(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년12월03일
(11) 등록번호 10-0781531
(24) 등록일자 2007년11월27일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2006-0090886
(22) 출원일자 2006년09월19일
심사청구일자 2006년09월19일
(56) 선행기술조사문헌
KR1020020029802 A

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
김형식
서울 서대문구 창천동 68-19 정년 유스빌 401호
장명수
서울 구로구 개봉3동 278-29호 20/1
김상현
서울 성북구 동선동3가 23번지 403호
(74) 대리인
정상빈, 특허법인가산

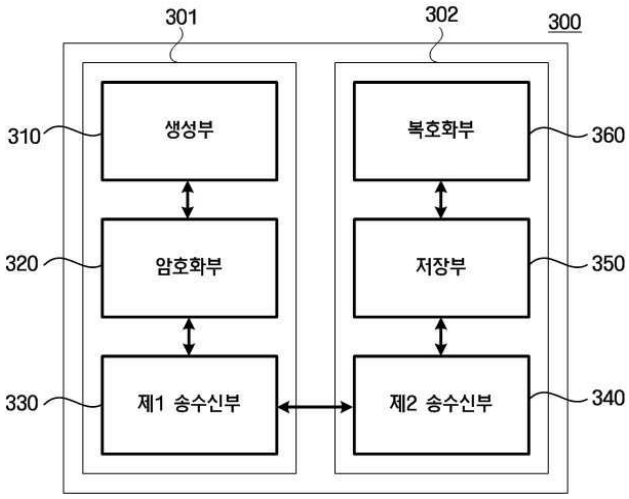
전체 청구항 수 : 총 11 항 심사관 : 장대근

(54) 컨텐츠 서비스 제공 방법 및 장치

(57) 요 약

컨텐츠 서비스 제공 방법 및 장치를 제공한다. 컨텐츠 서비스 제공 방법은 소정 컨텐츠에 대한 연속된 서비스 사용기간에 대응되는 복수개의 해독정보를 생성하는 단계와 컨텐츠를 암호화하는 단계 및 해독정보를 이용하여 암호화된 컨텐츠를 복호화하는 단계를 포함한다.

대표도 - 도3



특허청구의 범위

청구항 1

소정 컨텐츠에 대한 연속된 서비스 사용기간에 대응되는 복수개의 해독정보를 생성하는 단계;

상기 컨텐츠를 암호화하는 단계;

상기 해독정보를 이용하여 상기 암호화된 컨텐츠를 복호화하는 단계를 포함하는, 컨텐츠 서비스 제공 방법.

청구항 2

제 1항에 있어서,

상기 해독정보는 제1 해독정보 및 제2 해독정보로 구성되고, 상기 제1 해독정보는 상기 연속된 방송 서비스 사용기간의 시작 시간으로부터 포워드(forward)방향으로 단방향 해쉬 함수를 통해 생성되고, 상기 제2 해독정보는 상기 연속된 방송 서비스 사용기간의 만료 시간으로부터 백워드(backward)방향으로 단방향 해쉬 함수를 통해 생성되는, 컨텐츠 서비스 제공 방법.

청구항 3

제 1항에 있어서,

상기 해독정보는 상기 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경되고, 상기 암호화된 컨텐츠가 상기 변경된 값에 대응되게 복호화되는, 컨텐츠 서비스 제공 방법.

청구항 4

제 1항에 있어서,

상기 암호화된 컨텐츠는 상기 해독정보 생성시 사용된 단방향 해쉬 함수를 이용하여 생성되어 상기 컨텐츠 서비스의 가입자들에게 공통적으로 제공되는, 컨텐츠 서비스 제공 방법.

청구항 5

제 4항에 있어서,

상기 공통적으로 제공되는 암호화된 컨텐츠는 상기 가입자들의 해독정보에 따라 상기 가입자들의 연속된 방송 서비스 사용기간에 대응되도록 복호화되는, 컨텐츠 서비스 제공 방법.

청구항 6

소정 컨텐츠에 대한 연속된 서비스 사용기간에 대응되는 복수개의 해독정보를 생성하는 생성부;

상기 컨텐츠를 암호화하는 암호화부;

상기 해독정보를 이용하여 상기 암호화된 컨텐츠를 복호화하는 복호화부를 포함하는, 컨텐츠 서비스 제공 장치.

청구항 7

제 6항에 있어서,

상기 해독정보는 제1 해독정보 및 제2 해독정보로 구성되고, 상기 제1 해독정보는 상기 연속된 방송 서비스 사용기간의 시작 시간으로부터 포워드(forward)방향으로 단방향 해쉬 함수를 통해 생성되고, 상기 제2 해독정보는 상기 연속된 방송 서비스 사용기간의 만료 시간으로부터 백워드(backward)방향으로 단방향 해쉬 함수를 통해 생성되는, 컨텐츠 서비스 제공 장치.

청구항 8

제 6항에 있어서,

상기 해독정보는 상기 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경되고, 상기 암호화된 컨텐츠가 상기 변경된 값에 대응되게 복호화되는, 컨텐츠 서비스 제공 장치.

