(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0050013
(43) 공개일자 2013년05월15일

(51) 국제특허분류(Int. Cl.)
G06F 21/24 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2011-0115132
(22) 출원일자 2011년11월07일
심사청구일자 2011년11월07일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침3단지 아파트 1404호 (내수동)
박승환
서울특별시 동작구 노량진로6마길 8 (노량진동)
(뒷면에 계속)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 5 항

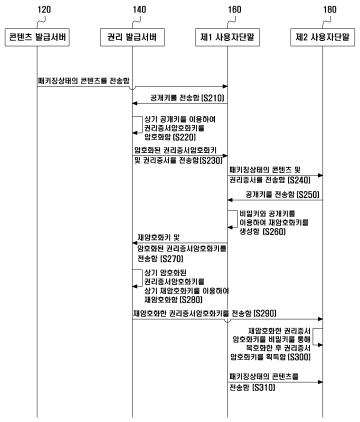
(54) 발명의 명칭 **DRM 시스템의 콘텐츠 공유방법**

(57) 요 약

본 발명은 DRM 시스템의 콘텐츠 공유방법에 관한 것으로, 보다 구체적으로는 권리발급서버가 상기 복수 개의 사용자단말 중 제1 사용자단말에 기저장된 공개키를 이용하여 상기 콘텐츠를 이용하기 위한 권리증서암호화키를 암호화하고, 암호화된 권리증서암호화키 및 상기 콘텐츠에 대한 암호화키를 포함하는 권리증서를 상기 제1 사용자단말로 전송하는 암호화단계; 상기 제1 사용자단말이 기저장된 패키징상태의 콘텐츠와, 상기 권리증서를 제2 사용자단말의 외부메모리로 전송하는 권리증서전송단계; 상기 제1 사용자단말이 기저장된 비밀키 및 상기 제2 사용자단말의 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성하고, 상기 암호화된 권리증서암호화키를 상기 권리발급서버로 전송하는 재암호화키생성단계; 상기 권리발급서버가 수신한 상기 암호화된 권리증서암호화키를 상기 재암호화키를 이용하여 재암호화한 후, 재암호화한 권리증서암호화키를 상기 제2 사용자단말의 외부메모리로 전송하는 재암호화단계; 상기 제2 사용자단말이 수신한 상기 재암호화한 권리증서암호화키를 자신의 외부메모리에 기저장된 비밀키를 이용하여 복호화하여 권리증서암호화키를 획득하는 키획득단계; 및 상기 제2 사용자단말이 획득한 상기 권리증서암호화키에 따라 상기 제1 사용자단말로부터 콘텐츠를 수신하는 콘텐츠수신단계;를 포함한다.

이러한 구성에 의해, 본 발명의 DRM 시스템의 콘텐츠 공유방법은 사용자단말의 공개키를 통해 암호화된 권리증서암호화키를 재암호화함에 따라, 복수 개의 사용자단말이 상기 암호화된 권리증서암호화키를 복호화하고 다시 암호화하는 과정을 수행하지 않고, 재암호화과정만을 수행함으로써, 상기 복수 개의 사용자단말간에 용이하게 콘텐츠를 공유할 수 있는 효과가 있다.

대 표 도 - 도2



(72) 발명자

김기탁

경기도 용인시 기흥구 고매동 동성아파트 102동 1407호

구우권

서울특별시 서초구 신반포로33길 15, 108동 1201호 (잠원동, 동아아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	ITAC1090111100020001000100100
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 연구센터(스마트 그리드 보안기술 개발)
주관기관	고려대학교 산학협력단
연구기간	2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

요청받은 콘텐츠를 발급하는 콘텐츠발급서버 및 상기 콘텐츠를 제공받을 수 있는 권리를 제공하는 권리발급서버를 통해 복수 개의 사용자단말이 상기 콘텐츠를 공유하는 DRM 시스템의 콘텐츠 공유 방법에 있어서,

