(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04N 7/173

(45) 공고일자 2005년11월08일
(11) 등록번호 10-0526843
(24) 등록일자 2005년10월31일

(21) 출원번호 10-2002-0067646
(22) 출원일자 2002년11월02일

(65) 공개번호 10-2003-0036108
(43) 공개일자 2003년05월09일

(30) 우선권주장 JP-P-2001-00338363 2001년11월02일 일본(JP)
JP-P-2002-00239775 2002년08월20일 일본(JP)

(73) 특허권자 캐논 가부시끼가이샤
일본 도꾜도 오오따꾸 시모마루꼬 3쪼메 30방 2고

(72) 발명자 타가시라노부히로
일본국도쿄도오오다꾸시모마루꼬3쪼메30방2고캐논가부시키가이샤나이

이와무라케이치
일본국도쿄도오오다꾸시모마루꼬3쪼메30방2고캐논가부시키가이샤나이

(74) 대리인 신중훈
임옥순

심사관 : 권기원

(54) 디지털 컨텐츠 처리장치, 디지털 컨텐츠 처리시스템,디지털 방송시스템, 디지털 컨텐츠 처리방법,컴퓨터판독가능한 저장매체 및 컴퓨터 프로그램

요약

네크워크에 의해 배포된 디지털 컨텐츠의 저작권을 보호하기 위하여, 디지털 컨텐츠의 편집의 허가/금지는 메타정보의 신뢰도에 따라서 디지털 컨텐츠에 관련된 메타정보에 의거하여 제어된다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은, 본 발명에 의한 시스템의 개요를 도시하는 도면.

도 2는, 본 발명에 의한 시스템의 구성을 도시하는 블록도.

도 3은, 본 발명에 의한 시스템의 구성을 도시하는 블록도.

도 4는, 본 발명에 의한 인증기관의 구조를 도시하는 블록도.

도 5는, 본 발명에 의한 시스템의 구성을 도시하는 블록도.

도 6은, 본 발명에 의한 시스템의 구성을 도시하는 블록도.

도 7은, 본 발명에 의한 메타정보의 신뢰도에 대응하는 등급정보의 예를 도시하는 도면.

도 8은, 조건부 접근방송을 실현하기 위한 종래 시스템의 구성의 예를 도시하는 블록도.

도 9는, 본 발명에 의한 시스템의 구성을 도시하는 블록도.

<도면의 주요부분에 대한 부호의 설명>

11,530,640 : 관리자 12,120,610 : 방송 사업자

13,130,510,620 : 메타정보 제공자 14,140,520,630 : 수신자

14a,14b,14c : 키 15,160,650 : 네트워크

16,17 : 통신 위성 121,611 : 스크램블부

122 : 스크램블키 123 : 제 1암호화부

124,618 : 다중화부 125,613 : 워크키

126,614 : 계약정보 127 : 제 2암호화부

128,131 : 제 1키 132,615 : 암호화부

133 : 제 2키 134,621 : 메타정보

135 : 제 3암호화부 145, 636 : 시청판정부

147,523,635 : 검증부 149,637 : 시청제어부

170 : 편집부 171 :편집제어부

511 : 디지털 서명부 512,617 : 제 1키관리부

616 : 제 1암호화/서명부 512 : 디지털 서명 검증부

522,623 : 제 2키관리부 622 : 제 2암호화/서명부

633 : 복호화/검증부 634 : 제 3키관리부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 다양한 컨텐츠에 대한 메타정보의 신뢰도와 유효성을 확인할 수 있는 시스템에 관한 것으로서, 더욱 상세하게는, 메타정보의 신뢰도와 유효성을 검증하고, 검증결과와 메타정보에 의거하여 프로그램 컨텐츠의 어떠한 변경도 제어할 수 있는 시스템에 관한 것이다.

디지털화에 대한 최근 경향에 따라, 디지털화는 다양한 분야에서 진행되고 있다. 방송분야에서도, 디지털화는 진행되고 있고, 디지털방송은 부분적으로 실현되었다. 디지털방송에서, 방송프로그램 뿐만 아니라 상기 프로그램의 컨텐츠를 설명하는 메타정보 등이 전송될 수 있다. 이와 같은 메타정보를 사용하여 대용량 저장기능(이하 "저장"이라 칭함)을 가진 수신기가 방송프로그램을 자동적으로 저장함으로써, 새로운 서비스(예를 들면, 장면검색과 다이제스트 시청)가 제안되었다.

또한, 대용량에 대한 하드디스크의 최근 경향에 따라, 디지털방송 컨텐츠를 기록하기 위한 하드디스크 레코더는 이미 상업화되었다. 상기 설명한 바와 같이, 그러한 서비스의 현실화에 대한 환경은 개선되었다. 또한, 디지털방송에서, 프로그램의 허가받지 않은 복제로부터 방송프로그램을 보호하기 위한 대책이 요망되고 있다.

대용량 저장기능을 가진 수신기는 또한 가정용 서버로서의 기능, 예를 들어, 인터넷이나 다른 정보가전제품에 접속하는 기능을 갖는 것이 예상되므로, "서버형 수신기"로 칭하는 것에 유의하여야 한다. 그러한 서버형 수신기에 대한 방송은 "서버형 방송"으로서 칭한다.

종래에는, 유료의 방송시스템으로서, 텔레비젼 방송과 고정세 텔레비젼 방송(이하 "하이비젼 방송"으로 칭함)에 적용되는 조건부 접속시스템은 널리 연구되었다. 유료의 방송시스템에서 일반적으로 방송되는 비디오 신호와 오디오 신호는, 인가되지 않은 사람이 상기 신호를 수신하는 것을 방지하기 위한 어떤 방법에 의해 스크램블되고, 스크램블된 신호를 디스크램블하기 위한 신호는 인가된 사람에게 전송되어, 수신을 제어한다.

상기 수신을 제어하기 위한 신호로서 전송된 정보는, 스크램블된 신호를 디스크램블하기 위한 키(스크램블키(Ks))에 대한 정보, 방송 프로그램이 수신자의 계약범위 내에 들어가는지의 여부를 결정하기 위한 정보, 방송국이 특정한 수신기를 강제적으로 온/오프하는 정보 등으로 구성된 관련정보를 칭한다.

유료의 텔레비젼 방송이나 유료의 하이비젼 방송은 위성방송에 의해 제공되고, 관련정보는 데이터채널을 통해 패킷의 형태로 전송된다. 이 경우, 스크램블키와 방송 프로그램(프로그램 컨텐츠로 칭함)에 관련된 정보는, 제 3자에게 상기 정보가 알려지거나 변경되는 것을 막기 위해 암호화된다.

스크램블키 또는 프로그램 컨텐츠를 암호화하기 위한 키는 워크키(Kw)로 칭하고, 수신자에 의해 이루어진 계약의 컨텐츠를 나타내는 계약정보와 함께, 각 수신자에게 수신된다. 정보의 이들 부분은 개별 정보로 칭하고, 방송전파, IC카드나 자기카드, 전화선 등의 물리적 매체를 통해 전송된다. 개별정보가 암호화될 때, 마스터키(Km)가 사용된다. 마스터키(Km)는 기본적으로 수신자에 따라 다르다.

도 8은, 스크램블 방식을 위한 구성을 도시한다. 도 8을 참조하면, 방송국측 장치는, 스크램블부(801), 다중화부(802), 스크램블키(Ks)(803), 워크키(Kw)(804), 계약정보(805), 암호화부(806),(807) 및 마스터키(Km)(808)를 포함한다.

수신측 장치는 분리부(809), 디스크램블부(810), 복호화부(811),(812), 시청판정부(813), 계약정보(814) 및 마스터키(Km)(815)를 포함한다.

발명이 이루고자 하는 기술적 과제

서버형 방송에서, 메타정보를 제공하는 자는 방송사업자에 한정되는 것은 아니고, 메타정보는 인터넷 등의 통신매체에 의해 다양한 사업자와 사용자로부터 배포되는 것도 예상된다.