청구항 9

제 6항에 있어서,

상기 암호화된 컨텐츠는 상기 해독정보 생성시 사용된 단방향 해쉬 함수를 이용하여 생성되어 상기 컨텐츠 서비스의 가입자들에게 공통적으로 제공되는, 컨텐츠 서비스 제공 장치.

청구항 10

제 9항에 있어서,

상기 공통적으로 제공되는 암호화된 컨텐츠는 상기 가입자들의 해독정보에 따라 상기 가입자들의 연속된 방송 서비스 사용기간에 대응되도록 복호화되는, 컨텐츠 서비스 제공 장치.

청구항 11

소정 컨텐츠에 대한 연속된 서비스 사용기간의 시작 시간으로부터 포워드(forward)방향의 제1 해독정보 및 상기 연속된 방송 서비스 사용기간의 만료 시간으로부터 백워드(backward)방향의 제2 해독정보를 단방향 해쉬 함수를 통해 생성하는 생성부;

상기 제1 해독정보 및 제2 해독정보 생성시 이용된 단방향 해쉬 함수를 이용하여 컨텐츠를 암호화하는 암호화부; 및

상기 암호화된 컨텐츠, 상기 제1 해독정보 및 제2 해독정보를 전송하는 제1 송수신부를 포함하는, 서비스 암호화부 및

상기 암호화된 컨텐츠를 수신하는 제2 송수신부; 및

상기 전송받은 암호화 컨텐츠를 상기 제1 해독정보 및 제2 해독정보를 이용하여 복호화하는 복호화부를 포함하는, 서비스 복호화부를 포함하고, 상기 제1 해독정보 및 제2 해독정보는 상기 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경되고, 상기 암호화된 컨텐츠가 상기 변경된 값에 대응되게 복호화되는, 컨텐츠 서비스 제공 장치.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<11> 본 발명은 컨텐츠 서비스 제공 방법 및 장치에 관한 것으로서, 더욱 상세하게는 컨텐츠 서비스를 이용하는 가입자가 복수개의 해독정보를 이용하여 자신이 가입한 컨텐츠 서비스 사용기간 동안 암호화된 컨텐츠를 복호화하여 컨텐츠를 제공받는 컨텐츠 서비스 제공 방법 및 장치에 관한 것이다.

<12> 방송 서비스는 일반적으로 특정 수신자를 대상으로 “일 대 일”로 전송되는 방식이 아닌, 불특정 N명의 수신자를 대상으로 “일 대 N” 의 방식으로 전송되는 특징을 가진다. 그리고, 정당한 시청 권한을 가진 방송 서비스 가입자(이하 가입자라 함)만이 특정 방송 컨텐츠를 수신할 수 있게 하고, 가입자에게 어느 특정 방송 컨텐츠에 대한 수신가능 여부를 각각의 디지털 방송 수신기가 결정하도록 하는 시스템이 사용되어 왔다.

<13> 도 1은 종래 방송 서비스 제공의 개념도이다.

<14> 방송 서비스 제공자는 방송 서비스에 대해서 권한이 있는 가입자에 대해서만 방송 서비스를 제공하기 원하고, 가입자는 자신이 원하는 기간 동안 방송 서비스를 제공받기를 원한다.

<15> 이를 위해, 종래의 방송 서비스를 제공하기 위한 암호화 시스템은 마스터 키(master key)(이하 Km이라 함) 처리부, 워크 키(work key)(이하 Kw라 함) 처리부, 스크램블 키(scramble key)(이하 Ks라 함) 처리부로 구성된다. 상기 Ks는 방송 컨텐츠를 암호화하는 키로 사용되며, Kw는 가입자가 방송 서비스 제공자와 계약한 방송 서비스 사용기간에 대응되도록 생성된다. 그리고, Km은 각 가입자 별로 유일한 고유키이다.

<16> 먼저, 방송 서비스를 제공하는 송신측(2)에서의 과정을 살펴보면, 가입자는 인증 프로토콜을 이용하여 송신측(2)과 통신하고, 인증이 성공적으로 끝날 경우, 송신측(2)으로부터 Km을 획득한다. 획득한 Km은 각 가입자 별로 유일하며 방송 서비스를 제공받는 수신측(4)의 소정 저장 장소에 저장된다. 또한, 이때 Kw, Ks도 함께 가입자로 전달한다.

<17> 다음 단계에서, 송신측(2)은 방송 컨텐츠를 Ks를 이용하여 암호화하고, Ks는 다시 Kw를 통해 암호화된다. 그리고, Kw는 가입자의 계약 정보(contract information)와 함께 Km을 통해 암호화되어 수신측(4)에 전달된다.

