



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl.

G06F 17/00 (2006.01)

G06F 15/00 (2006.01)

(45) 공고일자

2007년07월13일

(11) 등록번호

10-0739779

(24) 등록일자

2007년07월09일

(21) 출원번호

10-2005-0128708

(22) 출원일자

2005년 12월 23일

심사청구일자

2005년 12월 23일

(65) 공개번호

10-2007-0067427

(43) 공개일자

2007년 06월 28일

(73) 특허권자

삼성전자주식회사

경기도 수원시 영통구 매탄동 416

(72) 발명자

김명선

경기 의왕시 삼동 대우아파트 105-104

윤영선

경기 수원시 권선구 권선동 상록아파트 511-704

이전남

경기 수원시 영통구 매탄동 1254-7

김봉선

경기 성남시 분당구 금곡동 청솔마을주공9단지아파트 903-411

(74) 대리인

리앤목특허법인

(56) 선행기술조사문헌

KR1020050007830 A

WO2004070612A 1

심사관 : 김정진

전체 청구항 수 : 총 24 항

(54) 디지털 콘텐츠의 관리 방법 및 이를 위한 장치

(57) 요약

본 발명은 디지털 콘텐츠에 대한 암호화 키가 누출되거나, 암호화된 디지털 콘텐츠가 크래킹(cracking)된 경우 더 이상의 디지털 콘텐츠 누출을 막을 수 있도록 디지털 콘텐츠를 관리하는 방법에 관한 것으로, 본 발명에 의하면 암호화된 디지털 콘텐츠가 정당하지 않은 디바이스에 의해 복호화된 경우, 암호화된 디지털 콘텐츠와 링크된 모듈이 구동되어 자동으로 이를 디지털 콘텐츠 관리장치에 통지하여 디지털 콘텐츠 관리장치가 암호화 키를 변경할 수 있도록 함으로써 이후의 디지털 콘텐츠에 대하여는 동일한 암호화 키의 사용에 의한 계속적인 디지털 콘텐츠 누출을 방지할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.

디지털 콘텐츠를 관리하는 방법에 있어서,

- (a) 소정 도메인의 멤버들에 의해 공유되는 제 1 도메인 키로만 복호화할 수 있도록 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하는 단계;
- (b) 상기 판단 결과 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화된 경우 제 2 도메인 키를 생성하는 단계; 및
- (c) 상기 제 2 도메인 키를 상기 도메인의 멤버들에게 통지하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2.

제 1항에 있어서,

상기 제 1 도메인 키 및 상기 제 2 도메인 키는 대칭 키임을 특징으로 하는 방법.

청구항 3.

제 1항에 있어서,

상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하는 모듈을 생성하는 단계; 및

상기 암호화된 디지털 콘텐츠가 복호화되면 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 단계를 더 포함하며,

상기 (a)단계는 상기 모듈에 의해 수행되는 것을 특징으로 하는 방법.

청구항 4.

제 3항에 있어서,

상기 모듈은 상기 도메인의 멤버들에 대한 정보를 참조하여 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하는 것을 특징으로 하는 방법.

청구항 5.

제 4항에 있어서,

상기 정보는 상기 도메인의 멤버들의 공개 키(public key)들을 포함하며,

상기 모듈은 상기 정보를 상기 암호화된 디지털 콘텐츠를 복호화한 디바이스의 공개 키와 비교하는 것을 특징으로 하는 방법.

청구항 6.

제 4항에 있어서,

상기 도메인의 멤버가 변경되는 경우 상기 정보를 업데이트하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 7.

제 1항 내지 제 6항 중 어느 한 항에 의한 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

청구항 8.

디지털 콘텐츠를 관리하는 장치에 있어서,

소정 도메인의 멤버들에 의해 공유되는 제 1 도메인 키로만 복호화할 수 있도록 상기 디지털 콘텐츠를 암호화하는 암호화부;

상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었음이 통지되면 제 2 도메인 키를 생성하는 도메인키생성부; 및

상기 제 2 도메인 키를 상기 도메인의 멤버들에게 통지하는 통지부를 포함하는 것을 특징으로 하는 장치.

청구항 9.

제 8항에 있어서,

상기 제 1 도메인 키 및 상기 제 2 도메인 키는 대칭 키임을 특징으로 하는 장치.

청구항 10.

제 8항에 있어서,

상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하는 모듈을 생성하는 모듈생성부; 및

상기 암호화된 디지털 콘텐츠가 복호화되면 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 링크부를 더 포함하는 것을 특징으로 하는 장치.

청구항 11.

