(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04L 9/14

(45) 공고일자 2003년12월03일
(11) 등록번호 10-0408287
(24) 등록일자 2003년11월22일

(21) 출원번호 10-2001-0033909
(22) 출원일자 2001년06월15일

(65) 공개번호 특2002-0095726
(43) 공개일자 2002년12월28일

(73) 특허권자 삼성전자주식회사
경기도 수원시 팔달구 매탄3동 416번지

(72) 발명자 주창남
서울특별시은평구역촌동21-37호

(74) 대리인 이영필
이해영

심사관 : 문태진

(54) 컨텐트 보호 시스템 및 방법

요약

본 발명은 컨텐트 보호 시스템 및 방법에 관한 것이다. 컨텐트 보호 방법의 컨텐트 전송 방법은 (a) 메인 서버가 회원으로 등록된 사용자로부터 그에게 유일하게 할당된 고유 정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하고, 사용자 시스템으로부터 고유키(HUK)를 수신하며, 사용자키를 고유키(HUK)로 암호화하는 단계, (b) 컨텐트 제공서버가 사용자 시스템으로부터의 컨텐트 요청신호에 의해 상기 메인서버로부터 사용자키를 수신하면, 생성된 소정의 암호화키(CEK) 및 소정의 암호 알고리즘으로 컨텐트를 암호화하여 사용자 시스템으로 전송하는 단계, (c) 사용자 시스템이 외부 디바이스로부터의 컨텐트 요청신호에 의해 외부 디바이스의 상호 인증을 통하여 공유 채널 및 소정의 채널키를 생성하고, 채널키로 다운받은 컨텐트를 암호화하여 공유 채널을 통해 전송하는 단계를 포함한다. 본 발명에 따르면, 컨텐트의 사용 권리를 저작권자가 원하는 대로 유통될 수 있도록 컨텐트를 암호화함으로써 불법 복제를 예방하고 사용권을 규정대로 관리 해주는 효과가 있다. 또한 사용자 키를 HUK로 암호화하여 사용자 키 노출의 위험 소지를 제거할 수 있으며, DRM 데이터베이스를 이용하여 저작권자가 원하는 방식대로 컨텐트를 배포할 수 있는 효과가 있다.

대표도

도 8

명세서

도면의 간단한 설명

도 1은 종래의 컨텐트 보호 시스템의 구성을 보이는 블록도 이다.
도 2는 본 발명에 따른 컨텐트 보호 시스템의 구성을 보이는 블록도 이다.
도 3은 도 2의 상세도 이다.
도 4는 도 3 중 CSP 서버에서 암호화부의 상세도 이다.
도 5는 도 3 중 클라이언트 시스템에서 컨텐트 복호화부의 상세도 이다.

도 6은 CSP 서버에서 컨텐트의 암호화 포맷을 보이는 도면이다.
도 7은 도 2에 도시된 클라이언트 시스템에 구축된 DRM 데이터베이스의 포맷을 보이는 도면이다.
도 8는 컨텐트 보호 방법의 동작을 보이는 흐름도 이다.
도 9은 사용 권한 인증 방법의 동작을 보이는 흐름도 이다.
도 10은 본 발명에 따른 컨텐트 암호화 및 전송 방법의 동작을 보이는 흐름도 이다.
도 11은 도 10 중 컨텐트 암호화 방법의 동작을 보이는 흐름도 이다.
도 12는 본 발명에 따른 컨텐트 해독 및 재생 방법의 동작을 보이는 흐름도 이다.
도 13은 컨텐트 다운로드 방법의 동작을 보이는 흐름도 이다.
도 14는 컨텐트 업 로드 방법의 동작을 보이는 흐름도 이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 암호화 시스템 및 방법에 관한 것으로, 디지털 데이터로 존재하는 모든 종류의 컨텐트의 사용 권리를 저작권자가 원하는 대로 유통될 수 있도록 컨텐트를 암호화함으로써 불법 복제를 예방하고 사용권을 규정대로 관리 해주는 컨텐트 보호 시스템 및 방법에 관한 것이다.
인터넷이 확산되어 디지털 컨텐트의 유통이 자유로워지면서 많은 디지털 데이터 또는 컨텐트가 저작권의 보호를 받지 못한 채 불법적인 복제가 이루어지고 있으며, 특히 개인간이 P2P 불법 유통이 일어나 저작권의 침해 사례가 늘고 있다.
도 1은 종래의 컨텐트 보호 시스템의 구성을 보이는 블록도로, 메인 서버(10)는 사용자 시스템(10)으로부터 회원 등록을 받고, 컨텐트의 암호를 해독하기 위한 사용자 키를 생성하여 CSP(Content Service Provider) 서버(11) 및 CSP 서버(11)를 통해 사용자 시스템(10)으로 전송한다. CSP 서버(11)는 사용자의 컨텐트 요청에 대응하여 메인 서버(10)에 사용자키를 요청하고, 이를 수신하여 컨텐트를 암호화하여 사용자 시스템(10)으로 전송한다. 사용자 시스템(12)은 메인 서버(10)로부터 전송된 사용자 키를 저장하고 있으며, CSP 서버(11)에 컨텐트를 요청하고, CSP 서버(11)로부터 전송된 암호화된 컨텐트를 사용자키로 해독하여 재생 및 저장 한다. 또한 사용자 시스템(12)은 디바이스(예를 들어, MP3 등)에 컨텐트를 전송한다. 디바이스(13)는 사용자 시스템(12)으로부터 사용자키 및 암호화된 컨텐트를 수신하고, 컨텐를 해독 및 재생한다.
종래의 컨텐트 보호 시스템은 단순히 인터넷 사용자마다 회원 가입 시에 고유의 키를 생성하여 사용자 시스템(12)에 저장하고, 컨텐트 구입 시에 ID와 Password로 사용자를 분간하고 해당 사용자의 고유키로 암호화 알고리즘을 이용하여 컨텐트를 암호화 한 후 사용자 시스템(12)으로 다운 로드한다. 사용자 시스템(12)에서는 컨텐트 재생 프로그램에서 컨텐트 재생 시에 저장되어 있는 고유키를 읽어와서 컨텐트를 복호화 시켜 재생한다. 사용자 시스템(12)와 통신하는 디바이스(13)도 고유키를 저장하고, 이 고유키를 이용하여 다운로드된 컨텐트를 복호화 시켜 재생한다.
이와 같은 종래의 컨텐트 보호 시스템으로는 컨텐트의 불법 사용을 완전히 차단할 수가 없는 문제점이 발생한다. 우선, 사용자 ID나 Password를 노출 시에 아무나 다른 사용자의 고유키를 받아 그 사용자의 컨텐트를 재생할 수 있으며, 이미 다운로드받은 사용자키를 컨텐트와 함께 넘겨주면 역시 누구든 컨텐트 사용이 가능하게 된다. 또한 종래의 컨텐트 보호 시스템은 단순 암호화 방식이므로 컨텐트 저작권자의 의지대로 컨텐트의 사용권리를 관리 할 수 없는 문제점이 발생한다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적인 과제는 고유한 키들을 이용하여 합법적으로 구매 또는 취득한 컨텐트를 암호화하여 배포함으로써 불법 복제를 방지하고 적법한 사용자만이 그 컨텐트를 사용하게 하는 컨텐트 보호 시스템을 제공하는데 있다.
본 발명이 이루고자 하는 다른 기술적인 과제는 고유한 키들을 이용하여 사용권한을 인증하고 합법적으로 구매 또는 취득한 컨텐트를 암호화/배포하여 재생함으로써 불법 복제를 방지하고 적법한 사용자만이 컨텐트 재생을 가능하게 하는 컨텐트 보호 방법을 제공하는데 있다.