<18> 수신측(4)에서는 이미 Km, Kw, Ks 키를 송신측(2)으로부터 전달받아 저장하고 있으므로, 송신측(2)의 방송 컨텐츠를 암호화하는 순서의 역순으로 복호화(decryption)를 수행한다. 즉, 암호화된 방송 컨텐츠를 제공받은 경우 저장된 Km을 통해 Kw와 계약 정보를 복호화하고, 다시 저장된 Kw를 통해 Ks를 복호화한다. 또한, Ks를 통해 암호화된 방송 컨텐츠를 복호화하고 방송 컨텐츠에 접근한다.

<19> 그러나, 종래에는 방송 서비스 제공자가 가입자별로 서로 다른 방송 서비스 사용기간을 제공하고자 할 경우, 기존 가입자들은 다른 가입자가 방송 서비스 제공자와 방송 서비스에 대한 새로운 계약을 맺을 때마다, 방송 서비스 관련 키 (예를 들어 Kw)에 대해 업데이트 수행해야 했다. 따라서 키 관리 및 유지의 복잡성, 그로 인해 송수신되는 송신측(2)과 수신측(4)간의 데이터 교환의 증가에 따른 문제가 있었다. 이러한 문제점들에 대해서 이하 도2에서 보다 구체적으로 설명하기로 한다.

<20> 도 2는 종래 방송 서비스 제공에 있어서 키 분배의 개념도이다.

<21> 상기한 바와 같이, 방송 서비스 제공자는 허가된 가입자에게만 방송 서비스를 제공하기 위해 방송 컨텐츠를 암호화하여 제공한다. 그리고, 가입자는 방송 서비스 제공자와 방송 서비스에 대한 계약시 수신한 키(Km, Kw, Ks)를 이용하여 상기 제공받은 방송 컨텐츠를 복호화하여 이용하게 된다.

<22> 예를 들어 도 2에 도시된 바와 같이, 가입자1(C1)이 방송 서비스 제공자와 계약을 맺고, 제1 사용기간(12) 동안 방송 서비스를 제공받고자 한다. 마찬가지로, 가입자2(C2)은 제2 사용기간(14) 동안 그리고 가입자3(C3)은 제3 사용기간(16) 동안 방송 서비스 제공자와 계약을 맺고 방송 서비스를 제공받고자 한다. 방송 서비스 제공자는 가입자1과 방송 서비스에 대한 계약을 맺고, 제1 사용기간(12)에 대응되도록 생성된 Kw를 가입자1의 Km으로 암호화하여 제공한다. 또한, 방송 서비스 제공자가 가입자2와 방송 서비스에 대한 계약을 맺게 될 경우, 방송 서비스 제공자는 제2 사용기간(14)에 대응되도록 생성된 Kw를 가입자2의 Km으로 암호화하여 제공한다. 이후, 방송 컨텐츠는 방송 서비스 사용기간 동안 각 시간 단위(10)마다 암호화(11)되어 가입자들에게 전송된다. 이때, Ks는 수초별로 항시 업데이트되고, Kw는 신규 가입자가 가입할 때마다 업데이트되어야 한다. 이와 같이, 가입자수가 늘어날수록 키 분배 및 유지, 관리해야 하는 키가 늘어나는 문제점이 있다.

<23> 그리고 방송 컨텐츠가 암호화되어 제공되면, 가입자들은 자신의 Km, Kw, Ks 키를 이용하여 암호화된 방송 컨텐츠를 복호화하여 방송 서비스를 제공받게 된다.

<24> 한편, 가입자 C1, C3가 동일 방송 서비스 시간 단위(18)에서 방송 서비스를 제공받고 있을 때, 만약 가입자 C3가 방송 서비스를 해약하고 탈퇴할 경우에는, 탈퇴한 가입자 C3가 더 이상 방송 서비스를 제공받지 못하도록 방송 서비스 제공자는 가입자 C1의 키를 새롭게 업데이트하고 방송 서비스를 제공한다. 이와 같이, 종래에는 기존 가입자 입장에서 다른 가입자가 탈퇴하거나 신규 가입자가 방송 서비스를 제공받고자 가입할 경우, 기존 가입자가 새로운 키를 다시 업데이트 받아야 하는 문제점이 있다.

<25> 따라서 종래의 방송 서비스 제공을 위한 복잡한 키 분배, 관리 및 유지를 개선하고, 보다 효율적으로 방송 서비스를 사용자에게 제공할 필요성이 제공된다.

발명이 이루고자 하는 기술적 과제

<26> 본 발명은 컨텐츠 서비스 제공 방법 및 장치를 제공하여, 컨텐츠 서비스를 이용하는 가입자가 복수개의 해독정보를 이용하여 자신이 가입한 컨텐츠 서비스 사용기간 동안 암호화된 컨텐츠를 복호화하여 컨텐츠를 제공받을 수 있게 하는 데 그 목적이 있다.

<27> 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해되어질 수 있을 것이다.

발명의 구성 및 작용

<28> 상기 목적을 달성하기 위하여, 본 발명의 실시예에 따른 컨텐츠 서비스 제공 방법은 소정 컨텐츠에 대한 연속된 서비스 사용기간에 대응되는 복수개의 해독정보를 생성하는 단계와 컨텐츠를 암호화하는 단계 및 해독정보를 이용하여 암호화된 컨텐츠를 복호화하는 단계를 포함한다.