제 10항에 있어서,

상기 도메인의 멤버들에 대한 정보를 생성하는 정보생성부를 더 포함하며,

상기 모듈은 상기 정보를 참조하여 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하는 것을 특징으로 하는 장치.

청구항 12.

제 11항에 있어서,

상기 정보는 상기 도메인의 멤버들의 공개 키(public key)들을 포함하며,

상기 모듈은 상기 정보와 상기 암호화된 디지털 콘텐츠를 복호화한 디바이스의 공개 키를 비교하는 것을 특징으로 하는 장치.

청구항 13.

제 11항에 있어서,

상기 도메인의 멤버가 변경되는 경우 상기 정보를 업데이트하는 정보갱신부를 더 포함하는 것을 특징으로 하는 장치.

청구항 14.

디지털 콘텐츠를 관리하는 방법에 있어서,

제 1 디바이스 고유의 복호화 키에 대응하는 암호화 키를 이용하여 상기 제 1 디바이스가 보유한 디지털 콘텐츠를 암호화하는 단계;

상기 암호화된 디지털 콘텐츠가 상기 제 1 디바이스가 아닌 제 2 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 제 1 디바이스에 통지하는 모듈을 생성하는 단계; 및

상기 암호화된 디지털 콘텐츠가 복호화되면 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 15.

제 14항에 있어서,

상기 모듈이 상기 암호화된 디지털 콘텐츠가 상기 제 2 디바이스에 의해 복호화된 것으로 판단한 경우, 상기 암호화 키를 다른 값으로 변경하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 16.

제 14항에 있어서,

상기 모듈은 상기 제 1 디바이스의 소정 특성값을 참조하여 상기 암호화된 디지털 콘텐츠가 상기 제 2 디바이스에 의해 복호화되었는지의 여부를 판단하는 것을 특징으로 하는 방법.

청구항 17.

제 16항에 있어서,

상기 특성값은 상기 제 1 디바이스의 공개 키이며,

상기 모듈은 상기 제 2 디바이스의 공개 키를 상기 특성값과 비교하는 것을 특징으로 하는 방법.

청구항 18.

제 14항 내지 제 17항 중 어느 한 항에 의한 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

청구항 19.

디지털 콘텐츠를 관리하는 장치에 있어서,

제 1 디바이스 고유의 복호화 키에 대응하는 암호화 키를 이용하여 상기 디지털 콘텐츠를 암호화하는 암호화부;

상기 암호화된 디지털 콘텐츠가 상기 제 1 디바이스가 아닌 제 2 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 제 1 디바이스에 통지하는 모듈을 생성하는 모듈생성부; 및

상기 암호화된 디지털 콘텐츠가 복호화되면 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 링크부를 포함하는 것을 특징으로 하는 장치.

청구항 20.

제 19항에 있어서,

상기 모듈이 상기 암호화된 디지털 콘텐츠가 상기 제 2 디바이스에 의해 복호화되었음을 상기 제 1 디바이스에게 통지하면, 상기 암호화 키를 다른 값으로 변경하는 키변경부를 더 포함하는 것을 특징으로 하는 장치.

청구항 21.

제 19항에 있어서,

상기 모듈은 상기 제 1 디바이스의 소정 특성값을 참조하여 상기 암호화된 디지털 콘텐츠가 상기 제 2 디바이스에 의해 복호화되었는지의 여부를 판단하는 것을 특징으로 하는 장치.

청구항 22.

제 21항에 있어서,

상기 특성값은 상기 제 1 디바이스의 공개 키이며,

상기 모듈은 상기 제 2 디바이스의 공개 키를 상기 특성값과 비교하는 것을 특징으로 하는 장치.

청구항 23.

소정 도메인의 멤버들에 의해 공유되는 도메인 키로 암호화된 디지털 콘텐츠를 관리하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체로서, 상기 방법은,

상기 암호화된 디지털 콘텐츠가 복호화되었음을 감지하는 단계;

상기 암호화된 디지털 콘텐츠를 복호화한 디바이스가 상기 도메인의 멤버인지의 여부를 판단하는 단계; 및

상기 판단 결과에 기초하여 상기 도메인이 상기 도메인의 외부에 누출되었음을 상기 도메인에 선택적으로 통지하는 단계를 포함하는 것을 특징으로 하는 기록 매체.

청구항 24.