발명의 구성 및 작용

본 발명이 이루고자 하는 기술적인 과제를 해결하기 위한 컨텐트 보호 시스템의 컨텐트 전송 장치는 자체적으로 고유키(HUK)를 생성하고, 외부 디바이스와 공유하는 소정의 채널키를 생성하고, 상기 채널키로 다운받은 컨텐트를 암호화하여 상기 외부 디바이스로 전송하는 사용자 시스템; 회원으로 등록된 사용자로부터 그에게 유일하게 할당된 고유정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하고, 상기 사용자 시스템으로부터 고유키(HUK)를 수

신하며, 상기 사용자키를 상기 고유키(HUK)로 암호화하여 상기 사용자 시스템으로 전송하는 메인서버; 및 상기 사용자 시스템으로부터의 컨텐트 요청신호에 의해 상기 메인서버로부터 사용자키를 수신하면, 생성된 소정의 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하여 상기 사용자 시스템으로 전송하는 컨텐트 제공서버를 포함하는 것이 바람직하다.

본 발명이 이루고자 하는 기술적인 과제를 해결하기 위한 컨텐트 보호 시스템의 컨텐트 복호화 장치는 컨텐트 제공서버로부터 제공된 암호화된 컨텐트를 복호화하는 장치에 있어서, 내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된 고유키(HUK)로 회원으로 등록된 사용자의 사용권한을 인정하는 암호화된 사용자키를 복호화하고, 상기 복호화된 사용자키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하며, 상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하고, 외부의 컨텐트 요청으로 상호 인증이 승인되면 공유채널과 함께 채널키를 생성하는 사용자 시스템; 및 상기 사용자 시스템의 상호인증 승인으로 공유채널로부터 암호화된 컨텐트와 채널키를 수신하고, 상기 채널키 및 자신의 고유 정보 조합에 의해 생성된 고유키로 상기 복호화된 헤더를 복호화하여 복호화키(CEK)를 추출하고 상기 복호화키(CEK) 및 소정의 복호 알고리즘으로 상기 컨텐트를 복호화하는 외부 디바이스를 포함하는 것이 바람직하다. 본 발명이 이루고자 하는 다른 기술적인 과제를 해결하기 위한 컨텐트 보호 방법의 컨텐트 전송 방법은 컨텐트 제공/복호 관리를 위한 메인 서버, 소정의 컨텐트를 제공하는 컨텐트 제공서버를 포함하며, 상기 컨텐트 서버로부터의 컨텐트를 사용자 시스템 및 외부 디바이스로 제공하는 방법으로서, (a) 상기 메인 서버가 회원으로 등록된 사용자로부터 그에게 유일하게 할당된 고유 정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하고, 상기 사용자 시스템으로부터 고유키(HUK)를 수신하며, 상기 사용자키를 상기 고유키(HUK)로 암호화하는 단계; (b) 상기 컨텐트 제공서버가 상기 사용자 시스템으로부터의 컨텐트 요청신호에 의해 상기 메인서버로부터 사용자키를 수신하면, 생성된 소정의 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하여 상기 사용자 시스템으로 전송하는 단계; 및 (c) 상기 사용자 시스템이 상기 외부 디바이스로부터의 컨텐트 요청신호에 의해 상기 외부 디바이스의 상호 인증을 통하여 공유 채널 및 소정의 채널키를 생성하고, 상기 채널키로 다운받은 컨텐트를 암호화하여 상기 공유 채널을 통해 전송하는 단계를 포함하는 것이 바람직하다.

본 발명이 이루고자 하는 다른 기술적인 과제를 해결하기 위한 컨텐트 보호 방법의 컨텐트 복호화 방법은 컨텐트 제공/복호 관리를 위한 메인서버, 소정의 컨텐트를 제공하는 컨텐트 제공서버를 포함하며, 상기 컨텐트 서버로부터 제공된 컨텐트를 사용자 시스템 및 외부 디바이스에서 복호화 하는 방법으로서, (a) 상기 사용자 시스템이 내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된 고유키(HUK)로 회원으로 등록된 사용자로의 사용권한을 인정하는 암호화된 사용자키를 복호화하고, 상기 복호화된 사용자 키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하며, 상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하고, 외부의 컨텐트 요청으로 상호 인증이 승인되면 공유채널과 함께 채널키를 생성하는 단계; 및 (b) 상기 사용자 시스템의 상호인증 수행으로 공유채널로부터 암호화된 컨텐트와 채널키를 수신하고, 상기 채널키 및 자신의 고유 정보 조합에 의해 생성된 고유키로 상기 복호화된 헤더를 복호화하여 복호화키(CEK)를 추출하고 상기 복호화키(CEK) 및 소정의 복호 알고리즘으로 상기 컨텐트를 복호화하는 단계를 포함하는 것이 바람직하다.

이하, 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

본 발명에서 컨텐트를 암호화하고, 해독하는 데는 다음과 같은 네 가지 키가 이용되는데, 본 발명의 상세한 설명 부분에 앞서 그 각각의 키에 대해 먼저 설명하기로 한다.

첫째, 메인 서버에서 생성하는 사용자키이다. 본 발명의 암호화 방식은 비대칭형 암호화 방식을 사용하며, 메인 서버는 컨텐트를 암호화하는 Public 키와 암호화된 컨텐트를 복호화 하는 Private 키를 생성한다. Pulbic 키는 컨텐트의 암호화를 위해 컨텐트 제공 서버로 전송하고, Private 키는 암호화된 컨텐트의 복호화를 위해 사용자 시스템으로 전송된다. 메인 서버에서 생성하는 사용자키는 회원으로 등록된 사용자의 고유 정보(예를 들면, ID, Pass word, 주민등록 번호 등)에 의해 생성된다.

둘째, 사용자 시스템에서 생성하는 HUK(Host Unit Key) 이다. HUK는 사용자 시스템의 고유 정보로 생성되는 키로, 각 사용자 시스템마다 HUK가 다르다. HUK는 사용자 시스템 내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된다. HUK는 메인 서버로 전송되며, 메인 서버는 Private 키를 HUK로 암호화하여 사용자 시스템으로 전송한다. 이 밖에 휴대용 디바이스도 자신만의 고유키를 생성하여 컨텐트 암호화 및 복호화 시에 이용한다.

셋째, 컨텐트 제공 서버에서 생성하는 CEK(Content Encrytion Key, 컨텐트 암호화 키)이다. CEK는 사용자에게 제공할 컨텐트를 암호화하기 위해 생성된다. 사용자가 의뢰한 컨텐트는 CEK로 암호화되어 사용자 시스템으로 전송된다.

넷째, 사용자 시스템에서 생성하여 휴대용 디바이스와 공유하는 채널키(Channel Key)이다. 사용자 시스템에서 휴대용 디바이스로 컨텐트 전송 시에 채널 키로 컨텐트를 암호화하며, 휴대용 디바이스는 사용자 시스템으로부터 전송된 암호화된 컨텐트를 채널키로 복호화 한다.

도 1 도 7을 참조하여 컨텐트 보호 시스템을 설명한다.

도 2는 본 발명에 따른 컨텐트 보호 시스템의 구성을 보이는 블록도로서, 메인 서버(20), 컨텐트 제공서버(21), 사용자 시스템(22), 휴대용 디바이스(23)로 구성된다.