<29> 본 발명의 실시예에 따른 컨텐츠 서비스 제공 장치는 소정 컨텐츠에 대한 연속된 서비스 사용기간에 대응되는 복수개의 해독정보를 생성하는 생성부와 컨텐츠를 암호화하는 암호화부 및 해독정보를 이용하여 암호화된 컨텐츠를 복호화하는 복호화부를 포함한다.

<30> 본 발명의 다른 실시예에 따른 컨텐츠 서비스 제공 장치는 소정 컨텐츠에 대한 연속된 서비스 사용기간의 시작 시간으로부터 포워드(forward)방향의 제1 해독정보 및 연속된 방송 서비스 사용기간의 만료 시간으로부터 백워드(backward)방향의 제2 해독정보를 단방향 해쉬 함수를 통해 생성하는 생성부와 제1 해독정보 및 제2 해독정보 생성시 이용된 단방향 해쉬 함수를 이용하여 컨텐츠를 암호화하는 암호화부 및 암호화된 컨텐츠, 제1 해독정보 및 제2 해독정보를 전송하는 제1 송수신부를 포함하는, 서비스 암호화부 및 암호화된 컨텐츠를 수신하는 제2 송수신부 및 전송받은 암호화 컨텐츠를 제1 해독정보 및 제2 해독정보를 이용하여 복호화하는 복호화부를 포함하는, 서비스 복호화부를 포함하고, 제1 해독정보 및 제2 해독정보는 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경되고, 암호화된 컨텐츠가 상기 변경된 값에 대응되게 복호화된다.

<31> 기타 실시예들의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

<32> 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

<33> 도 3는 본 발명의 일 실시예에 따른 컨텐츠 서비스 제공 장치의 블록도이다.

<34> 이하 실시예에서는 본 발명을 설명하기 위해 방송 서비스를 예로 들어 설명하지만, 이에 한정되지 아니하고 시간의 순서대로 또는 연속적으로 사용자에게 제공되는 컨텐츠 서비스들에 대해서 본 발명이 적용가능하다.

<35> 컨텐츠 서비스 제공 장치(300)는 서비스 암호화부(301)와 서비스 복호화부(302)로 구성되고, 서비스 암호화부(301)는 생성부(310), 암호화부(320), 및 제1 송수신부(330)를 포함한다. 그리고, 서비스 복호화부(302)는 제2 송수신부(340), 저장부(350), 및 복호화부(360)를 포함한다. 상기 서비스 암호화부(301)는 방송 서비스를 제공하는 송신측의 기기에 설치될 수 있으며, 서비스 복호화부(302)는 방송 서비스를 제공받는 수신측의 기기에 설치될 수 있다.

<36> 먼저 서비스 암호화부(301)의 구성 요소에 대해서 설명하기로 한다.

<37> 생성부(310)는 가입자가 가입한 연속된 방송 서비스 사용기간에 대응되는 암호화된 방송 컨텐츠를 해독할 수 있는 복수개의 해독정보를 생성한다. 생성된 해독정보는 후술될 제1 송수신부(330)를 통해 전송되어 저장부(350)에 저장된다. 이때, 해독정보의 생성에는 단방향 해쉬 함수가 사용되어, 후술될 복호화부(360)가 가입자의 방송 서비스 사용기간에 대응되는 암호화된 방송 컨텐츠를 해독할 수 있도록 할 수 있다. 상기 해독정보는 최초 1회 제1 송수신부(330)를 통해 전송될 수 있고, 암호화된 방송 컨텐츠는 해독정보를 통해 각 가입자가 가입한 연속된 방송 서비스 사용기간 동안 복호화되어 가입자들에게 제공된다.

<38> 상기 해독정보는 제1 해독정보 및 제2 해독정보로 구성될 수 있다. 제1 해독정보는 연속된 방송 서비스 사용기간의 시작 시간으로부터 포워드(forward)방향으로 단방향 해쉬 함수를 통해 생성되고, 제2 해독정보는 연속된 방송 서비스 사용기간의 만료 시간으로부터 백워드(backward)방향으로 단방향 해쉬 함수를 통해 생성된다. 그리고, 해독정보는 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경되고, 암호화된 컨텐츠가 상기 변경된 값에 대응되게 복호화되므로, 종래의 시간 단위의 복잡한 키 분배의 문제가 해결될 수 있다.

<39> 따라서, 예를 들어 가입자(A)가 소정의 연속된 방송 서비스 사용기간(T_i 내지 T_j)에 대해서 방송 서비스에 가입한 경우, T_i 내지 T_j 기간에 대해서 제1 및 제2 해독정보의 값이 자동으로 변경되므로, 가입자(A)는 별도의 해독정보를 수신하지 않고도 연속된 방송 서비스 사용기간 동안 방송 컨텐츠를 지속적으로 제공받을 수 있게 된다. 그리고, 가입자(A)는 해당 기간이 만료되면 더 이상 방송 서비스를 이용 받을 수 없게 되는 데, 그 이유는 연속된 방송 서비스 사용기간에 대응되도록 제1 및 제2 해독정보가 단방향 해쉬 함수를 통해 생성되었기 때문이다.