또한, 메타정보는, 프로그램 제목 등의 간단한 메타정보 외에도, 다양한 기능을 가지는 메타정보, 예를 들면, 프로그램의 다이제스트를 생성하는 메타정보 등의 프로그램의 구조를 변경하는 메타정보인 것으로 가정한다.

프로그램의 구조를 변경하는 메타정보는 상기 프로그램을 변경하기 위해 사용되므로, 저작권을 고려하여야만 한다.

그러나, 종래에는, 메타정보를 배포하는 제공자의 신뢰도와 유효성 및 메타정보의 신뢰도와 유효성을 검증하는 메카니즘은 고려되지 않았다.

본 발명의 일 실시예의 제 1목적은 프로그램 컨텐츠에 대응하는 메타정보의 신뢰도와 유효성을 검증하는데 있다.

제 2목적은 메타정보의 신뢰성과 유효성에 따라 프로그램 컨텐츠의 재생과 편집을 제어할 수 있는 시스템을 제공하는데 있다.

본 발명의 기타 특징과 이점은, 동일한 참고문자가 도면부호 전체를 통하여 동일하거나 유사한 부분을 나타내는 첨부도면과 함께 취한, 다음 설명으로부터 자명하게 된다.

첨부도면은, 명세서의 부분을 구체화하여 구성하고, 본 발명의 실시예를 예시하고, 설명과 함께, 본 발명의 원리를 설명하고 있다.

발명의 구성 및 작용

(제 1실시예)

본 발명의 실시예에 따라 디지털 컨텐츠 처리장치, 디지털 컨텐츠 처리시스템, 디지털 방송 시스템, 디지털 컨텐츠 처리방법, 컴퓨터판독가능한 저장매체 및 컴퓨터 프로그램은 첨부도면을 참고하여 다음에 설명한다.

도 1은, 본 발명의 제 1실시예에 따라 시스템의 구성의 일례를 도시한다. 제 1실시예는 단일 또는 복수의 관리자, 단일 또는 복수의 방송 사업자 및 단일 또는 복수의 메타정보 제공자로 구성된다. 그들은 다수의 통신매체에 의해 서로 접속된다.

관리자(11)는 시스템의 전체적인 동작을 관리한다. 예를 들면, 관리자(11)는 시스템에서 사용된 키의 발행을 관리한다.

방송 사업자(12)는 방송에 의해 프로그램 컨텐츠를 제공하는 엔티티(entity)이고, 일반적으로 방송국에 대응한다. 그러나, 명백하게, 상기 실시예는 비디오 방송에 제한되는 것은 아니고, 라디오 방송 등의 음악방송에 적용될 수 있고, 또한 데이터 방송 등의 일반 컨텐츠의 방송에도 적용될 수 있다. 상기 실시예에서, 이러한 방송 컨텐츠는 총칭적으로 프로그램 컨텐츠라고 부른다.

메타정보 제공자(13)는 프로그램 컨텐츠에 대응하는 메타정보를 제공하기 위한 엔티티이다.

서버형 방송에서, 프로그램 컨텐츠는 저장매체에 유지되고, 메타정보도 또한 유지된다. 수신자(14)의 서버형 수신기는 네트워크(15)에 접속하는 기능을 가진다. 상기 서버형 수신기는 통신 위성(16),(17) 등에 의해 프로그램 컨텐츠와 메타정보를 수신한다. 서버형 수신기는 프로그램 컨텐츠와 독립해서 메타정보를 수신한다는 것에 유의하여야 한다.

이 동작에 의해, 방송 사업자(12) 이외의 엔티티는 메타정보를 제공할 수 있다. 수신자(14)는 프로그램 컨텐츠와 재생 프로그램 컨텐츠를 수신하는 엔티티이고, 메타정보에 의거하여 프로그램 컨텐츠를 편집한다.

방송 사업자(12)와 기타 엔티티는 라디오 방송으로 칭하는 통신매체를 사용함으로써 서로 통신하는 경우를 아래 설명한다. 방송 사업자(12)와 기타 엔티티는 광섬유 등의 또 다른 통신매체에 의해 서로 통신할 수 있다는 것에 유의하여야 한다. 또한, 수신자(14)와 메타정보 제공자(13)는 단방향 통신매체(예를 들면, 방송 사업자(12)에 의한 라디오 방송)뿐만 아니라, 전화 네트워크, 무선전화 네트워크 및 케이블 텔레비젼 네트워크 등의 다수의 양방향 통신매체에 의해 서로 통신할 수 있다. 방송 사업자(12)는 메타정보 제공자(13)와 관리자(11)를 수용할 수 있다.

도 2는, 메타정보 제공자(13)와 수신자(14)의 각 구성의 일례를 도시한다. 도 2에 도시한 바와 같이, 메타정보 제공자(13)는 통신매체에 의해 수신자(14)에 접속된다. 메타정보 제공자(13)는 관리자(11)로부터 배포된 제 1키(131)를 유지한다. 메타정보 제공자(13)는 암호화부(132)를 가진다.

암호화부(132)는 메타정보를 제 1키(131)로 암호화하고, 암호화된 메타정보를 출력한다. 상기 암호화 동작을 위해 사용된 암호화 알고리즘은 명세되지 않는다.

수신자(14)는 관리자(11)로부터 배포된 복수의 키 (14a),(14b),(14c)와 키신뢰도 리스트(141)를 유지한다. 복수의 키 (14a) 내지 (14c)는 관리자(11)에 의해 메타정보 제공자(13)에게 배포된 키를 포함한다.

키신뢰도 리스트(141)는 관리자(11)에 의해 결정된 각각의 키 (14a) 내지 (14c)의 신뢰도를 나타내는 데이터이다. 예를 들면, 하나의 키의 신뢰도는 상기 키를 유지하는 메타정보 제공자(13)의 신뢰도에 의거하여 결정된다. 예를 들면, 도 2에 도시한 바와 같이, 메타정보 제공자(13)가 방송 사업자(12)와 다를 경우, 상기 신뢰도는 낮다. 이에 반하여, 메타정보 제공자(13)가 방송 사업자(12)내에 수용되는 경우, 고신뢰도 정보가 결정된다. 또한 수신자(14)는 복호화부(142), 키선택부(143) 및 검증부(144)를 가진다.

복호화부(142)는 키선택부(143)로부터 출력된 키정보를 사용함으로써 암호화된 메타정보를 복호화한다. 사용된 복호화 알고리즘은 메타정보 제공자(13)의 암호화부(132)에 의해 사용된 암호화 알로리즘에 대응한다. 키선택부(143)로부터 출력된 키정보는 메타정보를 암호화하기 위한 암호화부(132)에 의해 사용된 키에 대응한다.

키선택부(143)는 복수의 키 (14a) 내지 (14c)로부터 복호화부(142)에 의해 사용된 키를 선택한다. 예를 들면, 다음 선택 방법, 상기 키 (14a) 내지 (14c) 모두를 연속적으로 선택하는 방법과 복호화부(142)에 입력된 암호화된 메타정보의 헤더부분에 부가된 키식별정보에 의거하여 키를 선택하는 방법, 중의 하나를 사용할 수 있다.

상기 실시예에서, 암호화된 통신은 메타정보 제공자(13)와 수신자(14)가 키를 공유함으로써 실현된다. 또한, 메타정보는 이진데이터가 아닌 어떤 형식을 가지고 있기 때문에, 메타정보의 유효성은 복호화부(142)에 의해 복호화된 정보가 특정 형식에 맞는지의 여부를 검사함으로써 검증될 수 있다.