메인 서버(20)는 키 관리 서버(KMS : Key Management Server)로, 본 발명의 청구범위에서는 관리수단으로 표기한다. 메인 서버(20)는 사용자 시스템(22)의 사용 권한을 검증하고, 사용자 키를 생성하며, 사용자키를 암호화하고, 이들을 관리한다. 도 3의 상세도를 보면, 사용자키 생성부(20-1)는 등록된 회원 정보(ID 및 Pass word) 외에 사용자에게 유일하게 할당된 고유 정보(예를 들면, 주민등록 번호 등)를 이용하여 컨텐트 암호화 및 복호화를 위한 사용자키(Public키, Private키)를 생성한다. 데이터베이스(20-2)는 회원으로 등록된 사용자 정보 및 사용자키를 저장한다. 암호화부(20-3)는 사용자 시스템(22)으로부터 HUK를 수신하고, 생성된 사용자키를 HUK로 암호화한다. 사용자키 중 H

UK로 암호화된 Public키는 컨텐트 제공서버(21)로 전송되고, 사용자키 중 HUK로 암호화된 Private키는 사용자 시스템(22)으로 전송된다. 암호화된 사용자키 또한 데이터베이스(20-2)에 저장된다. 사용권한 검증부(20-4)는 컨텐트 제공서버(21)의 요청으로 사용자키를 전송하기 위해 사용자 시스템(22)의 사용권한을 검증하고, 승인된 경우에만 사용자키 중 Public 키를 컨텐트 제공서버(21)로 전송한다. 사용자키는 메인 서버(20)에서 따로 관리되어 어느 사용자든 어느 컨텐트 제공 서버(21)를 통해 컨텐트를 제공받더라도 동일한 사용자키로 암호화 할 수 있게 한다. 각 컨텐트 제공 서버(21)마다 ID나 비밀번호가 다르더라도, 메인 서버(20)는 HUK를 이용하여 사용자키를 생성하기 때문에 어떤 컨텐트 제공 서버(21)에게도 같은 사용자키가 전송된다.

컨텐트 제공서버(21)는 사용자의 컨텐트 요청에 대해 메인 서버(20)로부터 사용자 키 중 Public키를 전송 받아 소정의 컨텐트를 암호화하여 전송한다. 도 3에 도시된 컨텐트 제공서버(21)의 상세도를 보면, 사용권한 검증부(21-1)는 사용자 시스템922)으로부터 입력된 사용자의 고유 정보(ID, Pass word, 주민등록번호)를 검증한다. 사용권한 검증부(21-1)는 메인 서버(20)에 접속하여 사용자의 고유 정보를 보내고, 승인이 난 경우 컨텐트 암호화를 위한 Public 키를 수신한다. 데이터베이스(21-2)는 사용자 정보 및 수신한 Public 키를 저장하고, 후에 암호화된 컨텐트 정보 또한 저장한다. 암호화부(21-3)는 메인 서버(20)로부터 전송된 Public 키로 컨텐트를 암호화한다. 암호화부(21-3)는 도 6에 도시된 바와 같은 포맷으로 컨텐트를 암호화하여 사용자 시스템(22)으로 전송한다. 도 6을 보면 컨텐트 암호화 포맷은 일반정보, DRM(Digital Right Management) 정보, 사용자 키 헤더 및 재 배포용 헤더로 구성된 헤더, 컨텐트로 구성된다. 일반 정보 영역에는 전송될 컨텐트의 ID가 기록된다. 전송될 컨텐트의 ID는 순수 컨텐트의 디지털 데이터를 일정 간격으로 추출하여 생성된다. DRM 정보 영역에는 저작권 소유자의 컨텐트 사용 규칙이 기록되는데, 그 규칙은 컨텐트를 재생할 수 있는 횟수, 재생할 수 있는 기간, 컨텐트를 전송할 수 있는 디바이스의 개수 등이 있다. 사용자 키 헤더 영역에는 컨텐트를 암호화할 CEK가 기록된다. 도 4에 암호화부(21-3)의 상세도가 도시되어 있다. CEK 생성부(21-31)는 컨텐트를 암호화하기 위해 랜덤하게 CEK를 생성한다. CEK는 사용자키 헤더 영역에 기록한다. 컨텐트 암호화부(21-32)는 CEK를 이용하여 승인된 사용자가 요청한 컨텐트를 암호화한다. 컨텐트 암호화부(21-32)는 CEK 및 암호화 알고리즘(예를 들어, SNAKE)을 이용하여 컨텐트를 암호화한다. DRM 정보 생성부(21-33)는 상기에 설명된 DRM 정보를 생성 및 지정하여 헤더의 DRM 정보 영역에 기록한다. 헤더 암호화부(21-34)는 사용자키 헤더, 재배포용 헤더를 포함하여 암호화될 컨텐트의 일반정보, DRM 정보를 암호화한다. 헤더 암호화부(21-34)는 메인 서버(20)로부터 전송된 Public 키 및 ECC 알고리즘으로 상기 헤더 및 그밖의 정보를 암호화 한다. 데이터 전송부(21-35)는 암호화된 컨텐트 및 헤더를 사용자 시스템(22)으로 전송한다.

사용자 시스템(22)은 전송된 컨텐트를 관리 및 재생하고 컨텐트를 휴대용 디바이스(23)로 전송한다. 도 3에 도시된 사용자 시스템(22)의 상세도를 보면, HUK 생성부(22-1)는 사용자 시스템만의 고유정보를 이용하여 HUK를 생성하여 저장부(22-2)에 저장하고, 메인 서버(20)로 전송한다. 컨텐트 복호화부(22-3)는 컨텐트 제공서버(21)로부터 전송된 컨텐트를 복호화 하여 재생한다. 도 5에 도시된 컨텐트 복호화부(22-3)의 상세도를 보면, DRM 데이터베이스 생성부(22-31)는 컨텐트 최초 재생 시에 저장부(22-2)의 안전한 장소에 DRM 데이터베이스를 생성한다. DRM 데이터베이스는 도 7에 도시된 바와 같은 형식으로 생성되는데, DRM 데이터베이스는 CID(Content ID), DRM 정보, 암호화된 컨텐트 형식으로 구성된다. CID에는 각 컨텐트 마다의 고유한 ID가 기록된다. CID는 암호화되기 전의 순수 컨텐트에 대해 일정 간격으로 추출된 디지털 데이터의 고유한 ID이다. DRM 정보에는 저작권자가 허용하는 컨텐트 관리 정보가 기록되어 있으며, 그 관리 정보는 컨텐트를 재생할 수 있는 횟수, 컨텐트를 재생할 수 있는 기간, 휴대용 디바이스(23)로 다운 로드할 수 있는 횟수 등이 있다. 암호화된 컨텐트에는 컨텐트 제공 서버(21)에서 전송된 암호화된 컨텐트가 기록되어 있다. DRM 데이터베이스는 컨텐트 사용 시마다 업데이트 된다. 컨텐트를 재생할 때 사용자는 CID를 이용하여 DRM 데이터베이스에 등록을 하고, 저작권자가 허용하는 컨텐트 관리 정보를 비교하여 사용 여부를 결정하고, 컨텐트 사용한 후에 DRM 데이터베이스를 업데이트 한다. DRM 데이터베이스는 유일하게 한 사용자 시스템(22)에서만 생성되어야 하고, 다른 사용자 시스템(미도시)을 사용할 때에는 Backup/Restore를 하여 컨텐트를 다른 사용자 시스템에 복사하여도 컨텐트 사용 여부는 같은 DRM 데이터베이스를 이용하기 때문에 제약을 받는다. 사용자키 복호화부(22-32)는 저장부(22-2)에 저장된 HUK로 메인 서버(20)에서 전송된 Private키를 복호화 하여 순수한 Private 키를 추출한다. CEK 복호화부(22-33)는 순수한 Private 키를 이용하여 ECC로 암호화된 헤더를 복호화 하여 CEK를 추출한다. 컨텐트 해독부(22-34)는 CEK를 이용하여 고유 알고리즘(예를 들어, SNAKE)로 암호화된 컨텐트를 복호화 한다. 컨텐트 재생부(22-35)는 복호화된 컨텐트를 재생한다. 사용자 시스템(22)은 컨텐트 재생 후에 DRM 데이터베이스를 업데이트 한다. 사용자 시스템(22)이 휴대용 디바이스(23)로 컨텐트를 전송하는 경우, DRM 데이터베이스에 CID로 다운로드 가능한지 확인을 한다. 컨텐트의 다운로드가 가능한 경우, 사용권한 검증부(22-4)는 휴대용 디바이스(23)와 통신하여 SAC(Secure Authenticate Channel)을 열어 상호 인증을 수행한다. 사용자 시스템(22)과 휴대용 디바이스(23)간에 인증이 승인되면, 채널키 생성부(22-5)는 채널키를 생성하여 휴대용 디바이스(23)와 공유한다. 컨텐트 암호화부(22-6)는 복호화된 컨텐트의 헤더를 채널키로 재 암호화하여 휴대용 디바이스(23)로 전송한다.