<40> 암호화부(320)는 가입자에게 제공할 방송 컨텐츠를 암호화한다. 이때, 상기 단방향 해쉬 함수를 이용하여 방송 컨텐츠를 암호화할 수 있다. 보다 구체적인 방송 컨텐츠를 암호화하는 방법은 이하 도 5를 참조하기 바란다.

<41> 제1 송수신부(330)는 해독정보 및 암호화된 방송 컨텐츠를 제2 송수신부(340)로 전송한다.

<42> 다음으로 서비스 복호화부(302)의 구성 요소에 대해서 설명하기로 한다.

<43> 제2 송수신부(340)는 제1 송수신부(330)로부터 수신된 해독정보를 저장부(350)에 저장하고, 암호화된 방송 컨텐츠를 복호화부(360)로 전송한다.

<44> 저장부(350)는 해독정보 및 기타 다양한 데이터를 저장한다.

<45> 복호화부(360)는 암호화된 방송 컨텐츠를 제2 송수신부(340)를 통해 수신하고, 저장부(350)에 저장되어 있는 해독정보를 이용하여 가입자가 가입한 방송 서비스 사용기간에 대해 암호화된 방송 컨텐츠를 복호화한다. 상기 암호화된 방송 컨텐츠는 상기 해독정보 생성시 사용되었던 단방향 해쉬 함수를 이용하여 생성되었으므로, 저장부(350)에 저장되어 있는 해독정보를 이용하여 가입자가 가입한 방송 서비스 사용기간에 대해 암호화된 방송 컨텐츠를 복호화할 수 있게 된다.

<46> 도 3에서 도시된 각각의 구성요소는 일종의 '모듈'로 구성될 수 있다. 상기 '모듈'은 소프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체(Application Specific Integrated Circuit, ASIC)과 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 따라서, 일 예로서 모듈은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.

<47> 도 4은 본 발명의 일 실시예에 따른 컨텐츠 서비스 제공 방법의 순서도이다.

<48> 생성부(310)는 가입자가 가입한 연속된 방송 서비스 사용기간에 대응되는 복수개의 해독정보를 생성한다(S401). 이때, 해독정보는 단방향 해쉬 함수를 이용하여 제1 및 제2 해독정보로 생성된다. 그리고, 제1 및 제2 해독정보의 값은 연속적인 방송 서비스 사용기간 동안 자동으로 변경된다.

<49> 다음 단계에서, 제1 송수신부(330)는 생성된 해독정보를 제2 송수신부(340)로 전송하고, 수신된 해독정보는 저장부(350)에 저장된다(S411).

<50> 그리고, 암호화부(320)는 가입자에게 제공할 방송 컨텐츠를 암호화한다(S421). 이때, 상기 단방향 해쉬 함수를 이용하여 방송 컨텐츠를 암호화할 수 있다. 따라서 암호화된 방송 컨텐츠가 수신측에 전송되면 상기 해독정보를 통해 가입자가 가입한 연속된 방송 서비스 사용기간에 대해서 복호화될 수 있다. 그리고 다수의 가입자가 있을 경우에도 가입자들은 자신의 방송 서비스 사용기간에 대해서 복호화된 방송 컨텐츠를 연속된 방송 서비스 사용기간에 대해서 제공받을 수 있게 된다.

<51> 다음 단계에서, 제1 송수신부(330)는 암호화된 방송 컨텐츠를 제2 송수신부(340)로 전송한다(S431).

<52> 그리고, 복호화부(360)는 암호화된 방송 컨텐츠를 제2 송수신부(340)를 통해 수신하고, 저장부(350)에 저장되어 있는 해독정보를 이용하여 가입자가 가입한 방송 서비스 사용기간에 대해 암호화된 방송 컨텐츠를 복호화한다(S441).

<53> 도 5는 본 발명의 일 실시예에 따른 방송 서비스 제공의 일 예를 도시한다. 도시된 바와 같이, 방송 서비스가 제공되는 사용 기간이 단방향 즉, 왼쪽에서 오른쪽 방향으로 시간의 순서대로 복수개의 시간 단위(502)로 표시되어 있다.

<54> 예를 들어 가입자가 방송 서비스 제공자와 계약을 맺고, 방송 서비스를 방송 서비스 시작 시점인 Ti(504)에서 방송 서비스 종료 시점인 Tj(506)까지의 연속된 방송 서비스 사용기간 동안 제공받으려고 한다.

<55> 먼저 방송 서비스를 제공하는 송신측에서의 동작을 설명하기로 한다.

<56> 생성부(310)는 Ti(504) 시간에 대응되는 제1 해독정보 및 Tj(506) 시간에 대응되는 제2 해독정보를 생성한다.

제1 및 제2 해독정보는 암호화된 방송 컨텐츠를 해독할 때 이용되는 정보이다.