검증부(144)는 복호화부(142)에 의해 얻은 복호화 결과에 의거한 신뢰도정보와, 복호화를 위해 사용된 키 및 키신뢰도 리스트(141)를 출력한다. 키선택부(143)는 상기 키(14a)를 선택하고 복호화부(142)는 상키 키(14a)를 사용함으로써 암호화된 메타정보를 복호화할 수 있다. 이 경우, 검증부(144)는 키신뢰도 리스트(141)로부터 상기 키(14a)의 신뢰도를 참조함으로써 신뢰도 정보를 출력한다.

메타정보의 유효성을 상기 방식에서 확인할 수 있는 경우, 복호화를 위해 사용된 키에 대응하는 신뢰도는 키신뢰도 리스트(141)를 참조함으로써 검사할 수 있다. 이것은 키를 유지하는 메타정보 제공자(13)의 신뢰도와 메타정보의 신뢰도를 결정할 수 있게 한다.

메타정보의 유효성이 검사될 수 없는 경우, 메타정보의 신뢰도는 최하급으로 결정될 수 있다. 예를 들면, 키신뢰도 리스트(141)가 키를 유지하는 메타정보 제공자(13)의 신뢰도를 나타내는 경우, 메타정보의 신뢰도 정보는 메타정보를 생성하는 메타정보 제공자(13)의 신뢰도와 일치한다.

도 3은, 상기 실시예가 조건부 접근방송에 적용되는 구성을 도시한다. 도 3에 도시된 구성은, 방송 사업자(120), 메타정보 제공자(130) 및 수신자(140)로 구성된다. 상기 방송 사업자(120)는 상기 수신자(140)를 위해 조건부 접근방송을 제공한다.

조건부 접근방송에 의해 제공된 프로그램 컨텐츠는 인가되지 않은 수신자(140)가 프로그램 컨텐츠를 재생하는 것을 방지하기 위하여 동일한 방법에 의해 스크램블된다. 인가된 수신자(140)는 스크램블된 프로그램을 디스크램블한 신호를 전송함으로써 스크램블된 프로그램 컨텐츠를 재생할 수 있다.

도 3을 참고하면, 방송 사업자(120)는 관리자(11)에 의해 배포된 제 1키(128)을 유지하고, 스크램블부(121), 다중화부(124), 제 1암호화부(123) 및 제 2암호화부(127)로 구성된다.

스크램블부(121)는 스크램블키(Ks)(122)를 사용함으로써 프로그램 컨텐츠를 스크램블한다. 제 1암호화부(123)는 워크키(Kw)(125)를 사용함으로써 스크램블키(Ks)(122)를 암호화한다.

제 2암호화부(127)는 제 1키(128)를 사용함으로써 워크키(Kw)(125)와 계약정보(126)를 암호화한다. 다중화부(124)는 스크램블부(121)로부터 출력된 암호화된 프로그램 컨텐츠, 제 1암호화부(123)로부터 출력된 암호화된 스크램블키(Ks)(122) 및 제 2암호화부(127)로부터 출력된 암호화된 정보를 다중화한다. 그러나, 제 2암호화부(127)로부터 출력된 암호화된 워크키(Kw)(125)와 암호화된 계약정보(126)를 다중화할 필요가 없다는 것에 유의하여야 한다.

제 1암호화부(123)와 2암호화부(127)로부터 출력된 정보를 다중화하는 것은 워크키(Kw)(125), 계약정보(126) 및 프로그램 컨텐츠의 허가/금지에 대한 제어를 허가하는 동안 데이터량에 재생의 허가/금지에 관한 제어가 필요한 것 등을 감소시킬 수 있다.

도 3을 참조하면, 메타정보 제공자(130)는 관리자(11)로부터 배포된 제 2키(133)를 유지하고, 제 3암호화부(135)를 가진다. 제 3암호화부(135)는 메타정보 제공자(130)에 의해 생성된 메타정보(134)를 제 2키(133)로 암호화하고, 네트워크(160)에 암호화된 메타정보를 출력한다.

도 3을 참조하면, 수신자(140)는 관리자(11)로부터 배포된 복수의 키(150n)와 키신뢰도 리스트(148)를 유지하고, 분리부(141), 디스크램블부(143), 제 1복호화부(142), 제 2복호화부(144), 키선택부(146), 검증부(147), 시청판정부(145) 및 시청제어부(149)로 구성된다.

분리부(141)는 방송 사업자(120)로부터 수신된 다중화 정보를 분리한다. 분리된 암호화된 프로그램 컨텐츠, 암호화된 스크램블키(Ks) 및 암호화된 정보는 각각, 디스크램블부(143), 제 1복호화부(141) 및 제 2복호화부(144)에 출력된다.

키선택부(146)는 복수의 키(150n)로부터 복호화를 위해 사용된 키를 선택한다. 제 2복호화부(144)는 상기 키선택부(146)로부터 출력된 키를 사용함으로써 워크키(Kw)(125)와 계약정보(126)을 복호화한다. 제 2복호화부(144)는 키선택부(146)로부터 출력된 상기 키를 사용함으로써, 네트워크(160)에 의해 제 3암호화부(135)로부터 출력된 암호화된 메타정보를 복호화한다. 제 1복호화부(142)는 제 2복호화부(144)로부터 입력된 워크키(Kw)(125)를 사용함으로써 암호화된 스크램블키(Ks)를 복호화한다.

시청판정부(145)는 제 2복호화부(144)로부터 입력된 계약정보(126)에 따라 제 1복호화부(142)로부터 스크램블키(Ks)를 얻고, 디스크램블부(143)에 상기 키를 입력한다.

디스크램블부(143)는 시청판정부(145)로부터 입력된 스크램블키(Ks)를 사용함으로써 분리부(141)로부터 입력된 암호화된 프로그램 컨텐츠를 디스크램블한다. 상기 키선택부(146)가 복수의 키 중에 특정한 키를 선택하는 것이 금지되는 경우, 대응 워크키(Kw)에 의해 암호화된 스크램블키(Ks)에 의해 암호화된 프로그램 컨텐츠는 복원될 수 없다. 키선택부(146)가 복수의 키 중에 특정한 키만을 선택하도록 설계되는 경우, 대응 워크키(Kw)에 의해 암호화된 스크램블키(Ks)에 의해 암호화된 프로그램 컨텐츠만이 복원될 수 있다. 즉, 키선택부(146)에 의해 선택된 키를 제어함으로써, 수신자(140)는 특정한 기간동안에만 프로그램 컨텐츠를 재생하는 것이 허가된다.

검증부(147)는, 복호화를 위해 사용된 상기 키(150n)와 키신뢰도 리스트(148)에 의거하여 메타정보의 신뢰도 정보를 출력한다.

시청제어부(149)는 메타정보와 상기 메타정보의 신뢰도 정보를 입력하고, 메타정보에 의거한 프로그램 컨텐츠의 편집의 허가/금지를 제어한다. 상기 시청제어부(149)는, 메타정보가 저신뢰도를 가지는 경우, 프로그램 컨텐츠의 편집이 금지되는 반면에, 메타정보가 고신뢰도를 가지는 경우, 프로그램 컨텐츠의 편집이 허가되도록 제어한다.

도 9는, 메타정보에 의거한 프로그램 컨텐츠의 편집이 메타정보의 신뢰도에 따라 제어되는 경우에 수신자(140)의 구성을 도시한다.

도 9에서 수신자(140)는 도 3에 도시한 구성에 부과하여 편집제어부(171)와 편집부(170)를 포함한다.

상기 편집제어부(171)는 메타정보와 신뢰도 정보에 따라 편집부(170)에 의해 프로그램 컨텐츠의 편집의 허가/금지를 제어한다.