휴대용 디바이스(23)는 사용자 시스템(22)에서 전송된 컨텐트를 재생하거나 저장부(23-3)에 저장하며, 이동 가능한 저장부(23-5)로 전송한다. 휴대용 디바이스(23)는 디지털 컨텐트를 재생 또는 오픈하는 모든 디지털 디바이스를 의미한다. 도 3에 도시된 휴대용 디바이스의 상세도를 보면, 사용권한 인증부(23-1)는 사용자 시스템과(22)의 인증을 통하여 채널키를 생성하고 공유한다. 컨텐트 복호화부(23-3)는 전송된 컨텐트 중 헤더를 채널키를 이용하여 복호화하고, 컨텐트 암호화부(23-4)는 휴대용 디바이스(23) 자신의 고유한 정보의 조합으로 생성된 고유키로 헤더를 재 암호화한다. 이를 PD(Portable Device) 바인딩(Binding)이라 한다. 재생 시에 컨텐트 복호화부(23-3)는 휴대용 디바이스(23) 고유키로 헤더를 복호화 하여 CEK를 추출하고 CEK를 이용하여 컨텐트를 복호화 한 후 재생한다. 이동이 가능한 저장부(23-5)에 컨텐트를 전송하고자 하는 경우, 휴대용 디바이스(23) 고유키로 헤더를 복호화 한 후 이동이 가

능한 저장부(23-5)에서 생성된 고유키로 헤더를 재 암호화하여 저장한다. 이를 PM(Portable Memory) Binding 이라 한다. 사용자 시스템(22)의 DRM 데이터베이스에 디바이스 전송 여부(디바이스로 다운 로드된 횟수)를 업데이트 한다. 휴대용 디바이스(23)에서 컨텐트를 업 로드하는 경우, 역시 사용권한 인증부(23-1)를 통하여 상호 인증을 수행하고, 사용자 시스템으로 업로드 함을 통보한다. 휴대용 디바이스(23)는 저장부(23-3) 또는 이동이 가능한 저장부(23-5)에 저장된 컨텐트를 삭제하고, 사용자 시스템922)은 DRM 데이터베이스에 컨텐트가 업 로드되었음을 업데이트 한다.

도 8 도 14를 참조하여 본 발명을 상세히 설명한다.

도 8은 컨텐트 보호 방법의 동작을 보이는 흐름도로써, 크게 사용자키 생성단계(80), 컨텐트 암호화 및 전송단계(81), 컨텐트 해독 및 재생단계(82), 휴대용 디바이스로 다운/업로드 단계(83)로 구성되며, 이하 도면에서 이들 단계에 대해 상세히 설명한다.

도 9에 도시된 사용자키 생성단계(80)는 메인 서버(20)에서 수행하며, 우선 사용자의 고유 정보(ID, Pass word, 주민등록번호 등)를 수신하여 회원으로 등록시킨다(80-1단계). 회원이 등록된 사용자로부터 사용중인 사용자 시스템(22)의 고유 정보로 생성되는 HUK를 수신한다(80-2단계). 사용자 고유 정보로 컨텐트 암호화 및 복호화를 위한 사용자키(Public 키, Private 키)를 생성하고 HUK와 함께 저장한다(80-3단계). 사용자 시스템(22)으로 전송하기 위해 사용자키 중 Private 키를 HUK로 암호화한다(80-4단계). 암호화된 Private 키를 사용자 시스템(22)으로 전송한다(80-5단계). 본 발명에서 사용자키는 사용자에게 유일하게 할당된 고유정보에 의해 생성되므로 그 자체를 컨텐트 제공서버(21) 및 사용자 시스템(22)을 전송할 수 있고, 상기 사용자키는 HUK로 암호화하여 사용자 시스템(22)으로 전송할 수 있다.

도 10 및 도 11에 도시된 컨텐트 암호화 및 전송단계(81)는 컨텐트 제공서버(21)에서 수행하며, 사용자로부터 컨텐트 구입 요청 신호를 수신한다(81-1단계). 메인 서버(20)에 사용자 정보를 보내어 인증이 승인된 경우 Public 키를 수신한다(81-2단계). 메인 서버(20)로부터 전송된 Public 키를 이용하여 컨텐트를 암호하한다(81-3)단계. 암호화된 컨텐트를 사용자 시스템(22)으로 전송한다. 도 11에는 컨텐트 제공서버(21)에서 수행하는 컨텐트 암호화 방법을 도시하고 있다. 컨텐트는 도 6과 같은 포맷으로 암호화되며, 일반정보, DRM 정보, 사용자 키 헤더, 재 배포용 헤더로 구성된 헤더 및 컨텐트로 구성된다. 일반 정보 영역에는 전송될 컨텐트의 ID가 기록된다. DRM 정보 영역에는 저작권 소유자의 컨텐트 사용 규칙이 기록되는데, 그 규칙은 컨텐트를 재생할 수 있는 횟수, 재생할 수 있는 기간, 컨텐트를 전송할 수 있는 디바이스의 개수 등이 있다. 사용자 키 헤더 영역에는 컨텐트를 암호화할 CEK가 기록된다. 컨텐트 암호화를 위해 CEK를 랜덤하게 생성한다(81-31단계). CEK 및 고유 암호화 알고리즘(예를들어, SNAKE)를 이용하여 컨텐트를 암호화한다(81-32단계). CEK를 사용자키 헤더 영역에 기록한다(81-33단계). DRM 정보를 지정한다(81-34단계). 상기에 설명된 DRM 정보를 생성 및 지정하여 헤더의 DRM 정보 영역에 기록한다. 일반정보 영역, DRM 정보 영역, 사용자키 헤더 영역, 재배포용 헤더 영역으로 구성된 헤더를 메인 서버(20)로부터 수신한 Public 키와 ECC 암호화 알고리즘으로 암호화하고(81-35단계), 사용자 시스템(22)으로 전송한다(81-4단계).