<57> 구체적으로 Ti(504) 시간에 대응되는 제1 해독정보는 수학식 1과 같이 나타낼 수 있다.

<58> (수학식 1)

<59> 제1 해독정보 = $H_F^i(S_F)$

<60> 수학식 1에서, H_F는 제1 단방향 해쉬 함수, S_F는 제1 난수값을 나타낸다. 여기서, 단방향 해쉬 함수는 메시지 원본에 대해서 역변환이 불가능한 함수를 의미한다. 그리고, 상기 S_F는 방송 서비스 제공자만이 알고 있는 비밀값일 수 있다. 따라서 i값이 증가할수록 포워드(forward)방향으로 제1 해독정보가 생성됨을 알 수 있다.

<61> 또한, Tj(506) 시간에 대응되는 제2 해독정보는 수학식 2과 같이 나타낼 수 있다.

<62> (수학식 2)

<63> 제2 해독정보 = $H_B^{n-j+1}(S_B)$

<64> 수학식 2에서, H_B는 제2 단방향 해쉬 함수, S_B는 제2 난수값을 나타낸다. 이때 j값이 증가할수록 백워드(forward)방향으로 제2 해독정보가 생성된다.

<65> 따라서 Ti(504) 내지 Tj(506) 까지의 연속된 방송 서비스 사용기간에 대해 가입자는 제1 및 제2 해독정보를 가지고 방송 서비스를 제공받을 수 있게 된다.

<66> 이때, 상기 제1 및 제2 해독정보는 최초 1회 가입자에게 전달되고, 연속된 방송 서비스 사용기간 동안 자동으로 값이 변경된다. 따라서 변경된 값에 따라 수신된 암호화된 컨텐츠가 복호화되어, 종래 시간 단위(502)마다 암호화 키들이 생성되어 가입자에게 배포되는 복잡한 키 분배 문제가 해결될 수 있다.

<67> 다음 단계에서, 암호화부(320)는 방송 컨텐츠를 암호화하여 가입자에게 제1 송수신부(330)를 통해 전송한다. 이때, 바람직하게는 수학식 3의 형태로 방송 컨텐츠가 암호화될 수 있다.

<68> (수학식 3)

<69> 암호화된 방송 컨텐츠 = $C(H_F^i(S_F), H_B^{n-j+1}(S_B))$

<70> 수학식 3에서, C는 컴포지트(composite) 연산자로서, 바람직하게는 XOR 연산자일 수 있으며, 상기 S_F, S_B는 방송 서비스 제공자만이 알고 있는 비밀값일 수 있다. 따라서 방송 서비스 제공자는 모든 가입자에 대해서 암호화된 방송 컨텐츠를 공통적으로 제공할 수 있게 된다.

<71> 다음으로, 방송 서비스를 제공받는 수신측에서의 동작을 설명하기로 한다.

<72> 복호화부(360)는 상기 제2 송수신부(340)로부터 전송받은 제1 및 제2 해독정보를 이용하여 암호화된 방송 컨텐츠를 가입자의 방송 서비스 사용기간에 대응되는 부분에 대해서 복호화한다. 따라서 가입자는 자신의 방송 서비스 사용기간 동안 해당 방송 컨텐츠를 이용할 수 있게 된다.

<73> 이때, 연속적인 방송 서비스 사용기간 동안 제1 및 제2 해독정보의 값은 자동으로 변경되므로, 가입자는 방송 서비스 사용기간 동안 방송 컨텐츠를 지속적으로 제공받을 수 있고, 방송 서비스 사용기간이 만료되면 자동으로 방송 서비스가 중단되게 된다. 즉, 단방향 해쉬 함수를 이용하여 생성된 제1 및 제2 해독정보가 가입자에게 전달되어 각 가입자는 자신의 방송 서비스 사용기간(Ti(504) 내지 Tj(506)) 동안 연속적으로 방송 컨텐츠를 제공받을 수 있게 된다.

<74> 이와 같이, 가입자가 가입한 연속된 방송 서비스 사용기간에 대응되는 최초 상기 제1 및 제2 해독정보가 가입자에게 제공되면, 가입자는 2개의 해독정보를 이용하여 자신이 가입한 방송 서비스 사용기간 동안 방송 컨텐츠를 제공받을 수 있게 된다. 그리고, 신규 가입자가 늘어날 경우에도 최초 제공받은 제1 및 제2 해독정보를 통해 연속적으로 방송 서비스를 가입자의 방송 서비스 사용기간 동안 제공받을 수 있어, 종래 다른 가입자의 탈퇴 또는 신규 가입자의 가입으로 인해 기존 가입자의 해독정보가 매번 업데이트되어야 하는 문제점을 해결할 수 있다.

<75> 이상 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을

가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

발명의 효과

<76> 상기한 바와 같은 본 발명의 컨텐츠 서비스 제공 방법 및 장치에 따르면 다음과 같은 효과가 하나 혹은 그 이상 있다.