상기 권리발급서버가 상기 복수 개의 사용자단말 중 제1 사용자단말에 기저장된 공개키를 이용하여 상기 콘텐츠를 이용하기 위한 권리증서암호화키를 암호화하고, 암호화된 권리증서암호화키 및 상기 콘텐츠에 대한 암호화키를 포함하는 권리증서를 상기 제1 사용자단말로 전송하는 암호화단계;

상기 제1 사용자단말이 기저장된 패키징상태의 콘텐츠와, 상기 권리증서를 제2 사용자단말의 외부메모리로 전송하는 권리증서전송단계;

상기 제1 사용자단말이 기저장된 비밀키 및 상기 제2 사용자단말의 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성하고, 상기 암호화된 권리증서암호화키를 상기 권리발급서버로 전송하는 재암호화키생성단계;

상기 권리발급서버가 수신한 상기 암호화된 권리증서암호화키를 상기 재암호화키를 이용하여 재암호화한 후, 재암호화한 권리증서암호화키를 상기 제2 사용자단말의 외부메모리로 전송하는 재암호화단계;

상기 제2 사용자단말이 수신한 상기 재암호화한 권리증서암호화키를 자신의 외부메모리에 기저장된 비밀키를 이용하여 복호화하여 권리증서암호화키를 획득하는 키획득단계; 및

상기 제2 사용자단말이 획득한 상기 권리증서암호화키에 따라 상기 제1 사용자단말로부터 콘텐츠를 수신하는 콘텐츠수신단계;

를 포함하는 것을 특징으로 하는 DRM 시스템의 콘텐츠 공유 방법.

청구항 2

제1항에 있어서,

상기 암호화단계는

상기 권리발급서버가 상기 제1 사용자단말로부터 상기 제1 사용자단말의외부메모리에 기저장된 공개키를 수신하는 공개키수신과정;

상기 권리발급서버가 상기 제1 사용자단말로부터 수신한 공개키를 이용하여 상기 콘텐츠를 이용하기 위한 권리증서암호화키를 암호화하는 암호화과정; 및

상기 권리발급서버가 암호화된 권리증서암호화키 및 상기 권리증서를 상기 제1 사용자단말의 외부메모리로 전송하는 전송과정;

을 포함하는 것을 특징으로 하는 DRM 시스템의 콘텐츠 공유 방법.

청구항 3

제1항에 있어서,

상기 재암호화키생성단계는

상기 제1 사용자단말이 상기 콘텐츠를 제공받고자 하는 제2 사용자단말의 외부메모리로부터 공개키를 수신하는 공개키수신과정;

상기 제1 사용자단말이 외부메모리에 기저장된 비밀키와 상기 제2 사용자단말의 외부메모리로부터 수신한 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성하는 재암호화키생성과

정; 및

상기 제1 사용자단말이 상기 재암호화키 및 상기 암호화된 권리증서암호화키를 상기 권리발급서버로 전송하는 전송과정;

을 포함하는 것을 특징으로 하는 DRM 시스템의 콘텐츠 공유 방법.

청구항 4

제1항에 있어서,

상기 외부메모리는 상기 제1 사용자단말 및 제2 사용자단말에 개별적으로 탈부착되는 스마트카드인 것을 특징으로 하는 DRM 시스템의 콘텐츠 공유 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 DRM 시스템의 콘텐츠 공유방법에 관한 것으로, 특히 복수 개의 사용자단말이 동일한 콘텐츠를 서로 공유하여 이용할 수 있는 DRM 시스템의 콘텐츠 공유방법에 관한 것이다.

배 경 기 술

[0002] IT분야의 기술이 급속도로 발전함에 따라, 다양한 콘텐츠들이 기하급수적으로 발생되어, 남녀노소 많은 사용자들에게 제공되고 있다. 이러한 콘텐츠들은 정당하게 비용을 지불하여 사용권을 가진 사용자만이 이용할 수 있도록 상기 콘텐츠들을 제공한 사람에게 권리와 이익을 보호해줘야 하지만, 다양한 방법을 통해 많은 사용자들이 상기 콘텐츠들을 불법복제하여 상기 콘텐츠들을 정당한 대가를 지불하지 않고, 무단으로 사용하고 있는 것이 현실이다.

