨 없이 많은 다른 특정 형태로 구체화 될 수 있다는 것을 이해하여야 한다.

발명의 효과

DVI 표준의 구현은 10 비트 전송 프로토콜에 기초한 정의된 문자 세트의 이용을 요구한다. 예를 들어, 최근에 구현된 것과 같이, 4개의 문자들이 hsync 및 vsync와 같이 정확한 제어 신호로써 사용되는 동안 데이터를 위한 리시버에 의해 사용된다. 이 배열에서, 어떠한 시간에서도 상기 리시버는 수신하고 그리고 데이터를 표현하는 미리 지정된 문자들 중의 하나를 인식한다. 함축적으로 수신된 것은 액티브로서 데이터 가능 신호(DE)를 정의하며, 그것에 의해 수신된 데이터가 트루(true) 데이터라는 것을 표시한다. 4개의 제어 문자들 중의 하나가 리시버에 의해 수신될 때마다, 데이터 가능(DE)이 비활성화라는 암시적 가정이 이루어진다.

HDCP 프로토콜은 그것의 상태 기계를 진척시키기 위해 DE의 상태, Hsync, Vsync, 그리고 CNTL3라 불리는 또 다른 제어 신호를 이용한다. 상기 DE, Hsync, Vsync 신호들은 "흐름" 방식에서 발생되는 래스터 비디오와 관련된 시간 신호들이다. 흐름 전송에서, 픽셀 데이터는 픽셀 비율에서 전송되고 그리고 데이터 구간으로의 블랭킹 구간의 비율이 보존된다. 패킷 전송의 경우에서, 이러한 타이밍 신호들은 표현되지 않는다. 타이밍 정보가 다른 방식으로 통신되는 동안, 단지 픽셀 데이터는 패킷 흐름 내에서 전송된다. 따라서 요구되는 것은 패킷 전송 모드에서 작동하는 링크에 대한 HDCP 또는 전송 매체와 같은 고 화질 저작 보호 프로토콜과 호환하는 고-화질 저작 보호를 지원하는 것이다.

(57) 청구의 범위

청구항 1.

패킷 기반 고 대역 카피 보호 방법은,

- 소스 장치에서 다수의 데이터 패킷들을 형성하고,
- 암호화 값 세트에 기초한 상기 데이터 패킷들을 암호화 하며,
- 상기 소스 장치로부터 거기에 연결된 흡수 장치까지 상기 암호화된 데이터 패킷들을 전송하고,
- 상기 암호화 값에 부분적으로 기초한 상기 암호화된 데이터 패킷들을 복호화 하며, 그리고,
- 상기 흡수 장치에 의해 상기 복호화 된 데이터 패킷들에 액세스 하는

단계를 포함하는 것을 특징으로 하는 상기 패킷 기반 고 대역 카피 보호 방법.

청구항 2.

제 1 항에 있어서, 이 때 상기 소스 장치는 비디오 소스이고, 그리고 이 때 상기 흡수 장치는 비디오 디스플레이며, 그리고 이 때 다수의 데이터 패킷들은 일부 오디오 데이터 패킷들 및 일부 비디오 데이터 패킷들을 포함하는 것을 특징으로 하는 상기 패킷 기반 고 대역 카피 보호 방법.

청구항 3.

제 2 항에 있어서, 이 때 상기 암호화/복호화 제어 신호들은 Vsync, Hsync 그리고 CNTL3을 포함하는 것을 특징으로 하는 상기 패킷 기반 고 대역 카피 보호 방법.

청구항 4.

제 3 항에 있어서, 이 때 상기 데이터 패킷 각각은 특정 제어 패킷과 관련되는 것을 특징으로 하는 상기 패킷 기반 고 대역 카피 보호 방법.

청구항 5.

제 4 항에 있어서, 이 때 상기 CNTL3이 액티브일 때, 상기 대응하는 데이터 패킷은 암호화 되고 그리고 대응하는 데이터 패킷이 암호화되면 CNTL3이 액티브 되는 것을 특징으로 하는 상기 패킷 기반 고 대역 카피 보호 방법.

청구항 6.

패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템으로서,

- 다수의 데이터 패킷들을 전송하기 위해 배열된 소스 유닛,
- 상기 소스 유닛으로부터 상기 데이터 패킷들을 수신하기 위해 배열된 상기 소스에 결합된 흡수 유닛,
- 상기 소스 유닛으로부터 상기 싱크 유닛까지 전송하는 상기 데이터 패킷들 중의 선택된 하나를 암호화하기 위해 배열된 상기 소스 유닛에 결합된 암호화 유닛,
- 상기 암호화된 데이터 패킷들을 복호화 하기 위해 배열된 상기 흡수 유닛에 결합된 복호화 유닛, 그리고,
- 상기 적합한 데이터 패킷들을 암호화 하고 그리고 복호화하기 위해 사용되는 암호화/복호화 값들의 세트를 제공하기 위해 배열된 암호화/복호화 값 발생기

를 포함하는 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 7.