도 12에 도시된 컨텐트 해독 및 재생단계(83)는 사용자 시스템(22)에서 수행하며, 컨텐트 최초 재생 시에 사용자 시스템의 안전한 장소(HDD)에 DRM 데이터베이스를 생성한다(82-1단계). DRM 데이터베이스는 도 7에 도시된 바와 같은 형식으로 생성되는데, DRM 데이터베이스는 CID(Content ID), DRM 정보, 암호화된 컨텐트 형식으로 구성된다. CID에는 각 컨텐트 마다의 고유한 ID가 기록된다. CID는 암호화되기 전의 순수 컨텐트에 대해 일정 간격으로 추출된 디지털 데이터의 고유한 ID이다. DRM 정보에는 저작권자가 허용하는 컨텐트 관리 정보가 기록되어 있으며, 그 관리 정보는 컨텐트를 재생할 수 있는 횟수, 컨텐트를 재생할 수 있는 기간, 휴대용 디바이스(23)로 다운 로드할 수 있는 횟수 등이 있다. 암호화된 컨텐트에는 컨텐트 제공 서버(21)에서 전송된 암호화된 컨텐트가 기록되어 있다. DRM 데이터베이스 생성 후에 HUK를 리드한다(82-2단계). 메인 서버(20)로부터 전송된 HUK로 암호화된 Private 키를 HUK로 복호화하여 순수한 사용자키 즉, Private 키를 추출한다(82-3단계). 순수한 Private 키를 이용하여 ECC 알고리즘으로 암호화된 헤더를 복호화 하여 CEK를 추출한다(82-4단계). CEK를 이용하여 고유 암호화 알고리즘(예를 들어, SNAKE)으로 암호화된 컨텐트를 복호화 하여 재생한다(82-5단계). 재생 후에 DRM 데이터베이스를 업데이트한다(82-6단계).

도 13 및 도 14의 휴대용 디바이스로 다운로드/업로드 단계(83)는 사용자 시스템(22) 및 휴대용 디바이스(23)에서 수행되며, 도 13은 다운로드 단계를, 도 14는 업로드 단계를 설명한다. 도 13 중 83a-1 83a-5 단계는 사용자 시스템(22)에서 수행되고, 이후 단계는 휴대용 디바이스(23)에서 수행된다. 컨텐트를 휴대용 디바이스로 다운로드하기 위해 우선, DRM 데이터베이스의 CID를 검색하여 다운로드가 가능한지 확인하다. 다운로드가 가능한 경우에, 사용자 시스템(22)은 휴대용 디바이스(23)와 SAC(Secure Authenticate Channel)을 열어 상호 인증을 수행한다(83a-1단계). 상호 인증이 확인되면, 채널키를 생성하고 휴대용 디바이스(23)와 공유한다(83a-2단계). 사용자 시스템(83a-3)은 HUK를 이용하여 순수 Private 키를 추출한 후 헤더를 복호화 한다(83a-3단계). 복호화된 헤더를 채널키로 재 암호화한다(83a-4단계). 재 암호화된 헤더 및 컨텐트를 휴대용 디바이스로 다운로드 한다(83a-5단계). 다운로드된 컨텐트는 휴대용 디바이스(23)에서 복호화 및 재생된다. 휴대용 디바이스(23)는 채널키로 암호화된 컨텐트의 헤더를 복호화한 후 자신의 고유한 정보의 조합으로 생성된 고유키로 헤더를 재 암호화하여 저장한다. 이를 PD(Portable Device) 바인딩(Binding)이라 한다. 재생 시에 자신의 고유키로 헤더를 복호화 하여 CEK를 추출하고 CEK를 이용하여 컨텐트를 복호화 한 후 재생한다. 컨텐트를 이동 가능한 저장부로 다운로드할 경우(83a-6단계), 컨텐트를 재 암호화한다(83a-7단계). 휴대용 디바이스(23)는 자신의 고유키 로 헤더를 복호화 한 후 이동이 가능한 저장부에서 생성된 고유키로 헤더를 재 암호화한다. 이를 PM(Portable Memory) Binding 이라 한다. 재 암호화된 컨텐트는 이동 가능한 저장부로 다운로드 된다(83a-8단계). 재생 시에 이동 가능한 저장부(다른 휴대용 디바이스에 장착)는 자신의 고유키로 헤더를 복호화 하여 CEK를 추출하고, CEK로 컨텐트를 복호화하여 재생이 가능하게 된다. 다운로드가 완료되면 사용자

시스템(22)의 DRM 데이터베이스에 디바이스 전송 여부(디바이스로 다운 로드된 횟수)를 업데이트 한다. 컨텐트 업로드의 경우, 사용자 시스템(22)과 휴대용 디바이스(23)는 SAC(Secure Authenticate Channel)을 열어 상호 인증을 수행한다(83b-1단계). 상호 인증이 확인되면, 휴대용 디바이스(23)는 사용자 시스템(22)으로 업로드 함으로 통보한다(83b-2단계). 통보 후에 휴대용 디바이스(23)는 내부 저장부 또는 이동이 가능한 저장부에 저장된 컨텐트를 삭제한다(83b-3단계). 컨텐트 삭제 후에 사용자 시스템(22)의 DRM 데이터베이스를 업데이트 한다(83b-4단계).
본 발명은 상술한 실시 예에 한정되지 않으며 본 발명의 사상 내에서 당업자에 의한 변형이 가능함은 물론이다.

발명의 효과

상술한 바와 같이 본 발명에 따르면, 컨텐트의 사용 권리를 저작권자가 원하는 대로 유통될 수 있도록 컨텐트를 암호화함으로써 불법 복제를 예방하고 사용권을 규정대로 관리 해주는 효과가 있다. 또한 사용자 키를 HUK로 암호화하여 사용자 키 노출의 위험 소지를 제거할 수 있으며, DRM 데이터베이스를 이용하여 저작권 자가 원하는 방식대로 컨텐트를 배포할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.
컨텐트 제공/복호 관리를 위한 메인 서버, 소정의 컨텐트를 제공하는 컨텐트 제공서버를 포함하며, 상기 컨텐트 서버로부터의 컨텐트를 사용자 시스템 및 외부 디바이스로 제공하는 방법으로서,
(a) 상기 메인 서버가 회원으로 등록된 사용자로부터 그에게 유일하게 할당된 고유 정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하고, 상기 사용자 시스템으로부터 고유키(HUK)를 수신하며, 상기 사용자키를 상기 고유키(HUK)로 암호화하는 단계;
(b) 상기 컨텐트 제공서버가 상기 사용자 시스템으로부터의 컨텐트 요청신호에 의해 상기 메인서버로부터 사용자키를 수신하면, 생성된 소정의 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하여 상기 사용자 시스템으로 전송하는 단계; 및
(c) 상기 사용자 시스템이 상기 외부 디바이스로부터의 컨텐트 요청신호에 의해 상기 외부 디바이스의 상호 인증을 통하여 공유 채널 및 소정의 채널키를 생성하고, 상기 채널키로 다운받은 컨텐트를 암호화하여 상기 공유 채널을 통해 전송하는 단계를 포함하는 컨텐트 제공 방법.

청구항 2.
제 1항에 있어서, 상기 (a)단계는
(a-1) 회원으로 등록된 상기 사용자로부터 그에게 유일하게 할당된 고유정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하는 단계;
(a-2) 상기 사용자 시스템으로부터 내부의 하드디스크 시리얼 번호 또는 O/S레벨 정보 등을 조합하여 생성된 고유키(HUK)를 수신하고, 상기 사용자키를 상기 고유키(HUK)로 암호화하는 단계; 및
(a-3) 상기 컨텐트 제공 서버의 요청으로 상기 사용자의 사용권한을 검증하여 상기 사용자키를 제공하는 단계를 포함하는 컨텐트 사용권한 검증부를 포함하는 것을 특징으로 하는 컨텐트 제공 방법.

청구항 3.
제 1항에 있어서, 상기 (b)단계는
(b-1) 상기 전송할 컨텐트를 암호화할 소정의 암호화키(CEK)를 생성하는 단계;
(b-2) 상기 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하고 상기 암호화키를 상기 컨텐트의 헤더에 기록하는 단계;
(b-3) 컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 생성하여 상기 컨텐트에 기록하는 단계;
(b-4) 상기 고유키와 소정의 암호 알고리즘으로 상기 헤더 및 컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 암호화하여 상기 컨텐트에 포함하는 단계; 및
(b-5) 상기 컨텐트의 데이터를 일정 간격으로 추출하여 생성한 컨텐트 ID, 상기 암호화된 컨텐트, 헤더 및 컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 상기 사용자 시스템으로 전송하는 단계를 포함하는 것을 특징으로 하는 컨텐트 제공방법.