상기 편집제어부(171)는 메타정보와 신뢰도 정보에 따라 상기 편집부(170)에 의해 프로그램 컨텐츠의 편집의 정도를 제어할 수 있다. 예를 들면, 메타정보의 신뢰도가 높은 경우, 편집부(170)는 고수준으로 프로그램 컨텐츠를 편집하도록 허가한다. 메타정보의 신뢰도가 낮은 경우, 편집부(170)는 저수준으로만 프로그램 컨텐츠를 편집하도록 허가한다. 고수준으로의 편집은, 프로그램 컨텐츠의 구조(예를 들면, 복수의 프로그램 컨텐츠로부터 그 장면을 절단함으로서 특정한 배우의 클립의 수집을 창작하기 위한 편집을 포함하는 각색)를 변경하는 편집이다. 저수준으로의 편집은, 프로그램 컨텐츠의 다이제

스트를 창작하기 위한 편집과 프로그램 컨텐츠의 헤드에 제목을 부가하는 것을 포함하는, 프로그램 컨텐츠의 구조를 유지하는 편집이다. 편집 명세서는 다양하게 생각할 수 있고, 본 발명은 특정한 편집에 제한되지 않는다는 것에 유의하여야 한다.

또한, 메타정보의 부분이 하나의 프로그램 컨텐츠를 위해 준비되는 경우, 메타정보의 부분이 프로그램 컨텐츠에 영향을 주도록 사용되는 우선순위는, 신뢰도를 사용함으로써 결정될 수 있다.

(제 2실시예)

본 발명의 제 2실시예는 아래 설명한다. 암호화와 복호화를 위해 다른 키를 사용하는 공개키 암호방식을 사용하는 시스템은, 인증기관(CA)을 사용하는 공개키 기반구조(PKI), 인증서 및 인증서 폐기목록(CRL)이 자주 사용된다.

인증기관(CA)에 의해 생성된 사용자의 공개키의 유효성은, 공개키를 위한 인증서와 공개키 양쪽 모두 사용함으로써 보증된다. 또한, 인증서를 검증하는 절차에서, 인증서가 폐기되는지의 여부는 인증서 폐기목록(CRL)을 참조함으로써 검사될 수 있다.

구조를 설명하기 위한 도면인 도 4에 의해 나타내는 바와 같이, 인증기관(CA)은 저수준의 인증기관(CA1)은 고수준의 인증기관(CA)에 의해 인증될 수 있도록 계층적으로 구성될 수 있다. 이것을 관리자의 서명 연쇄(signature chaining)로 칭한다.

일반적인 인증서 발행 서비스에서, 인증서의 클래스는 인증서 발행시에 식별을 엄격하게 함에 따라 정의된다. 그러나, 상기 실시예에서, 인증서의 클래스에 대해서는, 복수의 상기 인증서의 클래스는 인증서 발행시에 식별을 엄격하게 하는 대신에 메타정보의 신뢰도에 따라 정의된다.

예를 들면, 도 7에 도시한 바와 같이, 인증서의 각각의 클래스는 다수의 시청제어동작(예를 들면, "프로그램 컨텐츠의 시청제어가 완전히 허가된 클래스", "프로그램 컨텐츠의 시청이 제한된 클래스" 및 "프로그램 컨텐츠 다이제스트의 시청이 허가된 클래스")을 고려하여 정의된다. 인증서 폐기목록(CRL)은 허가받지 않은 메타정보를 배포하거나 허가받지 않은 메타정보의 클래스를 배제한 정보 제공자를 배제하기 위해 사용된다.

제 2실시예에 따른 시스템 구성의 일례는, 관리자가 인증기관(CA)의 기능을 갖는 것을 제외하고 제 1실시예의 그것과 동일하다. 도 5는 제 2실시예의 기본 구성의 일례를 도시한다. 도 5에 도시한 바와 같이, 제 2실시예의 기본 구성은 메타정보 제공자(510)와 수신자(520)에 의해 구성된다.

메타정보 제공자(510)는 공개키 암호계에서 공개키와 개인키를 생성하고, 관리자(530)로부터 공개키에 대한 인증서를 얻고, 그것을 유지한다. 메타정보 제공자(510)는 제 1키관리부(512)와 디지털 서명부(511)에 의해 구성된다.

제 1키관리부(512)는 개인키와 인증서를 유지하고 관리한다. 또한, 필요에 따라, 제 1키관리부(512)는 개인키를 디지털 서명부(511)에 출력한다. 디지털 서명부(511)는 제 1키관리부(512)로부터 입력된 개인키를 사용함으로써 메타정보에 대한 디지털 서명을 생성한다.

수신자(520)는, 관리자(530)로부터 메타정보 제공자(510) 등을 위해 인증서를 얻고 유지한다. 또한, 수신자(520)는 관리자(530)로부터 얻은 인증서 폐기목록(CRL)을 관리한다. 또한, 수신자(520)는 디지털 서명 검증부(521), 제 2키관리부(522) 및 검증부(523)로 구성된다.

제 2키관리부(522)는 메타정보 제공자(510) 등을 위해 인증서를 얻어 관리한다. 관리방법은, 미리 관리자(530)로부터 얻은 인증서를 등록함으로써 인증서를 관리하는 방법과, 필요에 따라 관리자(530)로부터 인증서를 얻음으로써 인증서를 관리하는 방법을 포함한다. 또한, 제 2키관리부(522)는 관리자(530)로부터 얻은 인증서 폐기목록(CRL)을 관리한다. 또한, 필요에 따라, 제 2키관리부(522)는 인증서를 출력한다.

디지털 서명검증부(521)는 제 2키관리부(522)로부터 입력된 인증서를 사용함으로써 메타정보에 대한 디지털 서명을 검증한다. 검증부(523)는 디지털 서명검증부(521)에 의해 얻은 검증결과와 검증을 위해 사용된 인증서로부터 신뢰도 정보를 얻는다. 상기 신뢰도 정보는 디지털 서명의 유효성이 검증될 수 있을 때, 인증서의 클래스와 인증서에 관한 관리자(530)의 서명연쇄에 의해 결정된다.

메타정보에 대한 서명은 방송사업자에 의해 이루어지고, 인증서의 클래스가 최상급이라고 가정한다. 이 경우, 신뢰도 정보가 최상급으로 분류되는지의 여부를 결정한다. 메타정보에 대한 서명이 제 3자인 메타정보 제공자(510)에 의해 이루어지고, 인증서의 클래스가 최하급이라고 가정한다. 이 경우, 신뢰도 정보는 최하급으로 분류된다.

제 2실시예에 의하면, 메타정보는 공개키 기반구조(PKI)에 의거하여 검증되고, 신뢰도 정보는 메타정보에 대한 디지털 서명에 대한 검증결과와 검증을 위해 사용된 인증서로부터 얻어진다. 제 1실시예와 달리, 제 2실시예에서는, 검증이 공개키 기반구조(PKI)에 의거하기 때문에, 메타정보는 복수의 개인키의 유지함이 없이 검증될 수 있다. 또한, 인증서 간에 계층 또는 우위/하위의 관계는 인증서 레벨이나 인증서에 관한 관리자(530)의 서명연쇄에 의해 용이하게 결정될 수 있다.

도 6은 도 5에 도시한 기본 구성이 기존의 조건부 접근방송에 적용되는 일례를 도시한다. 도 6을 참조하면, 방송 사업자(610)는 스크램블부(611), 다중화부(618), 암호화부(615), 제 1암호화/서명부(616) 및 제 1키관리부(617)로 구성된다. 방송 사업자(610), 다중화부(618) 및 암호화부(615)는 제 1실시예의 것과 동일한 구성을 가진다.

제 1암호화/서명부(616)는 워크키(613)와 계약정보(614)를 수신하고, 제 1키관리부(617)로부터 입력된 키를 사용함으로써 그것을 암호화하고, 디지털 서명을 생성한다.

제 1키관리부(617)는 개인키와 방송 사업자(610)의 인증서를 관리하고, 필요에 따라서, 관리자(640)로부터 얻은 인증서 폐기목록(CRL)을 또한 관리한다. 또한, 제 1키관리부(617)는 필요에 따라, 비밀키를 생성하거나, 디지털 서명처리를 위해 사용된 개인키를 출력한다.