<77> 첫째, 컨텐츠 서비스 가입자가 2개의 해독정보를 이용하여 자신이 가입한 컨텐츠 서비스 사용기간 동안 컨텐츠를 제공받을 수 있게 되어 컨텐츠 서비스 제공을 위한 복잡한 키 분배 문제를 해결할 수 있는 장점이 있다.

<78> 둘째, 최초 1회 해독정보가 가입자에게 전송한 후에는 연속된 컨텐츠 서비스 사용기간 동안 자동으로 해독정보의 값이 변경되어 종래의 키 재전송 및 유지, 관리의 복잡성을 단순화 시킬 수 있는 장점도 있다.

<79> 셋째, 단방향 해쉬 함수를 이용하여 가입자의 컨텐츠 서비스 사용기간에 대응되도록 해독정보를 생성함으로써, 종래 신규 가입자의 가입으로 인해 기존 가입자가 키를 매번 업데이트해야 하는 비효율성을 해결하고, 각 가입자들이 자신의 해독 정보를 이용하여 자신의 컨텐츠 서비스 사용기간 동안 컨텐츠 서비스를 제공받을 수 있는 장점도 있다.

도면의 간단한 설명

<1> 도 1은 종래 방송 서비스 제공의 개념도이다.

<2> 도 2는 종래 방송 서비스 제공에 있어서 키 분배의 개념도이다.

<3> 도 3는 본 발명의 일 실시예에 따른 컨텐츠 서비스 제공 장치의 블록도이다.

<4> 도 4은 본 발명의 일 실시예에 따른 컨텐츠 서비스 제공 방법의 순서도이다.

<5> 도 5는 본 발명의 일 실시예에 따른 방송 서비스 제공의 일 예를 도시한다.