제 6 항에 있어서, 이 때 상기 소스 유닛은 오디오 타입 데이터 패킷들 및/또는 비디오 타입 데이터 패킷들을 전송하기 위해 배열된 오디오/비디오 유닛인 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 8.

제 7 항에 있어서, 이 때 상기 흡수 유닛은 상기 비디오 데이터 패킷들 중의 처리된 하나를 디스플레이 하기 위해 배열된 디스플레이 유닛인 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 9.

제 8 항에 있어서, 이 때 상기 디스플레이 유닛은 상기 오디오 데이터 패킷들 중의 처리된 하나에 기초한 오디오 신호들을 전송하기 위해 배열된 다수의 스피커들을 포함하는 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 10.

제 9 항에 있어서, 이 때 암호화/복호화 제어 신호들의 세트는 Vsync, 상기 비디오 데이터 패킷에 대응하는 Hsync 를 포함하는 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 11.

제 10 항에 있어서, 이 때 암호화/복호화 제어 신호의 세트는 암호화되는 그러한 데이터 패킷들을 플래그 하기 위한 CNTL3 를 추가적으로 포함하는 것을 특징으로 하는 상기 패킷 시반 시스템에서 고 대역 카피 보호를 제공하는 시스템.

청구항 12.

패킷 기반 고 대역 카피 보호를 제공하기 위한 컴퓨터 프로그램 상품으로서,

- 소스 장치에서 다수의 데이터 패킷들을 형성하기 위한 컴퓨터 코드,
- 암호화 값들의 세트에 기초한 상기 데이터 패킷들을 암호화하기 위한 컴퓨터 코드,
- 상기 소스 장치로부터 거기에 결합된 싱크장치까지 상기 암호화된 데이터 패킷들을 전송하기 위한 컴퓨터 코드,
- 상기 암호화 값에 부분적으로 기초한 상기 암호화된 데이터 패킷들을 복호화 하기 위한 컴퓨터 코드,
- 상기 흡수 장치에 의한 상기 복호화 된 데이터 패킷들에 액세스하기 위한 컴퓨터 코드,
- 상기 컴퓨터 코드를 저장하기 위한 컴퓨터 판독형 매체

를 포함하는 것을 특징으로 하는 상기 컴퓨터 프로그램 장치.

청구항 13.

제 12 항에 있어서, 이 때 상기 소스 장치는 비디오 소스이고 그리고 이 때 상기 흡수 장치는 비디오 디스플레이며 그리고 이 때 다수의 데이터 패킷들은 일부 오디오 데이터 패킷들 및 일부 비디오 데이터 패킷들을 포함하는 것을 특징으로 하는 상기 컴퓨터 프로그램 장치.

청구항 14.

제 13 항에 있어서, 이 때 상기 암호화 제어 신호들은 Vsync, Hsync 그리고 CNTL3 를 포함하는 것을 특징으로 하는 상기 컴퓨터 프로그램 장치.

청구항 15.

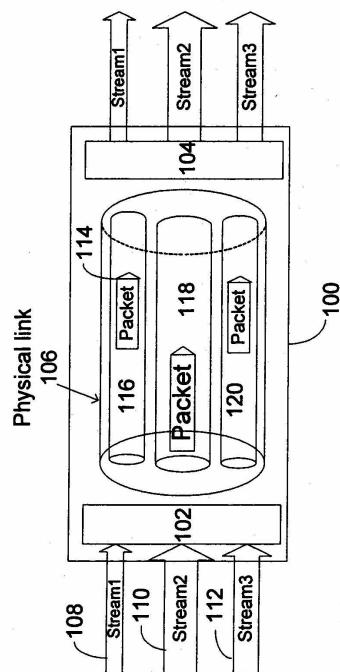
제 14 항에 있어서, 이 때 상기 데이터 패킷들의 각각은 특정 제어 값 CNTL3과 관련된 것을 특정으로 하는 상기 컴퓨터 프로그램 장치.

청구항 16.