도 6을 참조하면, 기본 구성처럼, 메타정보 제공자(620)는 공개키와 공개키 암호방식으로 개인키를 생산하고, 관리자(640)로부터 공개키에 대한 인증서를 얻고, 그것을 유지한다. 메타정보 제공자(620)는 제 2암호화/서명부(622)와 제 2키관리부(623)로 구성되고, 메타정보(621)에 대한 디지털 서명을 생성한다.

제 2키관리부(623)는 개인키와 인증서를 유지하여 관리하고, 필요에 따라, 개인키를 제 2암호화/서명부(622)에 출력한다. 제 2암호화/서명부(622)는 제 2키관리부(623)로부터 입력된 개인키를 사용함으로써 메타정보(621)에 관한 디지털 서명을 생성한다.

도 6을 참조하여, 수신자(630)는 분리부(631), 디스크램블부(638), 복호화부(632), 시청관정부(636), 시청제어부(637), 복호화/검증부(633), 검증부(635) 및 제 3키관리부(634)로 구성된다. 상기 분리부(631), 디스크램블부(638), 복호화부(632) 및 시청관정부(636)는 제 1실시예의 것과 동일한 구성을 가진다.

복호화/검증부(633)는 분리부(631) 또는 네트워크(650)로부터 입력된 암호화된 정보를 수신하고, 제 3키관리부(634)로부터 입력된 키를 사용함으로써 정보를 복호화하고, 디지털 서명을 검증한다.

제 3키관리부(634)는 방송 사업자(610)의 인증서를 유지하고 관리한다. 또한, 제 3키관리부(634)는 관리자(640)로부터 새로운 인증서와 인증서 폐기목록(CRL)을 얻고, 그것을 관리한다. 또한, 제 3키관리부(634)는, 필요에 따라, 디지털서명을 검증하는데 필요한 공개키를 출력한다. 이들 인증서 관리동작은 다수의 키관리동작을 실현하고, 제 1실시예와 같이 서버형 방송에 대한 특정한 조건부 접근방송 방식을 차례로 수행한다.

검증부(635)는 복호화/검증부(633), 상기 복호화/검증부(633)에 의해 사용된 인증서의 클래스 및 상기 인증서에 관한 관리자의 디지털 서명연쇄로부터 얻은 메타정보 검증결과를 검사하고, 이에 의해 신뢰도 정보를 얻는다.

상기 설명한 바와 같이, 제 2실시예에 따라, 메타정보는 검증되고, 신뢰도 정보는 메타정보에 대한 디지털 서명에 관한 검증결과와 상기 검증을 위해 사용된 인증서로부터 얻어진다.

(기타 실시예)

상기 설명한 실시예에 따라 디지털 컨텐츠 처리장치는 컴퓨터의 CPU 또는 MPU, RAM, ROM 등으로 구성되고, RAM이나 ROM에 기억된 프로그램이 동작할 때 수행될 수 있다.

이에 의해, 상기 장치는 상기 기능을 실현하기 위한 컴퓨터에 의해 동작하는 프로그램을 CD-ROM 등의 기록매체에 기록하고, 상기 프로그램을 컴퓨터에 적재함으로써 실현될 수 있다. 상기 프로그램을 기록하기 위한 기록매체로서, CD-ROM 외에 플렉시블 디스크, 하드 디스크, 자기 테이프, 광자기 디스크, 비휘발성 메모리카드 등이 사용될 수 있다.

컴퓨터가 공급된 프로그램을 실행할 때 상기 실시예의 기능이 실현되는 경우와, 컴퓨터에서 운영되는 OS(Operating System), 또 다른 어플리케이션 소프트웨어 등과 공동으로 프로그램에 의해 상기 실시예의 기능이 실현되는 경우, 및 공급된 프로그램의 처리의 전체 또는 일부가 컴퓨터에 삽입된 기능확장보드나 기능확장유닛에 의해 수행될 때 상기 실시예의 기능이 실현되는 경우에, 상기 프로그램은 본 발명의 실시예에 포함된다.

또한, 네트워크 환경에서 본 발명을 사용하기 위해서, 프로그램의 전체나 일부는 다른 컴퓨터에 의해 실행될 수 있다. 예를 들면, 원격의 단말 컴퓨터는 스크린 입력처리를 행하도록 사용하는 반면에, 다른 중앙컴퓨터 등이, 예를 들면, 다양한 결정과 로그 기록을 행하도록 사용될 수 있다.

발명의 효과

상기 실시예에 의하면, 프로그램 컨텐츠에 대응하는 메타정보의 신뢰도와 유효성을 검증하고, 상기 메타정보의 신뢰성과 유효성에 따라 프로그램 컨텐츠의 재생과 편집을 제어할 수 있는 시스템을 제공할 수 있다.

(57) 청구의 범위

청구항 1.

디지털 컨텐츠와, 상기 디지털 컨텐츠에 관련하는 메타정보를 취급하는 디지털 컨텐츠 처리장치에 있어서,

상기 디지털컨텐츠와, 암호화된 상기 메타정보를 수신하는 수신수단과;

상기 수신된 메타 정보를, 키를 이용하여 복호화하는 복호화수단과;

상기 복호화수단에서 사용된 키의 속성 정보에 의거하여 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정수단과;

상기 결정수단에 의해 결정된 레벨에 따라서 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어수단을 구비하고,

상기 수신수단으로 수신하는 상기 디지털컨텐츠와 상기 메타정보는, 다른 송신원으로부터 수신하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 2.

제 1항에 있어서,

상기 디지털 컨텐츠 처리장치는,

복수의 키를 기억하는 기억수단과;

상기 기억수단에 기억된 복수의 키로부터 1개의 키를 선택하는 선택수단;

을 부가하여 포함하고,

상기 복호화수단은 상기 선택수단에 의해 선택된 키를 사용하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 3.

제 1항에 있어서,

상기 결정수단은 상기 복호화수단에 의해서 복호화된 메타 정보가 소정의 형식을 갖는지의 여부에 따라서, 상기 재생 또는 편집의 레벨을 결정하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 4.

제 1항에 있어서,

상기 수신수단은 상기 디지털 컨텐츠에 관한 계약정보를 수신하고,

상기 제어수단은, 상기 수신된 계약 정보에 의거하여 상기 디지털 컨텐츠의 재생 여부를 판정하는 판정수단을 가지고, 상기 판정수단에 의한 판정에 따라서 상기 디지털 컨텐츠의 재생을 제어하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 5.

제 1항에 있어서,

상기 디지털 컨텐츠는, 제 1키에 의해 암호화되어 있으며,

상기 제 1키는 제 2키로 암호화되어 있고,

상기 수신수단은, 제 1키로 암호화된 상기 디지털 컨텐츠와 제 2키로 암호화된 상기 제 1키를 수신하고,

상기 복호화 수단은, 상기 제 2키를 이용하여 상기 제 1키를 복호화하고, 복호화된 제 1키를 이용하여 상기 디지털 컨텐츠를 복호화하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 6.

디지털 컨텐츠와, 상기 디지털 컨텐츠에 관련하는 메타정보를 취급하는 디지털 컨텐츠 처리장치에 있어서,

상기 디지털컨텐츠와, 상기 메타정보를 수신하는 수신수단과,

상기 수신된 메타 정보의 서명의 검증에 이용되는 키의 증명서에 의거하여, 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정수단과;

상기 결정수단에 의해 결정된 레벨에 따라서 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어수단을 구비하며,

상기 수신수단으로 수신하는 상기 디지털컨텐츠와 상기 메타정보는, 다른 송신원으로부터 수신하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 7.

