

ASSIGNMENT

Whereas, I/We, Myung-Sik YIM of 105-1101, Kolong Apt., 331, Yatap-dong, Pundang-gu, Sungnam-city, Kyungki-do, Korea

hereinafter called assignor(s), have invented certain improvements in

"COPY PREVENTION APPARATUS AND METHOD IN DIGITAL BROADCASTING RECEIVING SYSTEM"

and executed an application for Letters Patent of the United States of America therefor on

Feb. 21 2000
~~1999~~; and

Whereas, SAMSUNG ELECTRONICS CO., LTD. of 416, Maetan-dong, Paldal-gu, Suwon-city, Kyungki-do, Republic of Korea (assignee), desires to acquire the entire right, title and interest in the application and invention, and to any United States patents to be obtained therefor;

Now therefore, for valuable consideration, receipt whereof is hereby acknowledged,

I/We the above-named assignor(s), hereby sell, assign and transfer to the above named assignee, its successors and assigns, the entire right, title and interest in the application and the invention disclosed therein for the United States of America, including the right to claim priority under 35 U.S.C. § 119, and I/we request the Commissioner of Patents to issue any Letters Patent granted upon the invention set forth in the application to the assignee, its successors and assigns; and I/we will execute without further consideration all papers deemed necessary by the assignee in connection with the United States application when called upon to do so by the assignee.

I/We hereby authorize and request my attorneys SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC of 2100 Pennsylvania Avenue, N.W., Washington, D.C. 20037-3202 to insert here in parentheses (Application number _____, filed _____) the filing date and application number of said application when known.

Date: Feb 21 / 2000

s/ Myungsik Yim
Myung-Sik YIM

Date: _____

s/ _____

Date: _____

s/ _____

(Legalization not required for recording but is prima facie evidence of execution under 35 U.S.C. §261)
8/92

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0003
【제출일자】 1999.09.14
【국제특허분류】 H04N
【발명의 명칭】 하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치 및 방법
【발명의 영문명칭】 A COPY PROTECTION APPARATUS AND METHOD OF A BROADCAST RECEIVING SYSTEM HAVING A HDD
【출원인】
【명칭】 삼성전자 주식회사
【출원인코드】 1-1998-104271-3
【대리인】
【성명】 이건주
【대리인코드】 9-1998-000339-8
【포괄위임등록번호】 1999-006038-0
【발명자】
【성명의 국문표기】 임명식
【성명의 영문표기】 YIM, Myung Sik
【주민등록번호】 640820-1009314
【우편번호】 463-070
【주소】 경기도 성남시 분당구 야탑동 331 장미 코오롱 아파트 105-1101
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이건주 (인)
【수수료】
【기본출원료】 16 면 29,000 원
【가산출원료】 0 면 0 원
【우선권주장료】 0 건 0 원
【심사청구료】 0 항 0 원
【합계】 29,000 원
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】**【요약】**

본 발명은 하드 디스크 드라이브를 구비한 방송 수신 시스템에서 하드 디스크 드라이브에 데이터 저장시 허가되지 않은 제3자로부터 하드 디스크 드라이브의 저장정보를 보호하는 하드 디스크 드라이브 복사 방지장치에 있어서, 입력되는 다수 채널의 디지털 전송포트 데이터 스트림중 사용자에게 의해 선택 요구된 채널의 전송포트 데이터 스트림을 추출하여 디스크램블한 후, 출력시키는 TS 디멀티플렉서와, 상기 TS 디멀티플렉서로부터 디스크램블된 입력 전송포트 데이터 스트림을 다시 스크램블 처리하여 출력시키는 스크램블러와, 인크립트된 상기 스크램블러의 키를 입력하여 이를 디크립트한 후, 다시 새로이 인크립트하여 출력시키는 키인크립션부와, 저장시 상기 키인크립션부로부터 출력되는 인크립트된 상기 스크램블러의 키를 상기 스크램블러로부터 스크램블 처리된 전송포트 데이터 스트림과 함께 상기 하드 디스크 드라이브에 저장시키는 시스템 제어부를 포함하여 구성함을 특징으로 한다.