[0003] 이를 방지하고자 DRM 기술이 연구개발되었다. 상기 DRM 기술이란, 디지털 저작권 관리(Digital Right Management)를 나타내는 것으로서, 디지털 콘텐츠의 불법복제에 따른 무단 사용을 막아, 제공자의 권리와 이익을 보호해주는 기술과 서비스를 말한다.

[0004] 이러한 DRM 기술은 요청받은 콘텐츠를 공유하도록 발급하는 콘텐츠발급서버와, 상기 콘텐츠를 이용할 수 있는 권리를 제공하는 권리발급서버(또는 지역권리관리서버) 및 상기 콘텐츠를 제공받는 사용자단말 또는 DRM에이전트(이하, 사용자단말이라고 한다)로 구성되는 시스템을 통해 구현된다.

[0005] 이때, 복수 개의 사용자단말이 특정 콘텐츠를 상호 공유하기 위해서는 상기 콘텐츠에 접근하기 위한 권리증서암호화키를 상호 분배해야한다. 따라서, 복수 개의 사용자단말 중 사용자단말 A의 공개키로 암호화된 권리증서암호화키를 사용자단말 B에게 공유하기 위해서는 상기 사용자단말 B가 상기 사용자단말 A의 공개키로 암호화된 권리증서암호화키를 복호화한 후, 자신의 공개키로 다시 암호화해야함에 따라 문제점이 생성되었다.

[0006] 상술한 바와 같이, DRM 시스템의 콘텐츠 공유 방법에 대한 선행기술을 살펴보면 다음과 같다.

[0007] 선행기술 1은 한국공개특허공보 제2009-0060470호(2009.06.15)로서, 디지털 저작권 관리 방법에 관한 것이다. 이러한 선행기술 1은 인증을 이용한 신뢰할 수 있는 사용자에게 콘텐츠 제공 서비스를 지원하는 시스템에서, 라이센스와 콘텐츠에 포함된 키들의 조합으로 생성되는 암복호화 키의 제공을 통해 보다 안전한 디지털 저작권 관리를 지원할 수 있다.

[0008] 또한, 선행기술 2는 한국공개특허공보 제2011-0111256호(2011.10.10)로서, 방송 서비스의 암호화 키 관리 방법 및 시스템에 관한 것이다.

[0009] 이러한 선행기술 2는 DRM 에이전트로부터 적어도 하나의 영역으로 구분된 콘텐츠의 수신에 요구되는 권리 객체를 요청하는 메시지를 수신하고, 제1키 및 제2키를 포함하는 시드키 쌍을 생성하며, 제1키 및 제2키에 서로 다른 방향의 해시 체인을 적용하여 적어도 하나의 영역 각각에 대한 적어도 하나의 암호화키를 생성하며, 콘텐츠의 식별자를 포함하는 콘텍스트 엘리먼트와 키정보 엘리먼트를 포함하는 응답 메시지를 DRM 에이전트로 전송하며, 키정보 엘리먼트는 암호화키에 대한 정보를 포함하는 제1암호화키 엘리먼트, 권리 암호키 기준에 대한 정보를 포함하는 권리 암호키 정보 엘리먼트, 및 암호화 시드를 포함하는 암호데이터 엘리먼트를 포함하여, 방송 서비스 데이터의 콘텐츠 스트림을 보호할 수 있는 효율적인 암호화 키 관리 방식을 제공할 수 있다.

발명의 내용

해결하려는 과제

[0010] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 복수 개의 사용자단말의 공개키를 통해 암호화된 권리증서암호화키를 재암호화함으로써, 상기 복수 개의 사용자단말이 용이하게 콘텐츠를 공유할 수 있는 DRM 시스템의 콘텐츠 공유방법을 제공하고자 한다.