디지털 컨텐츠에 관련하는 메타정보를 취급하는 제 1정보처리장치와 제 2정보처리장치를 포함하는 디지털 컨텐츠 처리 시스템에 있어서,

상기 제 1정보처리장치는,

상기 메타정보를 암호화하는 암호화수단과;

상기 암호화수단에 의해 암호화된 메타정보를 상기 제 2 정보처리 장치에 송신하는 송신수단을 구비하고,

상기 제 2정보처리장치는,

상기 제 1정보처리장치에 의해 암호화된 메타정보와, 상기 제 1정보처리장치와는 다른 제 3정보처리장치로부터 상기 디지털컨텐츠를 수신하는 수신수단과;

상기 수신된 메타정보를 키를 이용하여 복호화하는 복호화수단과;

상기 복호화수단에서 이용된 키의 속성정보에 의거하여, 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정수단과;

상기 결정수단에 의해 결정된 레벨에 따라서, 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어수단을 구비하는 것을 특징으로 하는 디지털 컨텐츠 처리시스템.

청구항 8.

삭제

청구항 9.

디지털 컨텐츠와, 상기 디지털 컨텐츠에 관련하는 메타정보를 취급하는 디지털 컨텐츠 처리방법에 있어서,

상기 디지털컨텐츠와, 암호화된 상기 메타정보를 수신하는 수신단계와,

상기 수신된 메타 정보를, 키를 이용하여 복호화하는 복호화단계와;

상기 복호화단계에서 사용된 키의 속성 정보에 의거하여 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정단계와;

상기 결정단계에 의해 결정된 레벨에 따라서 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어단계를 구비하고,

상기 수신단계로부터 수신하는 상기 디지털컨텐츠와 상기 메타정보는, 다른 송신원으로부터 수신하는 것을 특징으로 하는 디지털 컨텐츠 처리방법.

청구항 10.

디지털 컨텐츠와, 상기 디지털 컨텐츠에 관련하는 메타정보를 취급하는 디지털 컨텐츠 처리방법을 컴퓨터에 실행시키기 위한 프로그램을 기록한 컴퓨터 판독가능한 기억매체로서,

상기 디지털 컨텐츠 처리방법은,

상기 디지털컨텐츠와, 암호화된 상기 메타정보를 수신하는 수신단계와;

상기 수신된 메타 정보를, 키를 이용하여 복호화하는 복호화단계와;

상기 복호화단계에서 사용된 키의 속성 정보에 의거하여 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정단계와;

상기 결정단계에 의해 결정된 레벨에 따라서 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어단계를 구비하고,

상기 수신단계로 수신하는 상기 디지털컨텐츠와 상기 메타정보는, 다른 송신원으로부터 수신하는 것을 특징으로 하는 컴퓨터 판독가능한 기억매체.

청구항 11.

삭제

청구항 12.

제 6항에 있어서,

상기 수신수단에 의해 수신된 메타정보는 상기 메타정보의 디지털 서명을 가지고 있으며, 상기 결정수단은 상기 디지털 서명의 검증을 실시하는 검증수단을 가지고 있으며, 상기 검증결과와 상기 증명서에 의거하여 상기 재생 또는 편집의 레벨을 결정하는 것을 특징으로 하는 디지털 컨텐츠 처리장치.

청구항 13.

디지털 컨텐츠와, 상기 디지털 컨텐츠에 관련하는 메타정보를 취급하는 디지털 컨텐츠 처리방법에 있어서,

상기 디지털컨텐츠와, 상기 메타정보를 수신하는 수신단계와;

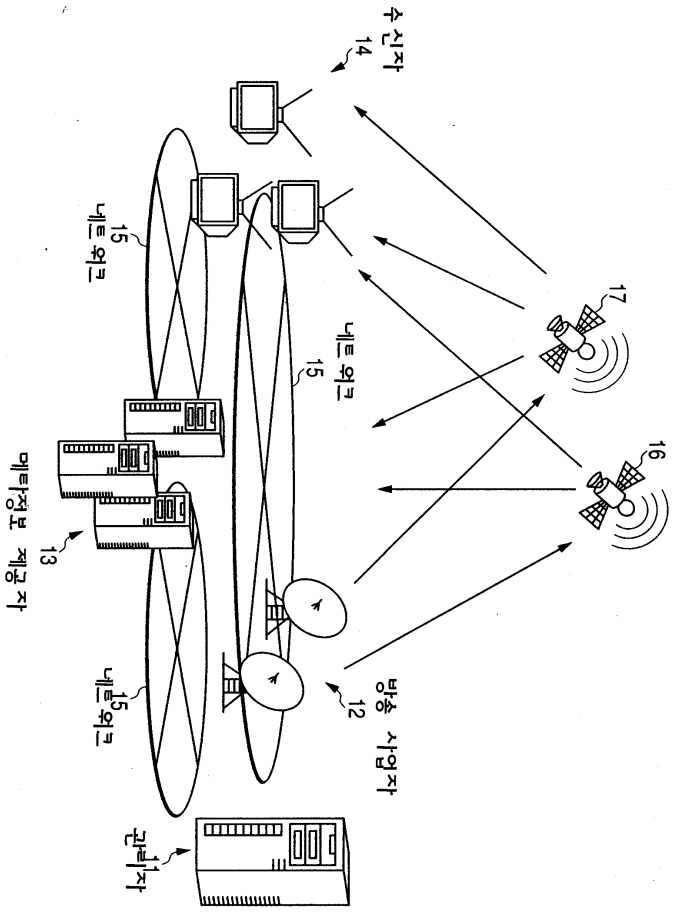
상기 수신된 메타 정보의 서명의 검증에 이용되는 키의 증명서에 의거하여, 상기 디지털 컨텐츠의 재생 또는 편집의 레벨을 결정하는 결정단계와;

상기 결정단계에 의해 결정된 레벨에 따라서 상기 디지털 컨텐츠의 재생 또는 편집을 제어하는 제어단계를 구비하며,

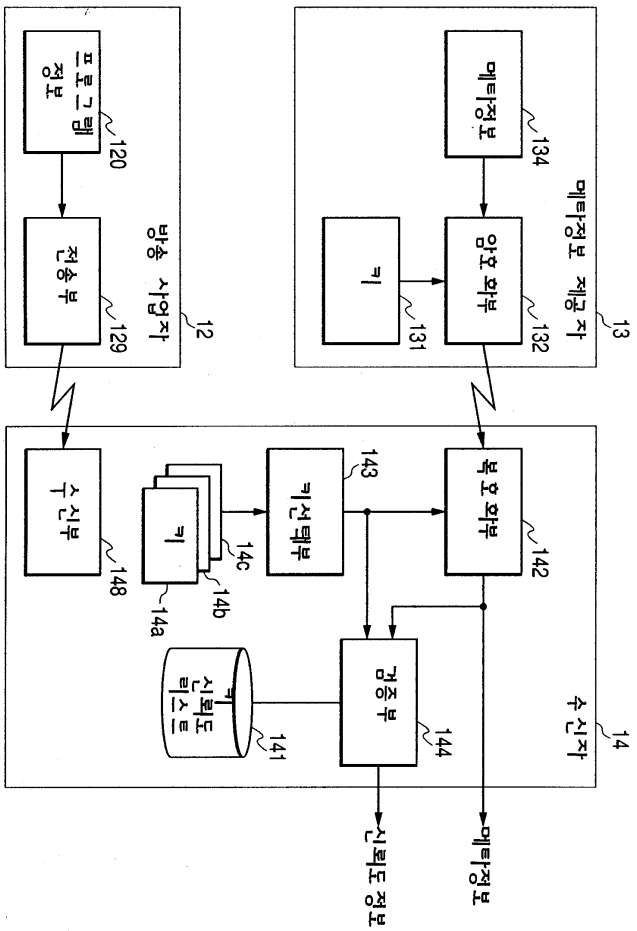
상기 수신단계로부터 수신하는 상기 디지털컨텐츠와, 상기 메타정보는 다른 송신원으로부터 수신하는 것을 특징으로 하는 디지털 컨텐츠 처리방법.