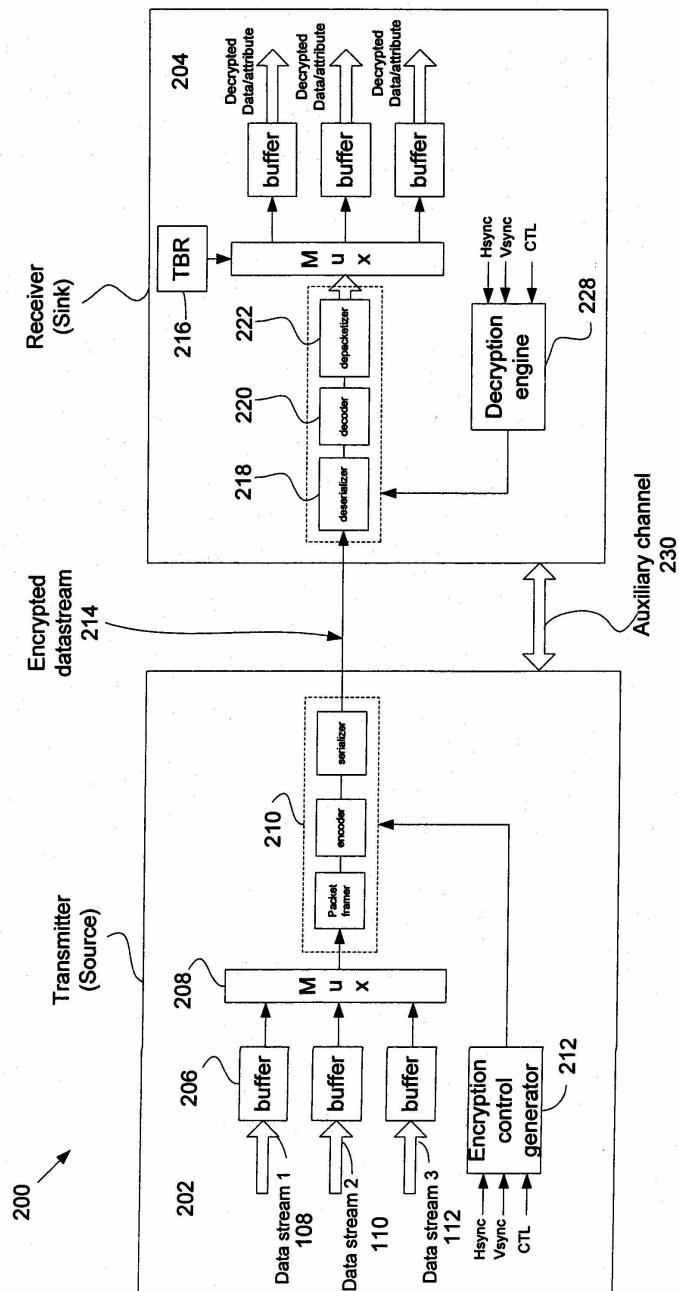
제 15 항에 있어서, 이 때 상기 CNTL3이 액티브일 때, 상기 대응하는 데이터 패킷은 암호화 되거나 대응하는 데이터 패킷이 암호화되면 CNTL3이 액티브 되는 것을 특정으로 하는 상기 컴퓨터 프로그램 장치.

도면

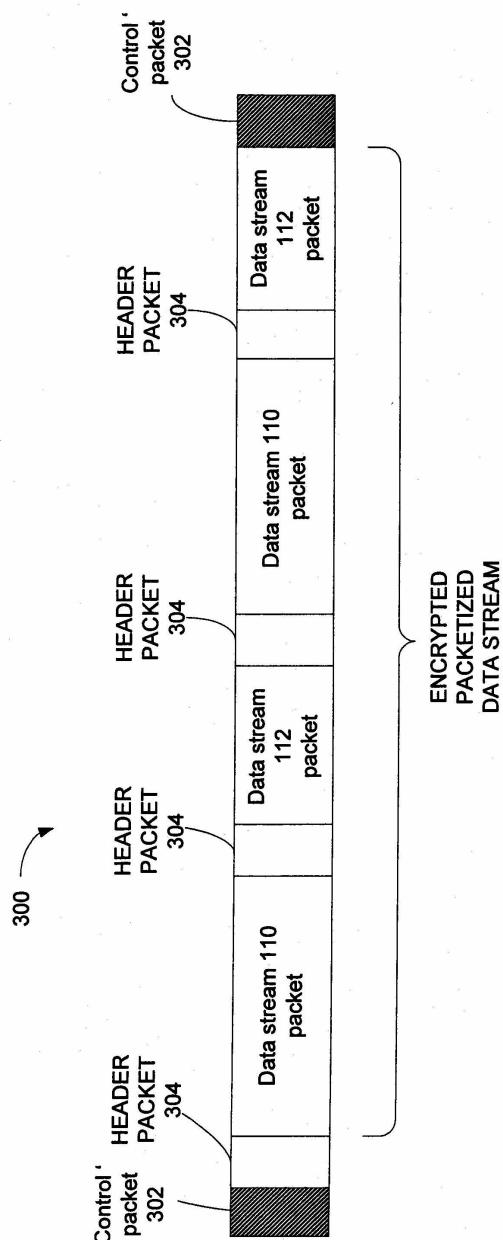
도면1



도면2



도면3



도면4