<6> <도면의 주요 부분에 관한 부호의 설명>

<7> 301: 서비스 암호화부 302: 서비스 복호화부

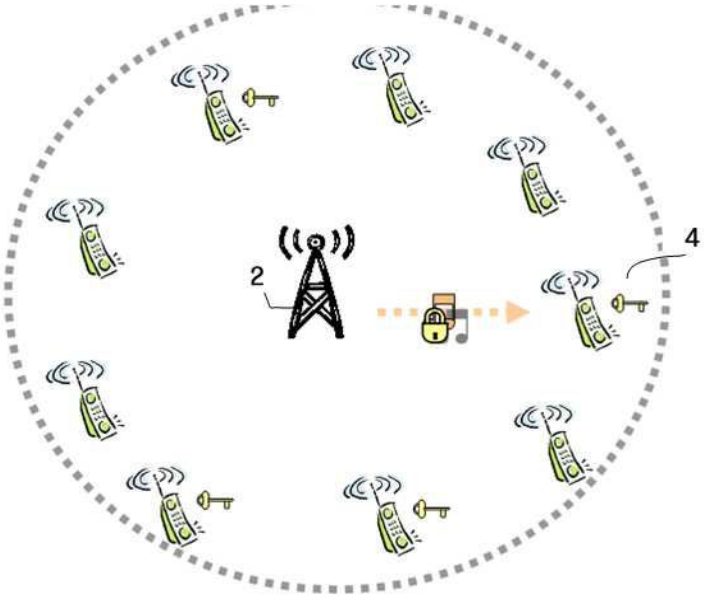
<8> 310: 생성부 320: 암호화부

<9> 330: 제1 송수신부 340: 제2 송수신부

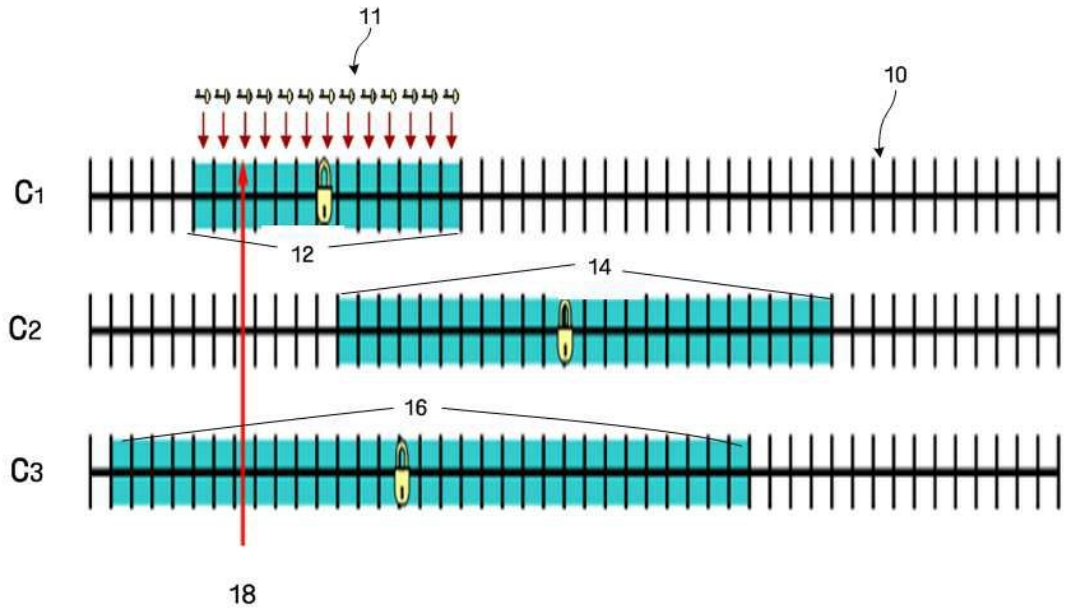
<10> 350: 저장부 360: 복호화부

도면

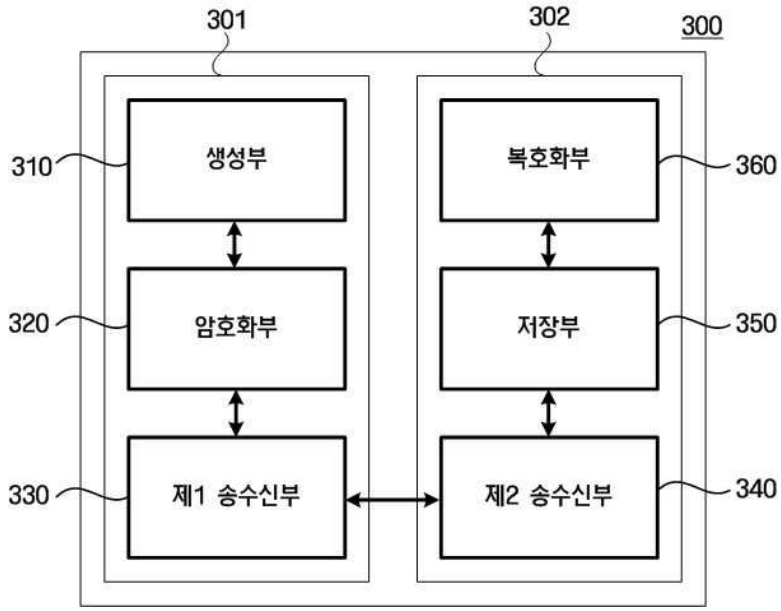
도면1



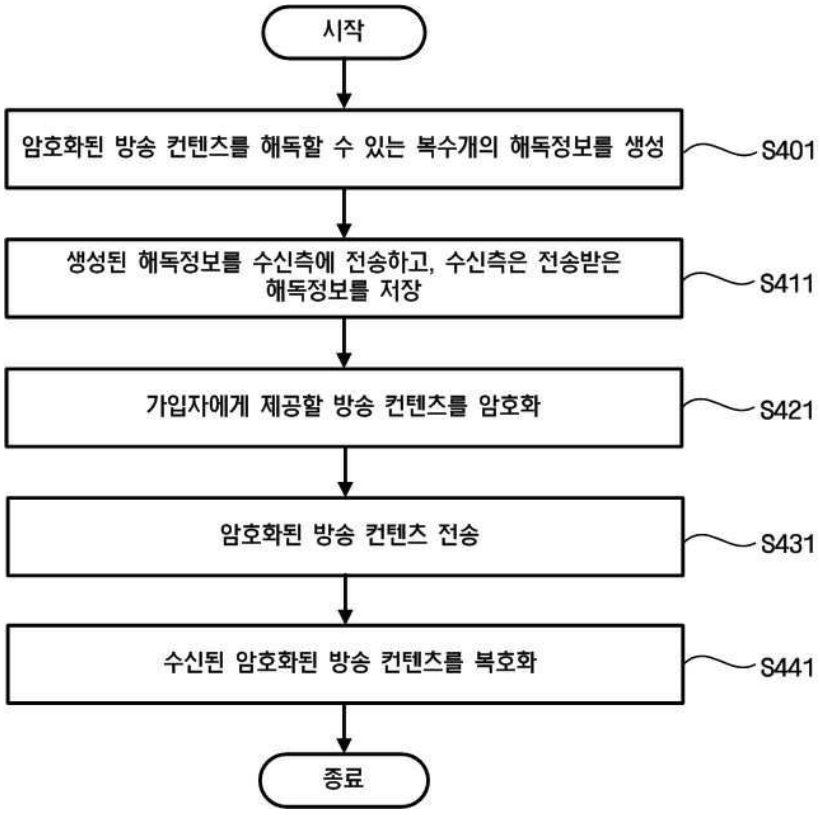
도면2



도면3


301
302
300
310
생성부
복호화부
360
320
암호화부
저장부
350
330
제1 송수신부
제2 송수신부
340

도면4


시작
암호화된 방송 컨텐츠를 해독할 수 있는 복수개의 해독정보를 생성
S401
생성된 해독정보를 수신측에 전송하고, 수신측은 전송받은 해독정보를 저장
S411
가입자에게 제공할 방송 컨텐츠를 암호화
S421
암호화된 방송 컨텐츠 전송
S431
수신된 암호화된 방송 컨텐츠를 복호화
S441
종료

도면5