청구항 4.
제 1항에 있어서, 상기 (c)단계는
(c-1) 내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 고유키(HUK)를 생성하는 단계;
(c-2) 상기 외부 디바이스와 상호 인증이 승인되면 공유채널과 함께 채널키를 생성하는 단계;
(c-3) 상기 고유키(HUK)로 상기 메인서버에서 전송된 사용자키의 암호를 복호화하고, 복호화된 상기 사용자키로 상기 컨텐트 중 암호화된 헤더를 복호화하는 단계; 및
(c-4) 상기 채널키로 상기 복호화된 헤더를 재 암호화한 후 상기 컨텐트에 삽입하여 상기 외부 디바이스로 전송하는 단계를 포함하는 것을 특징으로 하는 컨텐트 제공방법.

청구항 5.
삭제

청구항 6.

컨텐트 제공/복호 관리를 위한 메인서버, 소정의 컨텐트를 제공하는 컨텐트 제공서버를 포함하며, 상기 컨텐트 서버로부터 제공된 컨텐트를 사용자 시스템 및 외부 디바이스에서 복호화 하는 방법으로서,
(a) 상기 사용자 시스템이 내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된 고유키(HUK)로 회원으로 등록된 사용자로의 사용권한을 인정하는 암호화된 사용자키를 복호화하고, 상기 복호화된 사용자 키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하며, 상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하고, 외부의 컨텐트 요청으로 상호 인증이 승인되면 공유채널과 함께 채널키를 생성하는 단계; 및
(b) 상기 사용자 시스템의 상호인증 수행으로 공유채널로부터 암호화된 컨텐트와 채널키를 수신하고, 상기 채널키 및 자신의 고유 정보 조합에 의해 생성된 고유키로 상기 복호화된 헤더를 복호화하여 복호화키(CEK)를 추출하고 상기 복호화키(CEK) 및 소정의 복호 알고리즘으로 상기 컨텐트를 복호화하는 단계를 포함하는 컨텐트 복호화 방법.

청구항 7.

제 6항에 있어서, 상기 (a)단계는
(a-1) 상기 고유키(HUK)로 상기 메인서버에서 제공하는 회원으로 등록된 사용자로의 사용권한을 인정하는 암호화된 사용자키를 복호화하는 단계;
(a-2) 상기 복호화된 사용자키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하는 단계; 및
(a-3) 상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하는 단계를 포함하는 것을 특징으로 하는 컨텐트 복호화 방법.

청구항 8.

제 6항에 있어서, 상기 (b)단계는
(b-1) 상기 사용자 시스템의 상호인증 승인으로 공유채널로부터 암호화된 컨텐트와 채널키를 수신하는 단계;
(b-2) 상기 채널키 및 자신의 고유 정보 조합에 의해 생성된 고유키로 상기 복호화된 헤더를 복호화하여 복호화키(CEK)를 추출하는 단계; 및
(b-3) 상기 복호화키(CEK) 및 소정의 복호 알고리즘으로 상기 컨텐트를 복호화하는 단계를 포함하는 것을 특징으로 하는 컨텐트 복호화 방법.

청구항 9.

삭제

청구항 10.

삭제

청구항 11.

삭제

청구항 12.

삭제

청구항 13.

삭제

청구항 14.

삭제

청구항 15.

삭제

청구항 16.

삭제

청구항 17.

삭제

청구항 18.

삭제

청구항 19.

삭제

청구항 20.

삭제

청구항 21.

삭제

청구항 22.

삭제

청구항 23.

삭제

청구항 24.

삭제

청구항 25.

삭제

청구항 26.
자체적으로 고유키(HUK)를 생성하고, 외부 디바이스와 공유하는 소정의 채널키를 생성하고, 상기 채널키로 다운받은 컨텐트를 암호화하여 상기 외부 디바이스로 전송하는 사용자 시스템;
회원으로 등록된 사용자로부터 그에게 유일하게 할당된 고유정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하고, 상기 사용자 시스템으로부터 고유키(HUK)를 수신하며, 상기 사용자키를 상기 고유키(HUK)로 암호화하여 상기 사용자 시스템으로 전송하는 메인서버; 및
상기 사용자 시스템으로부터의 컨텐트 요청신호에 의해 상기 메인서버로부터 사용자키를 수신하면, 생성된 소정의 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하여 상기 사용자 시스템으로 전송하는 컨텐트 제공서버를 포함하는 컨텐트 전송장치.

청구항 27.
제 26항에 있어서, 상기 사용자 시스템은
내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 고유키(HUK)를 생성하는 고유키 생성부;
상기 외부 디바이스와 상호 인증이 승인되면 공유 채널과 함께 채널키를 생성하는 채널키 생성부; 및
상기 고유키(HUK)로 상기 메인서버에서 전송된 사용자키의 암호를 복호화하고, 복호화된 상기 사용자키로 상기 컨텐트 중 암호화된 헤더를 복호화하며, 상기 채널키로 상기 복호화된 헤더를 재암호화한 후 상기 컨텐트에 삽입하여 상기 외부 디바이스로 전송하는 암호화부를 포함하는 것을 특징으로 하는 컨텐트 전송 장치.

청구항 28.
제 26항에 있어서, 상기 메인 서버는
회원으로 등록된 상기 사용자로부터 그에게 유일하게 할당된 고유정보를 수신하여 컨텐트 사용권한을 인정하는 사용자키를 생성하는 사용자키 생성부;
상기 사용자 시스템으로부터 고유키(HUK)를 수신하고, 상기 사용자키를 상기 고유키(HUK)로 암호화하는 암호화부; 및
상기 컨텐트 제공 서버의 요청으로 상기 사용자의 사용권한을 검증하여 상기 사용자키를 제공하는 사용권한 검증부를 포함하는 것을 특징으로 하는 컨텐트 전송 장치.

청구항 29.
제 26항에 있어서, 상기 컨텐트 제공 서버는
상기 컨텐트를 암호화할 소정의 암호화키(CEK)를 생성하는 암호화키 생성부;
상기 암호화키(CEK) 및 소정의 암호 알고리즘으로 상기 컨텐트를 암호화하고 상기 암호화키를 상기 컨텐트의 헤더에 기록하는 컨텐트 암호화부;
컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 생성하여 상기 컨텐트에 기록하는 정보 생성부;
상기 고유키와 소정의 암호 알고리즘으로 상기 헤더 및 컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 암호화하여 상기 컨텐트에 포함하는 헤더 암호화부; 및
상기 컨텐트의 데이터를 일정 간격으로 추출하여 생성한 컨텐트 ID, 상기 암호화된 컨텐트, 헤더 및 컨텐트 저작권 소유자의 컨텐트 사용 규약 정보를 상기 사용자 시스템으로 전송하는 데이터 전송부를 포함하는 것을 특징으로 하는 컨텐트 전송 장치.

청구항 30.
컨텐트 제공 서버로부터 제공된 암호화된 컨텐트를 복호화하는 장치에 있어서,
내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된 고유키(HUK)로 회원으로 등록된 사용자의 사용권한을 인정하는 암호화된 사용자키를 복호화하고, 상기 복호화된 사용자키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하며, 상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하고, 외부의 컨텐트 요청으로 상호 인증이 승인되면 공유채널과 함께 채널키를 생성하는 사용자 시스템; 및
상기 사용자 시스템의 상호인증 승인으로 공유채널로부터 암호화된 컨텐트와 채널키를 수신하고, 상기 채널키 및 자신의 고유 정보 조합에 의해 생성된 고유키로 상기 복호화된 헤더를 복호화하여 복호화키(CEK)를 추출하고 상기 복호화키(CEK) 및 소정의 복호 알고리즘으로 상기 컨텐트를 복호화하는 외부 디바이스를 포함하는 컨텐트 복호화 장치.