【대표도】

도 3

【색인어】

하드 디스크 드라이브, 방송 수신 시스템, 복사 방지, 스크램블, 인크립션

【명세서】

【발명의 명칭】

하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치 및 방법(A COPY PROTECTION APPARATUS AND METHOD OF A BROADCAST RECEIVING SYSTEM HAVING A HDD)

【도면의 간단한 설명】

도 1은 일반적인 하드 디스크를 구비한 방송 수신 시스템 블록 구성도,

도 2는 본 발명의 실시 예에 따른 하드 디스크를 구비한 방송 수신 시스템 블록 구성도,

도 3은 본 발명의 실시 예에 따른 키인크립션부의 상세 블록 구성도,

도 4는 본 발명의 실시 예에 따른 하드 디스크 드라이브의 복사 방지를 위한 동작 제어 흐름도.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 방송국 또는 네트워크를 통해 전송되는 다수 채널의 디지털 오디오/비디오 데이터를 재생 및 저장하는 방송 수신 시스템에 관한 것으로, 특히 저장장치로 하드 디스크 드라이브(Hard Disk Drive: 이하 'HDD'라 함)를 장착한 방송 수신 시스템에서 입력되는 폐쇄화된 디지털 트랜스포트 데이터 스트림을 하드 디스크에 저장시 제3자의 하드 디스크 복사

에 의한 정보 유출을 방지하는 장치 및 방법에 관한 것이다.

<6> 근래에 들어 컴퓨터 시스템의 보조기억장치인 HDD는 랜덤 액세스가 가능하며, 데이터 전송속도가 고속인 동시에 타 보조기억장치보다 저가이면서도 대용량화할 수 있다는 이점으로 인해 상기 방송 수신 시스템의 랜덤 액세스 저장장치로 사용되고 있다.

<7> 상기 방송국 또는 네트워크를 통해 전송되는 디지털 오디오/비디오 데이터는 통상적으로 MPEG표준으로 엔코딩(Encoding)되어 많은 프로그램 채널들의 데이터를 포함하는 패킷화된 디지털 트랜스포트 데이터 스트림으로 형성되어 전송된다. 이때 상기 프로그램 채널들의 데이터는 일반적으로 인크립션(Encryption) 및 스크램블(Scramble) 등과 같은 방법으로 암호화되어 상기 프로그램의 시청이 허가된 방송 수신 시스템내에서만 디코딩(Decoding)되도록 하여 왔다.

<8> 상기 내용을 종래 하드 디스크 드라이브가 장착된 방송 수신 시스템의 개략적인 블록 구성을 도시한 도 1을 참조하여 좀더 상세히 설명하면,

<9> 네트워크 또는 방송국을 통해 MPEG 표준으로 엔코딩되어 패킷화되고, 상기한 바와 같이 허가된 방송 수신 시스템내에서만 디코딩가능하도록 미리 스크램블 처리된 다수 채널의 트랜스포트 데이터 스트림(TS1)이 입력되는 경우 TS 디멀티플렉서(Transport Stream demultiplexer)(100)는 상기 입력된 MPEG 트랜스포트 데이터 스트림(TS1)에 포함된 인크립트된(Encrypted) 스크램블러의 키(Key)를

추출하여 스마트 카드(Smartcard)상에 미리 프로그램된 사용자 정보에 따라 디크립트(Decrypted)한 후, 상기 디크립트된 키와 함께 상기 입력된 트랜스포트 데이터 스트림(TS1)을 디스크램블러(Descrambler)(102)로 인가시킨다. 그러면 디스크램블러(102)는 상기 디크립트된 키를 이용하여 상기 입력된 트랜스포트 데이터 스트림(TS1)을 디스크램블 처리하여 출력시키게 된다. 이에 따라 상기 디스크램블 처리된 트랜스포트 데이터 스트림(TS2)은 사용자의 재생 또는 저장요구에 응답한 시스템 제어부(System Controller)(108)의 제어에 따라 A/V디코더(Audio/Video decoder)(106)로 입력되어 디코딩된 후, 방송 수신 시스템의 디스플레이 장치(도시하지 않았음)를 통해 디스플레이되거나, HDD 인터페이스부(110)를 통해 HDD(도시하지 않았음)에 저장되게 되는 것이다.