과제의 해결 수단

[0011] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 요청받은 콘텐츠를 발급하는 콘텐츠발급서버 및 상기 콘텐츠를 제공받을 수 있는 권리를 제공하는 권리발급서버를 통해 복수 개의 사용자단말이 상기 콘텐츠를 공유하는 DRM 시스템의 콘텐츠 공유 방법은 상기 권리발급서버가 상기 복수 개의 사용자단말 중 제1 사용자단말에 기저장된 공개키를 이용하여 상기 콘텐츠를 이용하기 위한 권리증서암호화키를 암호화하고, 암호화된 권리증서암호화키 및 상기 콘텐츠에 대한 암호화키를 포함하는 권리증서를 상기 제1 사용자단말로 전송하는 암호화단계; 상기 제1 사용자단말이 기저장된 패키징상태의 콘텐츠와, 상기 권리증서를 제2 사용자단말의 외부메모리로 전송하는 권리증서전송단계; 상기 제1 사용자단말이 기저장된 비밀키 및 상기 제2 사용자단말의 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성하고, 상기 암호화된 권리증서암호화키를 상기 권리발급서버로 전송하는 재암호화키생성단계; 상기 권리발급서버가 수신한 상기 암호화된 권리증서암호화키를 상기 재암호화키를 이용하여 재암호화한 후, 재암호화한 권리증서암호화키를 상기 제2 사용자단말의 외부메모리로 전송하는 재암호화단계; 상기 제2 사용자단말이 수신한 상기 재암호화한 권리증서암호화키를 자신의 외부메모리에 기저장된 비밀키를 이용하여 복호화하여 권리증서암호화키를 획득하는 키획득단계; 및 상기 제2 사용자단말이 획득한 상기 권리증서암호화키에 따라 상기 제1 사용자단말로부터 콘텐츠를 수신하는 콘텐츠수신단계;를 포함하는 것을 특징으로 한다.

[0012] 보다 바람직하게는 상기 권리발급서버가 상기 제1 사용자단말로부터 상기 제1 사용자단말의외부메모리에 기저장된 공개키를 수신하는 공개키수신과정; 상기 권리발급서버가 상기 제1 사용자단말로부터 수신한 공개키를 이용하여 상기 콘텐츠를 이용하기 위한 권리증서암호화키를 암호화하는 암호화과정; 및 상기 권리발급서버가 암호화된 권리증서암호화키 및 상기 권리증서를 상기 제1 사용자단말의 외부메모리로 전송하는 전송과정;을 포함하는 암호화단계를 포함할 수 있다.

[0013] 보다 바람직하게는 상기 제1 사용자단말이 상기 콘텐츠를 제공받고자 하는 제2 사용자단말의 외부메모리로부터 공개키를 수신하는 공개키수신과정; 상기 제1 사용자단말이 외부메모리에 기저장된 비밀키와 상기 제2 사용자단말의 외부메모리로부터 수신한 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성하는 재암호화키생성과정; 및 상기 제1 사용자단말이 상기 재암호화키 및 상기 암호화된 권리증서암호화키를 상기 권리발급서버로 전송하는 전송과정;을 포함하는 재암호화키생성단계를 포함할 수 있다.

[0014] 특히, 상기 외부메모리는 상기 제1 사용자단말 및 제2 사용자단말에 개별적으로 탈부착되는 스마트카드일 수 있다.

발명의 효과

[0015] 본 발명의 DRM 시스템의 콘텐츠 공유방법은 사용자단말의 공개키를 통해 암호화된 권리증서암호화키를 재암호화함에 따라, 복수 개의 사용자단말이 상기 암호화된 권리증서암호화키를 복호화하고 다시 암호화하는 과정을 수행하지 않고, 재암호화과정만을 수행함으로써, 상기 복수 개의 사용자단말간에 용이하게 콘텐츠를 공유할 수 있는 효과가 있다.

[0016] 또한 본 발명의 DRM 시스템의 콘텐츠 공유방법은 콘텐츠를 공유하고자 하는 복수 개의 사용자단말간에 재암호화키 및 권리증서암호화키와 같은 그 크기가 작은 키들이 상호 공유됨에 따라, 키 분배가 빠르고 효율적으로 될 수 있는 효과가 있다.