청구항 31.
제 30항에 있어서, 상기 사용자 시스템은
내부의 하드디스크 시리얼 번호 또는 O/S 레벨 정보 등을 조합하여 생성된 고유키(HUK)로 회원으로 등록된 사용자의 사용권한을 인정하는 암호화된 사용자키를 복호화하는 사용자키 복호화부;
상기 복호화된 사용자키로 상기 컨텐트의 헤더를 복호화하여 복호화키(CEK)를 추출하는 복호화키 추출부;
상기 복호화키 및 소정의 알고리즘에 의해 상기 컨텐트를 복호화하는 컨텐트 복호화부; 및
상기 외부 디바이스의 컨텐트 요청으로 상기 외부 디바이스와 상호 인증이 승인되면 공유 채널과 함께 채널키를 생성하는 사용권한 검증부를 포함하는 것을 특징으로 하는 컨텐트 복호화 장치.

청구항 32.
삭제

청구항 33.
삭제

청구항 34.

삭제

청구항 35.

삭제

청구항 36.

삭제

청구항 37.

삭제

청구항 38.

삭제

청구항 39.

삭제

청구항 40.

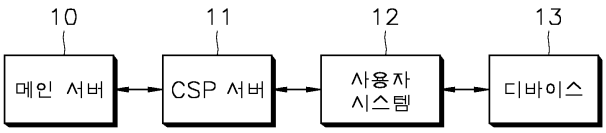
삭제

청구항 41.

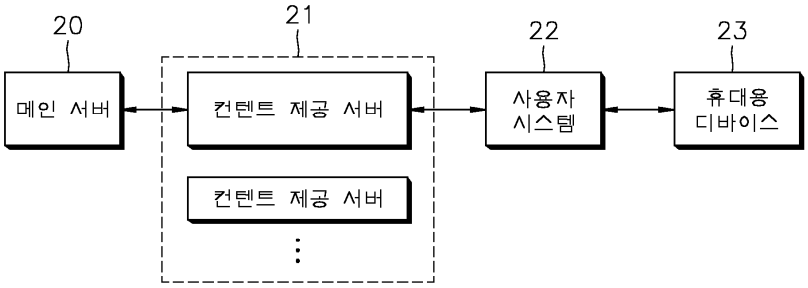
삭제

도면

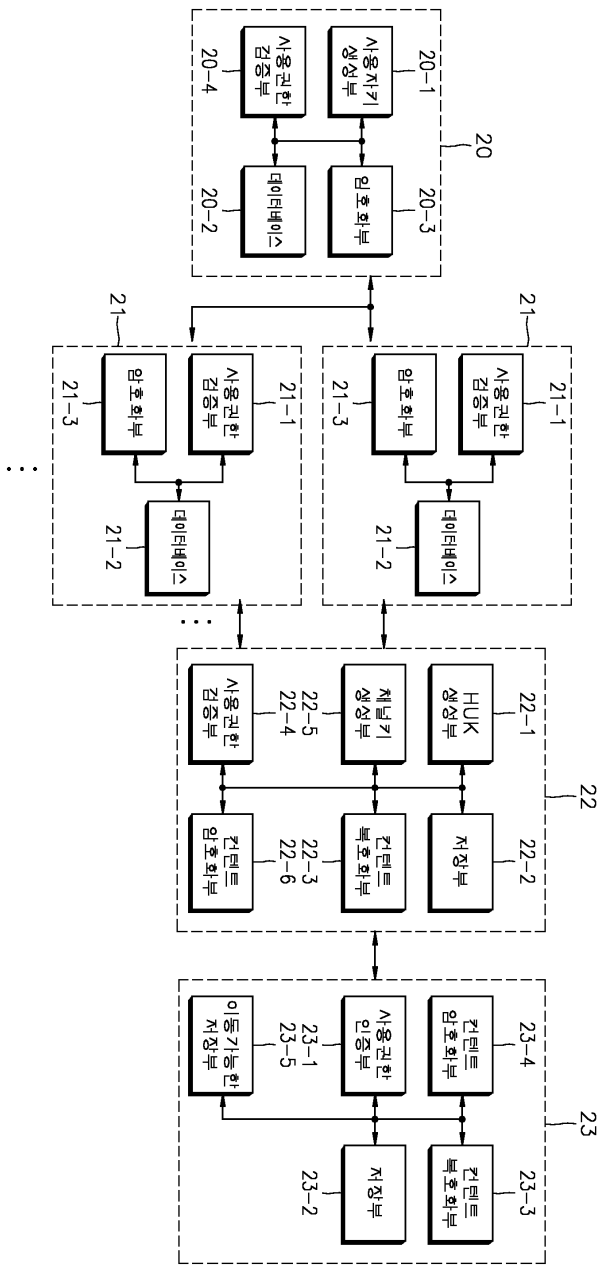
도면1



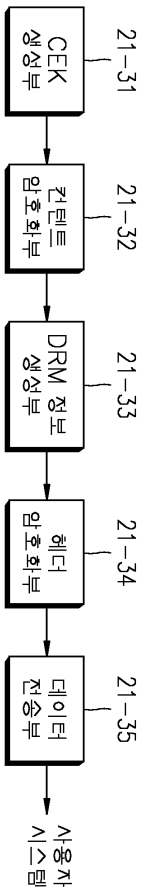
도면2



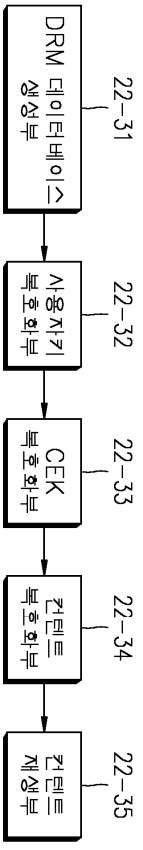
도면3


20
20-1
사용자키 생성부
20-4
사용권한 검증부
20-2
데이터베이스
20-3
암호화부
21
21-1
사용권한 검증부
21-3
암호화부
21-2
데이터베이스
22
22-1
HUK 생성부
22-5
22-4
사용권한 검증부
채널키 생성부
22-2
저장부
22-3
22-6
컨텐트 암호화부
컨텐트 복호화부
23
23-1
23-5
이동가능한 저장부
사용권한 인증부
23-4
컨텐트 암호화부
23-2
저장부
23-3
컨텐트 복호화부

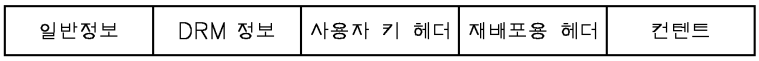
도면4


CEK 생성부
21-31
컨텐트 암호화부
21-32
DRM 정보 생성부
21-33
헤더 암호화부
21-34
데이터 전송부
21-35
사용자 시스템