<10> 그런데 상기 도 1의 종래 방송 수신 시스템에서는 TS 디멀티플렉서를 통해 출력되는 디스크램블 처리된 트랜스포트 데이터 스트림을 HDD에 저장하는 경우에 있어 디스크램블 처리된 트랜스포트 데이터 스트림을 다시 디스크램블하는 별도의 처리없이 그대로 HDD에 저장시킴으로써 허가되지 않은 제3자에 의해 HDD가 복사되는 경우 HDD에 저장된 정보가 외부로 유출되는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<11> 상술한 바와 같이 종래 방송 수신 시스템에서는 TS 디멀티플렉서를 통해 출력되는 디스크램블 처리된 트랜스포트 데이터 스트림을 HDD에 저장하는 경우에 있어 디스크램블 처리된 트랜스포트 데이터 스트림을 다시 디스크램블하는 별도의 처리없이 그대로 HDD에 저장시킴으로써 허가되지 않은 제3자의 HDD 복사에 의한 저장정보의 유출을 방지할 수 없는 문제점이 있었다.

<12> 따라서 본 발명의 목적은 HDD를 구비한 방송 수신 시스템에서 HDD에 데이터 저장시 허가되지 않은 제3자로부터 HDD의 저장정보를 보호하는 HDD 복사 방지장치 및 방법을 제 공함에 있다.

【발명의 구성 및 작용】

<13> 상술한 목적을 달성하기 위한 본 발명은 HDD를 구비한 방송 수신 시스템에서 HDD에 데이터 저장시 허가되지 않은 제3자로부터 HDD의 저장정보를 보호하는 HDD 복사 방지장 치에 있어서, 입력되는 다수 채널의 디지털 트랜스포트 데이터 스트림중 사용자에 의해 선택 요구된 채널의 트랜스포트 데이터 스트림을 추출하여 디스크램블한 후, 출력시키는 TS 디멀 티플렉서와, 상기 TS 디멀티플렉서로부터 디스크램블된 입력 트랜스포트 데이터 스트림을 다시 스크램블 처리하여 출력시키는 스크램블러와, 인크립트된 상기 스크램블러의 키를 입 력하여 이를 디크립트한 후, 다시 새로이 인크립트하여 출력시키는 키인크립션부와, 저장시 상기 키인크립션부로부터 출력되는 인크립트된 상기 스크램블러의 키를 상기 스크램블러로 부터 스크램블 처리된 트랜스포트 데이터 스트림과 함께 상기 HDD에 저장시키는 시스템 제 어부를 포함하여 구성함을 특징으로 한다.

<14> 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기 설 명 및 첨부 도면에서 구체적인 처리 흐름과 같은 많은 특정 상세들이 본 발명의 보다 전반적 인 이해를 제공하기 위해 나타나 있다. 이들 특정 상세들없이 본 발명이 실시될 수 있다는 것 은 이 기술분야에서 통상의 지식을 가진 자에게 자명할 것이다. 그리고 본 발명의 요지를 불 필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

<15> 도 2는 본 발명의 실시 예에 따른 HDD 복사 방지기능이 구현된 방송 수신 시스템의 블록 구성을 도시한 것으로, 본 발명의 실시 예에 따른 방송 수신 시스템은 상기 도 1에 도시된 종래 방송 수신 시스템의 저장기능 수행 블록에 스크램블러와 키인크립션부를 새로이 추가하여 구성된다.