제 1 디바이스 고유의 암호화 키로 암호화된 디지털 콘텐츠를 관리하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체로서, 상기 방법은,

상기 암호화된 디지털 콘텐츠가 복호화되었음을 감지하는 단계;

상기 암호화된 디지털 콘텐츠를 복호화한 제 2 디바이스가 상기 제 1 디바이스와 동일한지의 여부를 상기 제 1 디바이스 및 상기 제 2 디바이스의 소정 특성값을 이용하여 판단하는 단계; 및

상기 판단 결과에 기초하여 상기 암호화 키가 외부에 누출되었음을 상기 제 1 디바이스에 선택적으로 통지하는 단계를 포함하는 것을 특징으로 하는 기록 매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털 콘텐츠 관리 방법에 관한 것으로, 더욱 상세하게는 디지털 콘텐츠에 대한 암호화 키가 누출된 경우 더 이상의 디지털 콘텐츠 누출을 막을 수 있도록 디지털 콘텐츠를 관리하는 방법에 관한 것이다.

최근 들어, 인터넷, 지상파, 케이블, 위성 등의 다양한 통신 매체들을 이용한 디지털 콘텐츠의 전송이 급증하고 있고, CD (Compact Disk), DVD(Digital Versatile Disk) 등의 대용량 기록 매체들을 이용한 디지털 콘텐츠의 판매 및 대여가 급증하고 있다. 이에 따라, 디지털 콘텐츠의 저작권을 보호하기 위한 솔루션인 DRM(Digital Rights Management)이 중요한 이슈로 떠오르고 있다. 특히, 어떤 홈 도메인(domain)의 정당한 사용자가 이 홈 도메인에 속해 있는 디바이스들을 통하여 다양한 콘텐츠 서비스를 자유롭게 제공받을 수 있도록 하는 분야에 대한 연구가 활발히 진행되고 있는데, 이에 따르면 동일한 도메인에 속한 디지털TV나 PDA 등의 디바이스들은 각자 저장하고 있는 콘텐츠를 다른 디바이스들과 공유할 수 있게 된다.

그러나, 콘텐츠를 이상적으로 보호하기 위해서는, 도메인 내의 콘텐츠를 도메인에 등록된 디바이스들만 사용할 수 있고, 도메인에 등록되지 않은 디바이스는 이를 이용할 수 없도록 해야 한다. 이를 위해 일반적으로 도메인에서는 도메인에 등록된 디바이스들간 도메인 키(domain key)를 공유하게 되는데, 이하에서 자세히 설명한다.

도 1은 일반적인 도메인에서 디지털 콘텐츠를 관리하는 방법을 설명하기 위한 도면이다. 도 1에 도시된 바와 같이 도메인 X에는 디바이스A, 디바이스B 및 디바이스C가 도메인 멤버로 포함되어 있고, 도메인 관리장치는 이 디바이스들을 관리하는 역할을 한다. 외부로부터 이 도메인X로 디지털 콘텐츠 C가 유입되면, 도메인 관리장치는 소정의 암호화 키를 이용하여 디지털 콘텐츠 C를 암호화하고, 각 디바이스의 요청에 따라 해당 디바이스로 암호화된 디지털 콘텐츠 E(k,C)를 전송한다.

한편, 디바이스들은 이미 도메인 관리장치로부터 도메인 키를 분배받는데, 도메인 관리장치가 디지털 콘텐츠 C를 암호화한 암호화 키 k는 이 도메인 키에 의해서만 복호화될 수 있도록 하는 암호화 키이다. 만약 대칭 키(symmetric key)인 경우라면 도메인 키와 암호화 키 k는 동일할 것이다. 이렇게 함으로써, 디지털 콘텐츠 C는 도메인 키를 보유하고 있는 도메인 X의 멤버들끼리만 공유할 수 있다. 즉, 도메인 X에 등록되지 않은 다른 디바이스가 암호화된 디지털 콘텐츠 E(k,C)를 수신하더라도 그 디바이스는 도메인 키를 가지고 있지 않으므로 수신된 E(k,C)를 복호화할 수 없는 것이다.

그런데, 만약 도메인 키가 도메인 X의 외부로 누출된 경우, 도메인 관리장치가 이를 감지하지 못한다면 이후 도메인에 유입되는 디지털 콘텐츠가 모두 누출되는 문제가 있다. 즉, 도메인 키가 누출되었거나, 외부에서 크래킹(cracking)에 의해 E(k,C)가 복호화되었음에도 불구하고 도메인 관리 장치가 이를 알지 못한다면, 이후에 도메인 X에 유입되는 디지털 콘텐츠에 대하여도 기존의 도메인 키를 사용하여 암호화를 수행할 것이고, 이렇게 암호화된 디지털 콘텐츠는 계속 도메인 X의 외부에서 복호화될 수 있게 되어 하나의 도메인 내에서만 공유되어야 할 디지털 콘텐츠가 적절히 보호되지 못하게 된다. 또한, 이러한 문제는 도메인 뿐만 아니라 일반적으로 특정 디바이스에서만 사용하기 위한 디지털 콘텐츠를 그 디바이스 고유의 암호화 키를 이용하여 암호화하는 경우에도 발생한다.