[0017] 더불어, 본 발명의 DRM 시스템의 콘텐츠 공유방법은 권리발급서버가 공격자에 의해 공격받았다고 하더라도 암호화되지 않은 권리증서암호화키에 대한 정보를 확인할 수 없어 공격자로부터 보다 안전하게 콘텐츠를 공유할 수 있는 효과가 있다.

[0018] 이와 더불어, 본 발명의 DRM 시스템의 콘텐츠 공유방법은 복수 개의 사용자단말이 콘텐츠 공유에 사용되는 비밀키, 공개키, 권리증서암호화키 등을 탈부착가능한 외부메모리에 저장함으로써, 키 정보가 외부로 노출되지 않도록 안전하게 보호할 수 있는 효과가 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시 예에 따른 DRM 시스템의 콘텐츠 공유방법을 개략적으로 나타낸 도면이다.

도 2는 도 1의 DRM 시스템의 콘텐츠 공유방법을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[0021] 먼저, 본 발명의 DRM 시스템의 콘텐츠 공유방법을 개략적으로 살펴보도록 한다.

[0022] 도 1은 본 발명의 일 실시 예에 따른 DRM 시스템의 콘텐츠 공유방법을 개략적으로 나타낸 도면이다.

[0023] 도 1에 도시된 바와 같이, DRM 시스템(100)은 사용자단말로부터 이용을 요청받은 콘텐츠를 발급하는 콘텐츠발급서버(120), 상기 콘텐츠의 이용을 위해 요청한 사용자단말에 대하여 상기 콘텐츠를 이용할 수 있는 권리증서(Right Object)를 발급하는 권리발급서버(140), 상기 콘텐츠발급서버(120)로부터 발급된 상기 콘텐츠를 제공받는 복수 개의 사용자단말(160, 180)로 구성된다.

[0024] 상기 권리발급서버(140)는 사용자단말의 공개키를 이용하여 권리증서암호화키를 암호화한다.

[0025] 상기 복수 개의 사용자단말 중 제1 사용자단말(160)은 상기 콘텐츠발급서버(120)로부터 패키징상태(DCF: DRM Content Format)의 콘텐츠와 상기 콘텐츠를 이용할 수 있는 권리증서를 제공받고, 제공받은 패키징상태의 콘텐츠 및 권리증서를 상기 콘텐츠를 공유하고자 하는 제2 사용자단말로 전송하여, 자신의 공개키로 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성한다.

[0026] 상기 권리발급서버(140)가 암호화된 권리증서암호화키를 상기 재암호화키를 이용하여 재암호화하면, 상기 콘텐츠를 공유하고자 하는 제2 사용자단말(180)이 재암호화한 권리증서암호화키를 기저장된 비밀키를 이용하여 복호화하고, 상기 콘텐츠를 이용할 수 있는 권리증서암호화키를 획득하여, 상기 제1 사용자단말과 함께 동일한 콘텐츠를 공유할 수 있다.

[0027] 이하, 도 2를 참조하여, 본 발명의 DRM 시스템의 콘텐츠 공유 방법에 대하여 자세히 살펴보도록 한다.

[0028] 도 2는 도 1의 DRM 시스템의 콘텐츠 공유방법을 나타낸 순서도이다.

[0029] 도 2에 도시된 바와 같이, 먼저, 콘텐츠를 발급하는 콘텐츠발급서버(120)가 복수 개의 사용자단말 중 제1 사용

자단말(160)로 요청한 콘텐츠를 제공하여, 상기 제1 사용자단말은 해당 콘텐츠를 이용할 수 있게 된다.

[0030] 이어서, 상기 제1 사용자단말(160)은 상기 권리발급서버(140)로 자신에게 부착되어 있는 외부메모리 즉, 스마트카드에 기저장된 공개키를 전송한다(S210).

[0031] 이에 따라, 상기 권리발급서버(140)는 상기 제1 사용자단말(160)로부터 수신한 상기 제1 사용자단말(160)의 공개키를 이용하여 콘텐츠 이용을 위해 사용되는 권리증서암호화키를 암호화한다(S220).