<16> 이제 상기 도 2를 참조하여 본 발명의 실시 예에 따른 방송 수신 시스템 각 부의 동작을 살펴보면, 상기 TS 디멀티플렉서(100)는 입력되는 트랜스포트 데이터 스트림을 디스크램블러(102) 및 스마트 카드(104)를 이용하여 디스크램블 처리되도록 하고 이를 스크램블러(200)를 통해 HDD인터페이스부(110)로 출력하며, 상기 스크램블러의 키를 소프트웨어적으로 인크립션하여 키인크립션부(Key encryption)(202)로 출력한다. 이때 키인크립션부(202)에 인크립트된 키를 전송하는 것은 인크립트하지 않은 키를 전송하여 새로운 인크립트 키를 생성시킬 경우 인크립트되지 않은 키와 인크립트된 키간의 직접적인 1:1관계가 쉽게 노출되는 것을 방지하기 위함이다.

<17> 상기 스크램블러(200)는 종래와는 달리 TS 디멀티플렉서(100)로부터 디스크램블 처리되어 출력되는 트랜스포트 데이터 스트림(TS2)을 HDD에 저장시키기 전에 다시한번 스크램블 처리를 수행하게 된다. 이때 상기 스크램블러(200)는 각 방송 수신 시스템 제작업체의 고유한 스크램블러를 사용하게 된다.

<18> 키인크립션부(202)는 상기 TS 디멀티플렉서(100)로부터 인가되는 인크립션 키를 입력받아 이를 디크립트한 후, 다시 인크립트하여 새로운 인크립션 키를 생성 출력시킨다. 이에 따라 스크램블러(200)로부터 스크램블 처리된 트랜스포트 데이터 스트림과 키인크립션부(202)로부터의 인크립트된 키가 맵핑되어 HDD에 저장되게 된다.

<19> 시스템 제어부는 상기 방송 수신 시스템 각 부의 동작을 제어하고 시스템 제어동작시

발생하는 데이터를 일시 저장하기 위한 램(RAM)과 시스템 제어 프로그램 데이터가 저장된 롬(ROM)으로 구성되는 메모리를 내부에 구비하며, 재생 및 저장을 동시에 지원하기 위한 일련의 제어동작을 수행한다.

<20> 상기 키인크립션부(202)의 상세 블록 구성을 도시한 도 3을 참조하여 상기 키인크립션부(202)의 동작을 좀더 상세히 살펴보면,

<21> 키인크립션부(202)의 마이크로 컨트롤러(300)는 상기 TS 디멀티플렉서(100)로부터 최초 인크립트된 상기 스크램블러의 키를 입력받으면 이를 디크립트한 후, 메모리(304)에 저장된 난수를 이용하여 상기 디크립트된 키를 새로이 인크립트하여 출력시킨다. 난수 생성부(Random Number Generator)(302)는 방송 수신 시스템의 최초 동작시 난수를 생성시키며, 타 방송 수신 시스템에서 상기 HDD에 저장된 데이터 스트림이 디스크램블되는 것을 방지하기 위해 각 방송 수신 시스템마다 서로 다른 초기값을 갖게 한다.

<22> 도 3은 본 발명의 실시 예에 따라 HDD를 구비한 방송 수신 시스템에서 HDD에 데이터 저장시 허가되지 않은 제3자로부터 HDD의 저장정보를 보호하는 HDD 복사 방지를 시스템 제어부에서의 동작 제어 흐름을 도시한 것이다. 이하 상기 도 2 및 도 3을 참조하여 본 발명의 실시 예를 상세히 설명한다.

<23> 먼저 네트워크 또는 방송국을 통해 스크램블된 MPEG 트랜스포트 데이터 스트림이 입력되는 경우 시스템 제어부(108)는 TS 디멀티플렉서(100), 디스크램블러(102) 등 프로그램 재생에 필요한 각 부를 제어하여 사용자에게 의해 선택된 특정 채널의 프로그램이 방송 수신 시스템의 디스플레이 장치를 통해 디스플레이되도록 한다.