도면

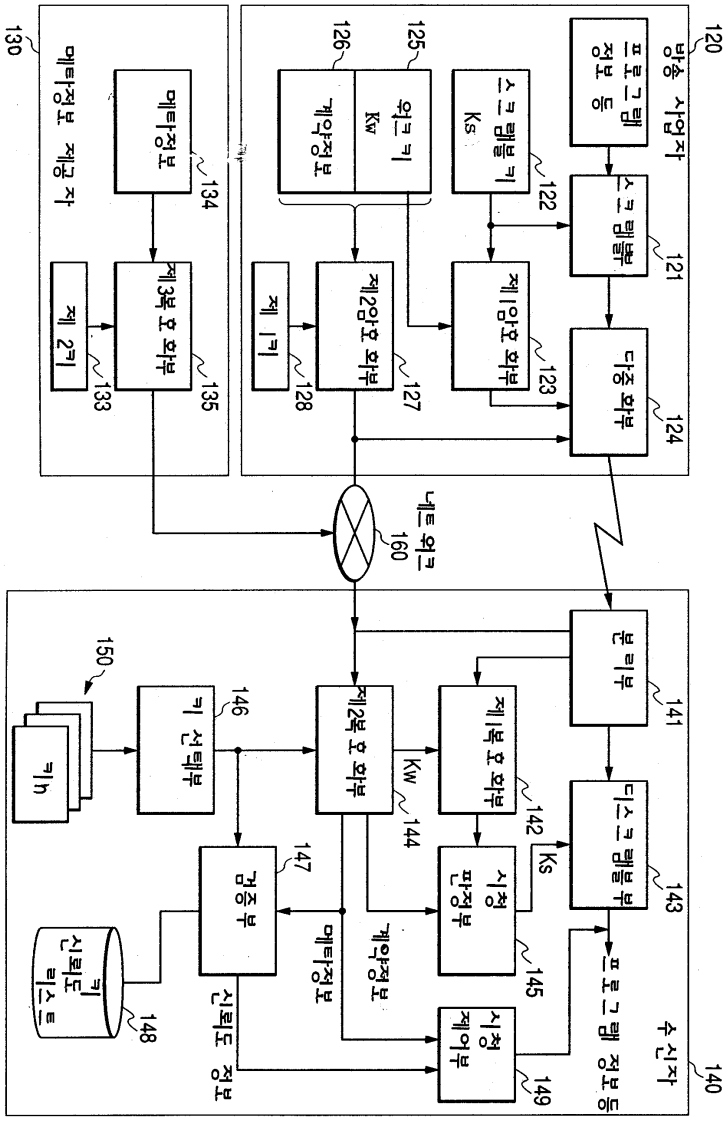
도면1



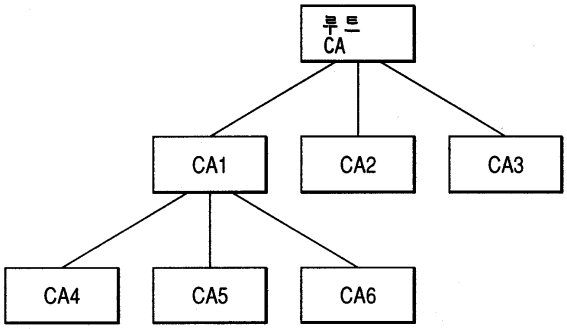
도면2


방송 사업자
12
프로그램 정보
120
전송부
129
메타정보 제공자
13
메타정보
134
암호화부
132
키
131
수신자
14
복호화부
142
키선택부
143
키
14a
14b
14c
수신부
148
신뢰도 리스트
141
검증부
144
신뢰도 정보
메타정보

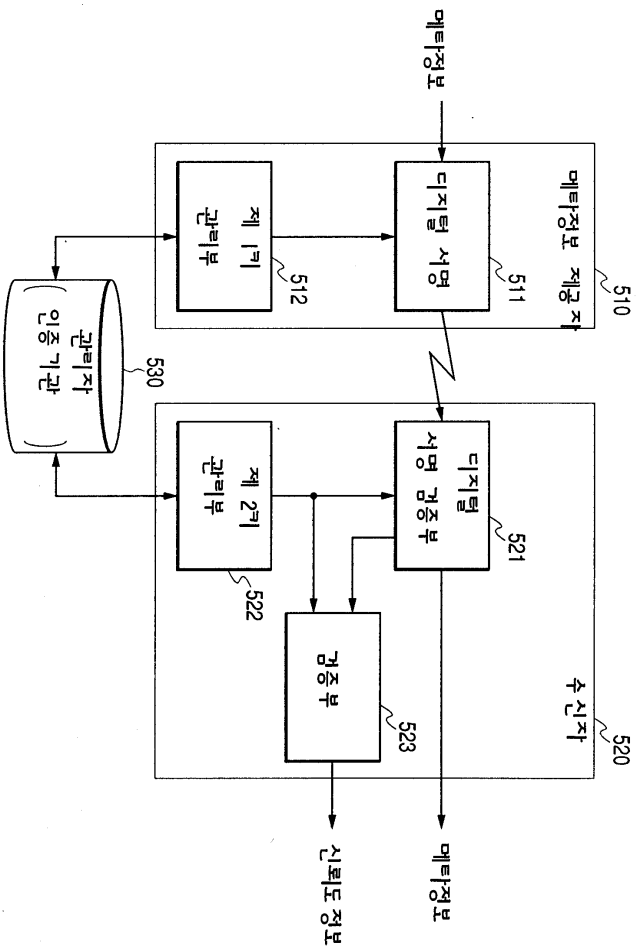
도면3


120
방송 사업자
프로그램 정보 등
스크램블 키
Ks
122
스크램블부
121
디중 화부
124
워크 키
Kw
125
계약정보
126
제1암호 화부
123
제2암호 화부
127
제 1키
128
제 2키
133
제3복호 화부
135
메타정보
134
메타정보 제공 자
130
네트 워크
160
분리부
141
제1복호 화부
142
제2복호 화부
144
키 선택부
146
키h
150
디스크램블부
143
Ks
시청 판정부
145
검증 부
147
메타정보
계약정보
신뢰도 정보
시청 제어부
149
키 신뢰도 리스트
148
프로그램 정보 등
수신자
140