[0032] 이후, 상기 권리발급서버(140)는 앞서 과정 S220을 통해 암호화된 권리증서암호화키와, 기저장하고 있는 권리증서(Right Object)를 상기 제1 사용자단말(160)에 부착된 스마트카드로 전송한다(S230).

[0033] 이와 같이, 상기 권리발급서버(120)로부터 암호화된 권리증서암호화키와, 권리증서를 수신한 상기 제1 사용자단말(160)은 앞서 상기 권리발급서버(120)로부터 제공받은 패키징상태의 콘텐츠와, 앞서 과정 S230에서 수신한 권리증서를 상기 콘텐츠를 공유하고자 하는 제2 사용자단말(180)에 부착된 스마트카드로 전송한다(S240).

[0034] 이에 따라, 상기 제2 사용자단말(180)은 암호화된 권리증서암호화키를 재암호화하도록 재암호화키 생성에 사용되며, 자신에게 부착된 스마트카드에 기저장된 공개키를 상기 제1 사용자단말(160)로 전송한다(S250).

[0035] 이후, 상기 제1 사용자단말(160)은 자신에게 부착된 스마트카드에 기저장된 비밀키와, 앞서 과정 S250을 통해 상기 제2 사용자단말(180)로부터 수신한 상기 공개키를 이용하여 상기 암호화된 권리증서암호화키를 재암호화하기 위한 재암호화키를 생성한다(S260).

[0036] 이러한 제1 사용자단말(160)은 앞서 과정 S260을 통해 생성한 재암호화키와, 암호화된 권리증서암호화키를 상기 권리발급서버(140)로 전송한다(S270).

[0037] 이에 따라, 상기 권리발급서버(140)는 상기 제1 사용자단말(160)로부터 수신한 암호화된 권리증서암호화키를 앞서 생성된 상기 재암호화키를 이용하여 재암호화한다(S280).

[0038] 이후, 상기 권리발급서버(140)는 앞서 과정 S280을 통해 재암호화한 권리증서암호화키를 콘텐츠를 공유하고자 하는 제2 사용자단말(180)에 부착된 스마트카드로 전송한다(S290).

[0039] 이어서, 상기 제2 사용자단말(180)은 상기 권리발급서버(140)로부터 수신한 재암호화한 권리증서암호화키를 자신에게 부착된 스마트카드에 기저장된 비밀키를 이용하여 복호화함으로써, 권리증서암호화키를 획득한다(S300).

[0040] 이에 따라, 상기 제1 사용자단말(160)은 패키징상태의 콘텐츠를 상기 제2 사용자단말(180)로 전송(S310)하여, 동일한 콘텐츠가 상기 제1 사용자단말과 제2 사용자단말 사이에 공유되도록 한다.

[0041] 이러한 본 발명의 DRM 시스템의 콘텐츠 공유 방법은 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0042] 본 발명의 DRM 시스템의 콘텐츠 공유방법은 사용자단말의 공개키를 통해 암호화된 권리증서암호화키를 재암호화함에 따라, 복수 개의 사용자단말이 상기 암호화된 권리증서암호화키를 복호화하고 다시 암호화하는 과정을 수행하지 않고, 재암호화과정만을 수행함으로써, 상기 복수 개의 사용자단말간에 용이하게 콘텐츠를 공유할 수 있는 효과가 있다.

[0043] 또한 본 발명의 DRM 시스템의 콘텐츠 공유방법은 콘텐츠를 공유하고자 하는 복수 개의 사용자단말간에 재암호화키 및 권리증서암호화키와 같은 그 크기가 작은 키들이 상호 공유됨에 따라, 키 분배가 빠르고 효율적으로 될 수 있는 효과가 있다.

[0044] 더불어, 본 발명의 DRM 시스템의 콘텐츠 공유방법은 권리발급서버가 공격자에 의해 공격받았다고 하더라도 암호화되지 않은 권리증서암호화키에 대한 정보를 확인할 수 없어 공격자로부터 보다 안전하게 콘텐츠를 공유할 수 있는 효과가 있다.