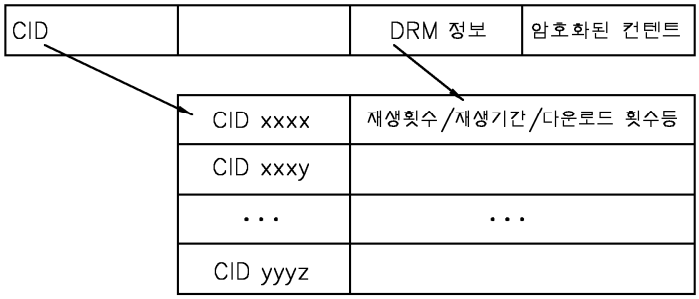
도면5


DRM 데이터베이스 생성부
22-31
사용자키 복호화부
22-32
CEK 복호화부
22-33
컨텐트 복호화부
22-34
컨텐트 제생부
22-35

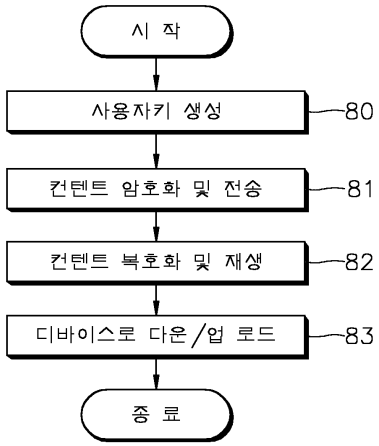
도면6



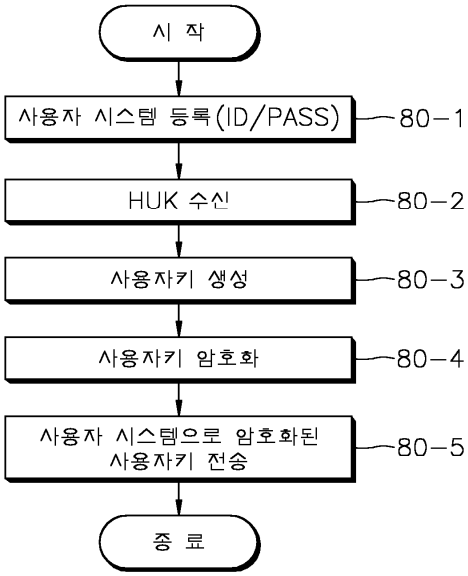
도면7



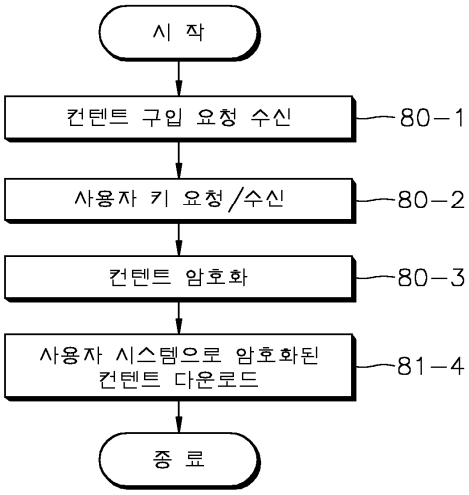
도면8



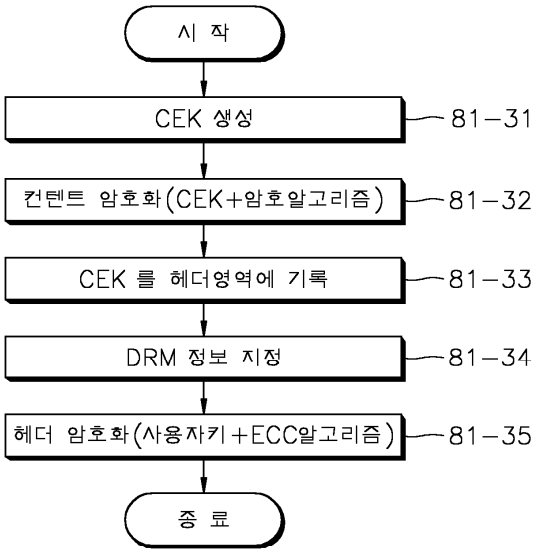
도면9



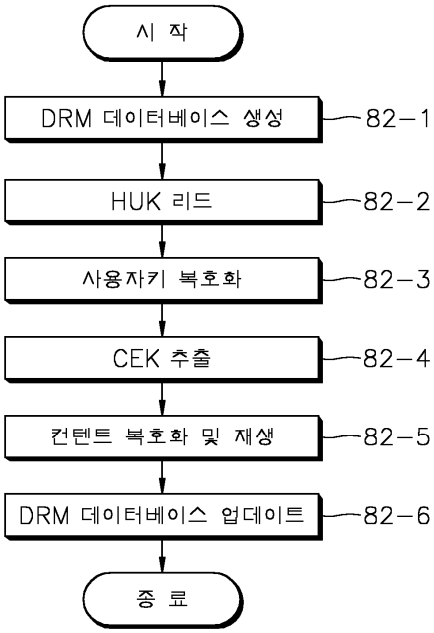
도면10



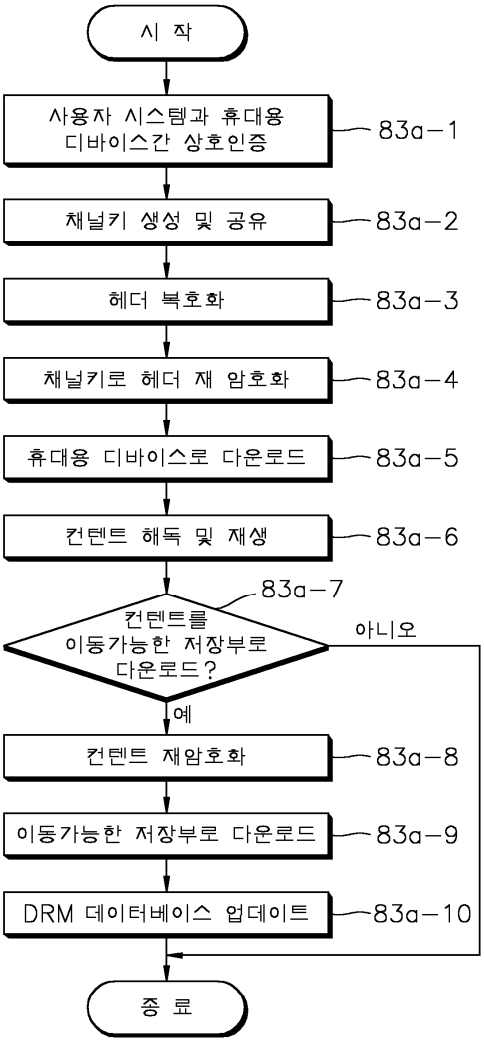
도면11



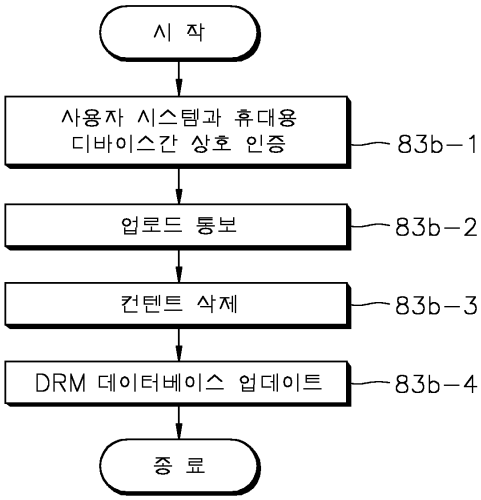
도면12



도면13


시 작
사용자 시스템과 휴대용 디바이스간 상호인증
83a-1
채널키 생성 및 공유
83a-2
헤더 복호화
83a-3
채널키로 헤더 재 암호화
83a-4
휴대용 디바이스로 다운로드
83a-5
컨텐트 해독 및 재생
83a-6
83a-7
컨텐트를 이동가능한 저장부로 다운로드?
아니오
예
컨텐트 재암호화
83a-8
이동가능한 저장부로 다운로드
83a-9
DRM 데이터베이스 업데이트
83a-10
종 료

도면14


시 작
사용자 시스템과 휴대용 디바이스간 상호 인증
83b-1
업로드 통보
83b-2
컨텐트 삭제
83b-3
DRM 데이터베이스 업데이트
83b-4
종 료