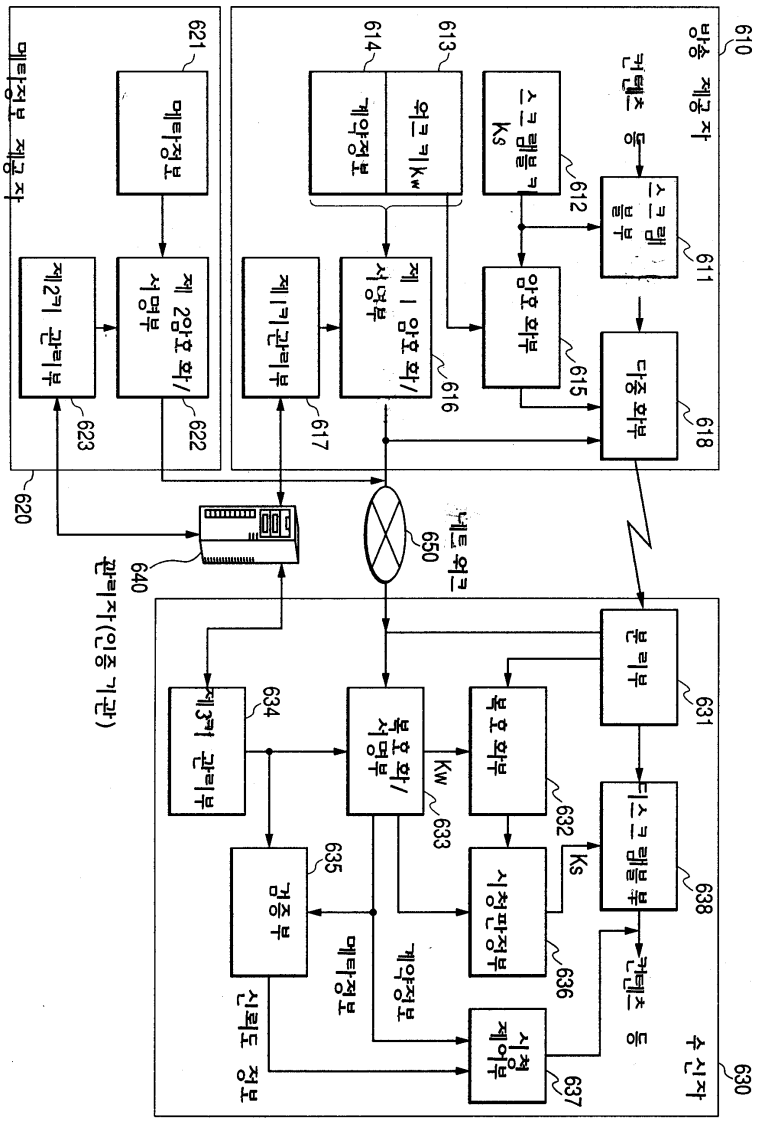
도면4


미디어 CA
CA1
CA2
CA3
CA4
CA5
CA6

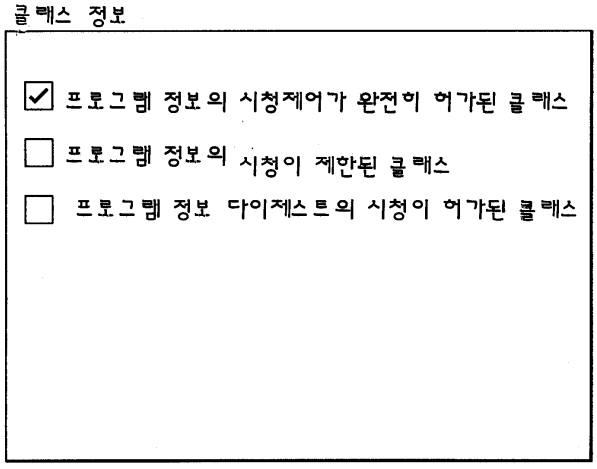
도면5


메타정보
메타정보 제공자
510
디지털 서명
511
제 1키 관리부
512
관리자 (인증 기관)
530
수신자
520
디지털 서명 검증부
521
제 2키 관리부
522
검증부
523
신뢰도 정보
메타정보

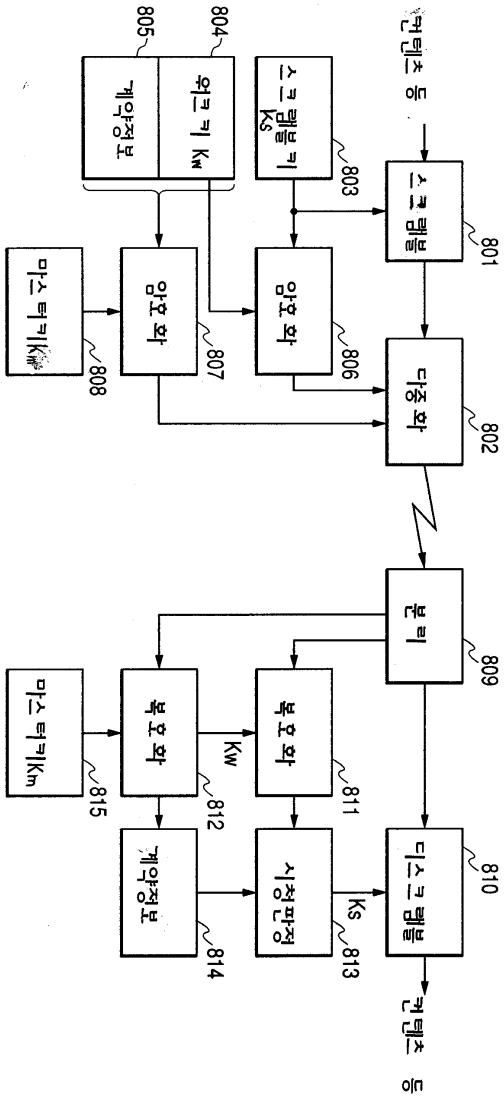
도면6


610
방송 제공 자
612
611
613
614
615
616
617
618
621
622
623
620
640
650
630
수신자
631
632
633
634
635
636
637
638
네트워크
관리자(인증 기관)
메타정보 제공 자
메타정보
계약정보
신뢰도 정보

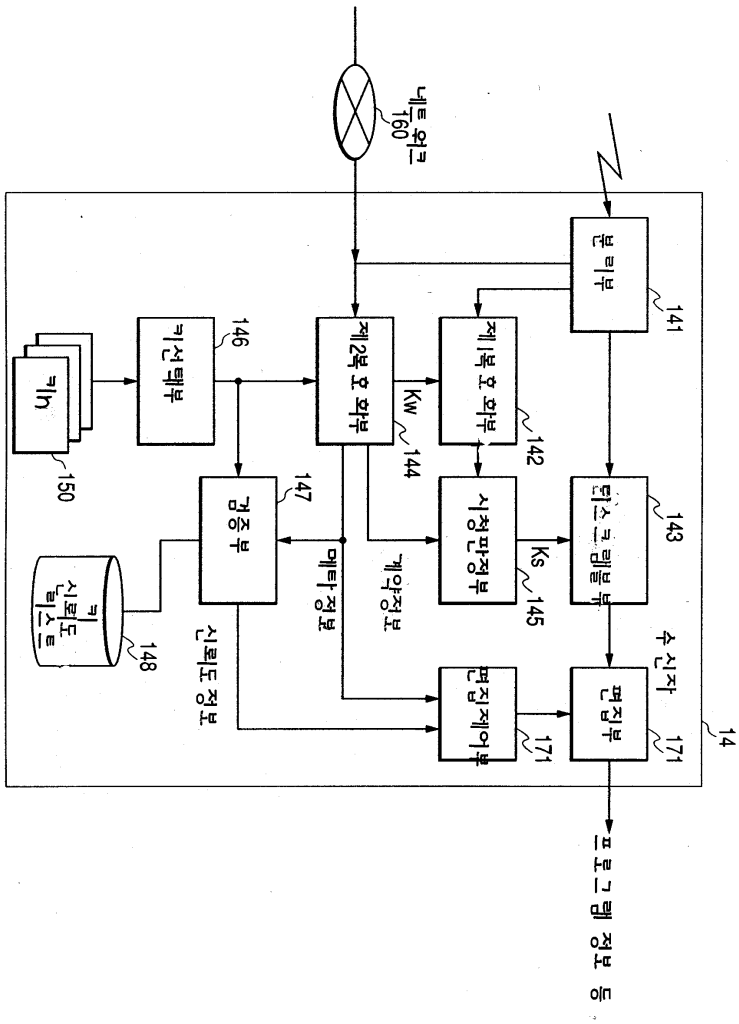
도면7


클래스 정보
프로그램 정보의 시청제어가 완전히 허가된 클래스
프로그램 정보의 시청이 제한된 클래스
프로그램 정보 다이제스트의 시청이 허가된 클래스

도면8


컨텐츠 등
스크램블
801
다중화
802
분리
809
디스크램블
810
컨텐츠 등
스크램블키
KS
803
워크키 Kw
804
계약정보
805
암호화
806
암호화
807
마스터키Km
808
복호화
811
복호화
812
마스터키Km
815
시청판정
813
Ks
계약정보
814
Kw

도면9


네트워크
160
분리부
141
제1복호화부
142
제2복호화부
144
Kw
키선택부
146
키In
150
검증부
147
시퀀스 넘버 정보
메타정보
계약정보
시퀀스 넘버 리스트
148
시퀀스 정보
시청판정부
145
Ks
디스크램블부
143
수신자
편집제어부
171
편집부
171
14
프로그램 정보 등