<24> 즉, 전술한 바와 같이 TS 디멀티플렉서(100)는 시스템 제어부(108)의 제어에 따라

네트워크 또는 방송국을 통해 입력되는 스크램블된 MPEG 트랜스포트 데이터 스트림(TS1) 중 사용자에게 의해 선택된 특정 채널의 프로그램 데이터 스트림을 선택하여 이를 디스크램블러(102)에 전송하고, 상기 입력 트랜스포트 데이터 스트림에 포함된 인크립트된 스크램블러 키를 스마트 카드(104)상에 미리 프로그램된 사용자 정보에 따라 디크립트하여 디크립트된 키를 디스크램블러(102)로 전송한다. 그러면 디스크램블러(102)는 상기 TS 디멀티플렉서(100)로부터 인가된 디크립트된 스크램블러 키를 이용하여 상기 입력 트랜스포트 데이터 스트림(TS1)을 디스크램블한다. 따라서 상기 디스크램블된 트랜스포트 데이터 스트림(TS2)이 A/V디코더(106)로부터 디코딩되어 방송 수신 시스템의 디스플레이장치로 디스플레이되거나 HDD인터페이스부(110)를 통해 HDD에 저장되는 것이다. 이에 따라 사용자는 시청하고자 하는 임의의 채널에 대한 프로그램을 시청할 수 있게 된다.

<25> 그리고 이때 사용자는 저장하고자 하는 프로그램이 있는 경우 방송 수신 시스템에 구비된 키입력부 또는 리모트 컨트롤러(도시하지 않았음) 등을 이용하여 저장 명령을 입력시키게 되는데, 상기와 같이 키입력부 또는 리모트 컨트롤러를 통해 사용자로부터의 저장 명령이 있는 경우 시스템 제어부(108)는 (400)단계에서 이에 응답하여 상기 저장요구된 프로그램의 데이터를 HDD에 저장하기 위한 본 발명의 실시 예에 따른 일련의 동작을 수행하게 된다.

<26> 즉, 상기 저장 명령에 응답한 시스템 제어부(108)는 상기 (400)단계에서 (402)단계로 진행해서 TS 디멀티플렉서(100)로부터 디스크램블되어 출력되는 해당 프로그램의 트랜스포트 데이터 스트림을 스크램블러(200)를 통해 다시 스크램블 처리시킨다. 이어 시스템 제어부(108)는 (404)단계로 진행하여 스크램블러 키를 소프트웨어적으로 인크립트하여 키인크립션부(202)로 인가한다. 이때 상기 키인크립션부(202)에 키를 인크립트하여 인가되

는 것은 전술한 바와 같이 키를 인크립트하지 않고 키인크립션부로 인가하는 경우 상기 키인크립션부(202)로부터 생성된 인크립트된 키와 키인크립션부(202)로 인가되기 전의 인크립트되지 않은 키간의 직접적인 1:1관계가 쉽게 노출되는 것을 방지하기 위함이다. 이에 따라 키인크립션부(202)에서는 상기 인크립트된 키가 디크립트된 후, 다시 인크립트되어 새로이 인크립트된 키가 출력되게 된다. 그러면 시스템 제어부(108)는 (406)단계로 진행하여 상기 키인크립션부(202)로부터 출력된 인크립트된 키와 상기 스크램블러(200)로부터 스크램블 처리된 해당 프로그램의 트랜스포트 데이터 스트림을 HDD인터페이스부(110)를 통해 HDD에 저장시킨다. 이어 시스템 제어부(108)는 (408)단계로 진행하여 키입력부 또는 리모트 컨트롤러를 통해 사용자로부터 저장 중지 요구가 있는지 여부를 검사하고, 저장 중지 요구가 없는 경우에는 상기 (402)단계로 돌아가서 다시 상기 (402)~(406)단계를 수행하면서 해당 프로그램의 트랜스포트 데이터 스트림을 스크램블하고 스크램블러 키를 새로이 인크립트하여 HDD에 저장시키며, 이와 달리 저장 중지 요구가 있는 경우 시스템 제어부(108)는 저장 동작을 종료하게 된다.