[0045] 이와 더불어, 본 발명의 DRM 시스템의 콘텐츠 공유방법은 복수 개의 사용자단말이 콘텐츠 공유에 사용되는 비밀키, 공개키, 권리증서암호화키 등을 탈부착가능한 외부메모리에 저장함으로써, 키 정보가 외부로 노출되지 않도록 안전하게 보호할 수 있는 효과가 있다.

[0046] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명

의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

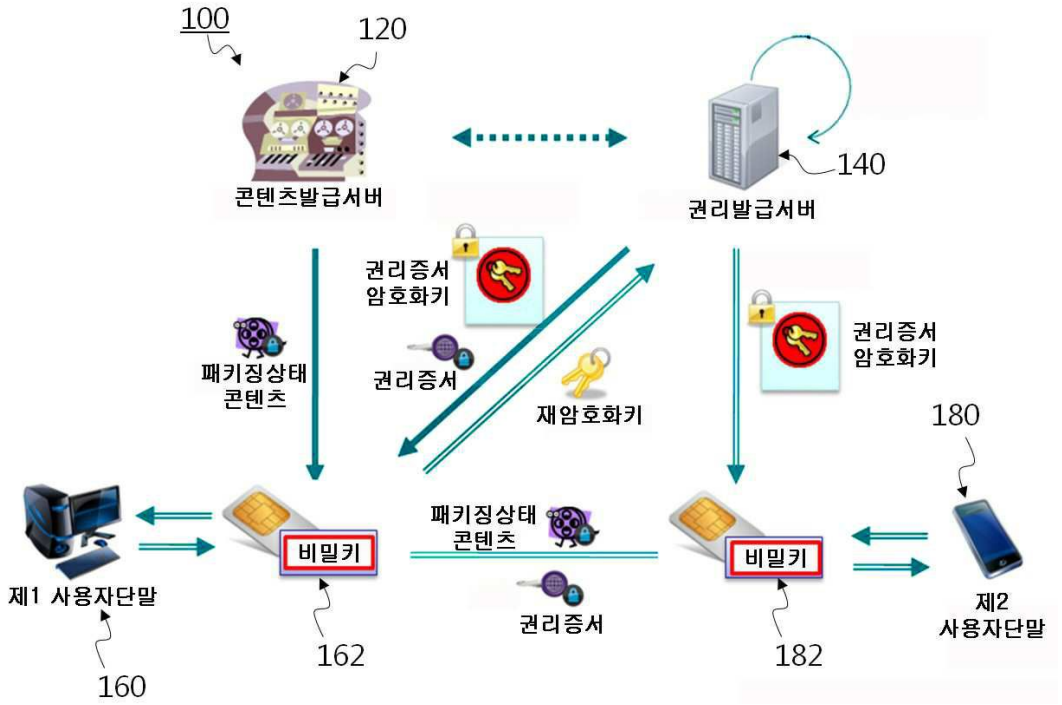
부호의 설명

[0047] 120: 콘텐츠발급서버 140: 권리발급서버

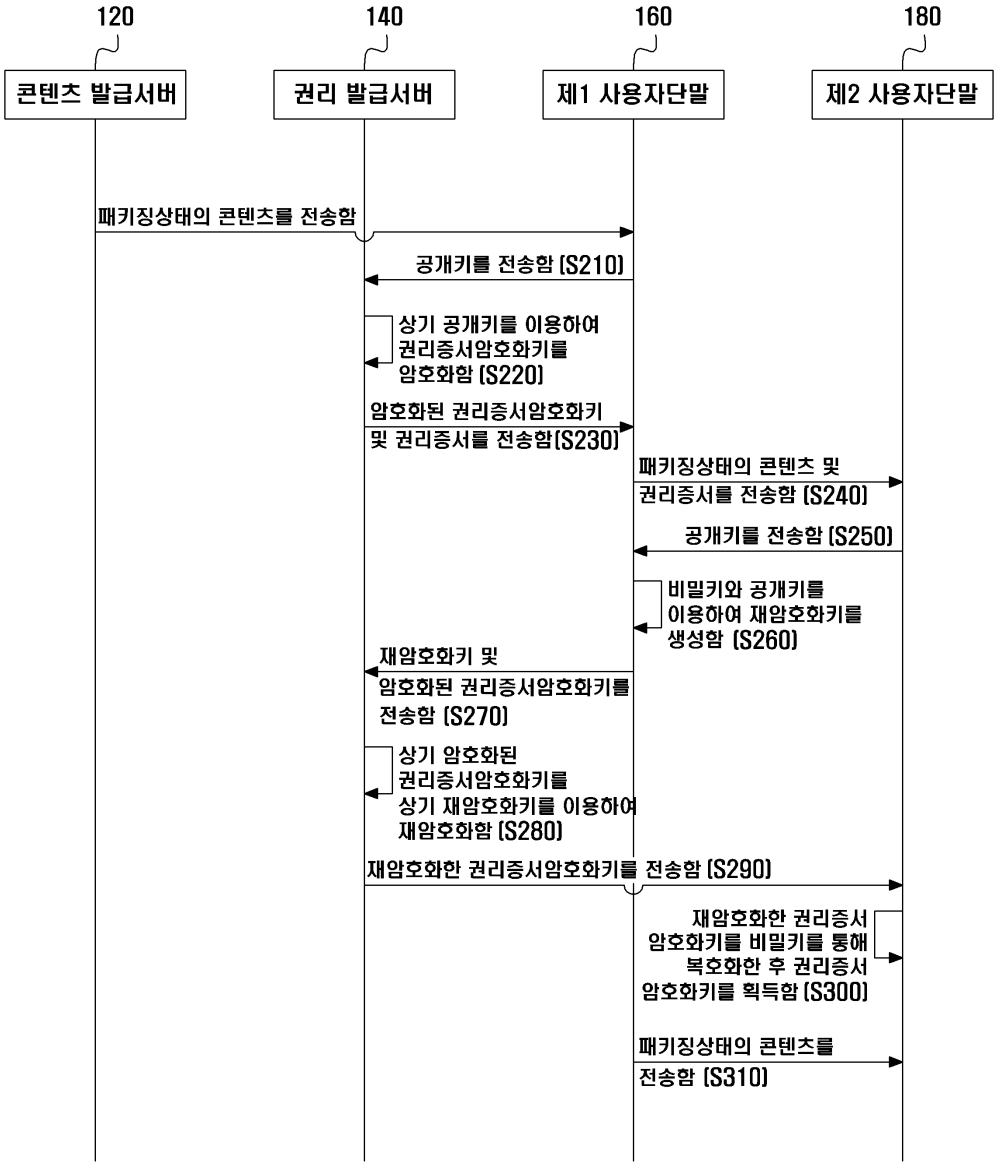
160: 제1 사용자단말 180: 제2 사용자단말

도면

도면1



도면2


120
140
160
180
콘텐츠 발급서버
권리 발급서버
제1 사용자단말
제2 사용자단말
패키징상태의 콘텐츠를 전송함
공개키를 전송함 (S210)
상기 공개키를 이용하여
권리증서암호화키를
암호화함 (S220)
암호화된 권리증서암호화키
및 권리증서를 전송함(S230)
패키징상태의 콘텐츠 및
권리증서를 전송함 (S240)
공개키를 전송함 (S250)
비밀키와 공개키를
이용하여 재암호화키를
생성함 (S260)
재암호화키 및
암호화된 권리증서암호화키를
전송함 (S270)
상기 암호화된
권리증서암호화키를
상기 재암호화키를 이용하여
재암호화함 (S280)
재암호화한 권리증서암호화키를 전송함 (S290)
재암호화한 권리증서
암호화키를 비밀키를 통해
복호화한 후 권리증서
암호화키를 획득함 (S300)
패키징상태의 콘텐츠를
전송함 (S310)