<27> 따라서 HDD를 구비한 방송 수신 시스템에서 HDD에 데이터 저장시 디스크램블된 데이터 스트림을 다시 한번 고유의 방식으로 스크램블 처리하여 저장시킴으로써 제3자의 HDD 복사에 의한 정보 유출을 방지할 수 있게 된다.

【발명의 효과】

<28> 상술한 바와 같이 본 발명은 HDD를 구비한 방송 수신 시스템에서 HDD에 데이터 저장

시 디스크램블된 데이터 스트림을 다시 한번 고유의 방식으로 스크램블 처리하여 저장시킴으로써 제3자의 HDD복사에 의한 정보 유출을 방지할 수 있게 되는 이점이 있다.

【특허청구범위】

【청구항 1】

하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치에 있어서,

입력되는 다수 채널의 디지털 전송포트 데이터 스트림중 사용자에게 의해 선택 요구된 채널의 전송포트 데이터 스트림을 추출하여 디스크램블한 후, 출력시키는 TS 디멀티플렉서와

상기 TS 디멀티플렉서로부터 디스크램블된 입력 전송포트 데이터 스트림을 다시 디스크램블시켜 출력시키는 스크램블러와,

인크립트된 상기 스크램블러의 키를 입력하여 이를 디크립트한 후, 다시 새로이 인크립트하여 출력시키는 키인크립션부와,

저장시 상기 키인크립션부로부터 출력되는 인크립트된 상기 스크램블러의 키를 상기 스크램블러로부터 스크램블 처리된 전송포트 데이터 스트림과 함께 상기 하드 디스크 드라이브에 저장시키는 시스템 제어부로 이루어짐을 특징으로 하는 하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치.

【청구항 2】

제1항에 있어서, 상기 키인크립션부는,

상기 방송 수신 시스템의 최초 동작시 난수를 발생시키는 난수 생성부와,

상기 난수 생성부로부터 발생된 난수를 저장하는 불휘발성 메모리와,

상기 스크램블러의 인크립트된 키를 입력받으면 이를 디크립트한 후, 상기 메모리에 저장된 난수를 이용하여 상기 디크립트된 키를 새로이 인크립트하여 출력시키는 마이크로 콘트롤러로 구성됨을 특징으로 하는 하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치.

【청구항 3】

제2항에 있어서, 상기 난수 생성부는,

타 방송 수신 시스템에서 상기 하드 디스크에 저장된 데이터 스트림이 디스크램블되는 것을 방지하기 위해 각 방송 수신 시스템마다 서로 다른 초기값을 발생시킴을 특징으로 하는 하드 디스크 드라이브를 구비하는 방송 수신 시스템의 복사 방지장치.

【청구항 4】

하드 디스크 드라이브를 구비하는 방송 수신 시스템내 TS 디멀티플렉서, 스크램블러, 키인크립션부를 적어도 구비하는 복사 방지장치에서 상기 하드 디스크 드라이브의 복사를 방지하는 방법에 있어서,

저장시 상기 TS 디멀티플렉서로부터 디스크램블된 트랜스포트 데이터 스트림을 상기 스크램블러를 통해 다시 스크램블 처리하는 과정과,

상기 스크램블러의 키를 인크립트하여 상기 키인크립션부로 인가시키는 과정과,

상기 키인크립션부로부터 새로이 인크립트되어 출력되는 키를 상기 스크램블 처리된

트랜스포트 데이터 스트림과 함께 상기 하드 디스크 드라이브에 저장시키는 과정으로 이루어짐을 특징으로 하는 하드 디스크 드라이브를 구비한 방송 수신 시스템의 복사 방지방법.