발명이 이루고자 하는 기술적 과제

본 발명은 디지털 콘텐츠를 암호화하는데 사용된 암호화 키가 누출된 경우 이를 감지할 수 있도록 디지털 콘텐츠를 관리하는 장치 및 방법을 제공하는데 그 목적이 있다.

발명의 구성

이러한 목적을 달성하기 위한 본 발명은, 하나의 도메인에서 공유하기 위한 디지털 콘텐츠를 관리하는 방법에 있어서, (a) 상기 도메인의 멤버들에 의해 공유되는 도메인 키로만 복호화할 수 있도록 상기 디지털 콘텐츠를 암호화하는 단계; (b) 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 도메인에 통지하는 모듈을 생성하는 단계; 및 (c) 상기 암호화된 디지털 콘텐츠가 복호화되면 자동으로 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 단계를 포함한다.

여기서, 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 디바이스에 의해 복호화되었음이 통지되면, 상기 도메인 키가 아닌 다른 도메인 키를 생성하는 단계; 및 상기 생성된 도메인 키를 상기 도메인의 멤버들에게 통지하는 단계를 더 포함하는 것이 바람직하다.

또한, 본 발명은 상기 디지털 콘텐츠 관리 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

또한, 본 발명은 하나의 도메인에서 공유하기 위한 디지털 콘텐츠를 관리하는 장치에 있어서, 상기 도메인의 멤버들에 의해 공유되는 도메인 키로만 복호화할 수 있도록 상기 디지털 콘텐츠를 암호화하는 암호화부; 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 도메인에 통지하는 모듈을 생성하는 모듈생성부; 및 상기 암호화된 디지털 콘텐츠가 복호화되면 자동으로 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 링크부를 포함한다.

여기서, 상기 암호화된 디지털 콘텐츠가 상기 도메인의 멤버가 아닌 디바이스에 의해 복호화되었음이 통지되면, 상기 도메인 키가 아닌 다른 도메인 키를 생성하는 도메인키생성부; 및 상기 생성된 도메인 키를 상기 도메인의 멤버들에게 통지하는 통지부를 더 포함하는 것이 바람직하다.

또한 본 발명은, 소정의 디바이스에서 디지털 콘텐츠를 관리하는 방법에 있어서, 상기 디바이스 고유의 복호화 키에 대응하는 암호화 키를 이용하여 상기 디지털 콘텐츠를 암호화하는 단계; 상기 암호화된 디지털 콘텐츠가 상기 디바이스가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 디바이스에 통지하는 모듈을 생성하는 단계; 및 상기 암호화된 디지털 콘텐츠가 복호화되면 자동으로 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 단계를 포함한다.

또한, 본 발명은 상기 디지털 콘텐츠 관리 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

또한, 본 발명은 디지털 콘텐츠를 관리하는 디바이스에 있어서, 상기 디바이스 고유의 복호화 키에 대응하는 암호화 키를 이용하여 상기 디지털 콘텐츠를 암호화하는 암호화부; 상기 암호화된 디지털 콘텐츠가 상기 디바이스가 아닌 다른 디바이스에 의해 복호화되었는지의 여부를 판단하여 그 결과를 상기 디바이스에 통지하는 모듈을 생성하는 모듈생성부; 및 상기 암호화된 디지털 콘텐츠가 복호화되면 자동으로 상기 모듈이 구동되도록 상기 암호화된 디지털 콘텐츠를 상기 모듈과 링크시키는 링크부를 포함한다.

또한, 본 발명은 하나의 도메인 내에서 상기 도메인의 멤버들이 공유하는 도메인 키에 대응하는 암호화 키에 의해 암호화된 디지털 콘텐츠를 관리하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 있어서, 상기 암호화된 디지털 콘텐츠가 복호화되었음을 인지하는 단계; 디바이스마다 존재하는 소정 특성값을 이용하여 상기 복호화를 수행한 디바이스가 상기 도메인의 멤버인지의 여부를 판단하는 단계; 및 상기 판단 결과에 기초하여 택일적으로 상기 도메인 키가 외부로 유출되었음을 상기 도메인으로 통지하는 단계를 수행하는 프로그램을 기록한 기록 매체를 제공한다.

또한, 본 발명은 소정의 디바이스에서 상기 디바이스 고유의 복호화에 대응하는 암호화 키에 의해 암호화된 디지털 콘텐츠를 관리하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체에 있어서, 상기 암호화된 디지털 콘텐츠가 복호화되었음을 인지하는 단계; 디바이스마다 존재하는 소정 특성값을 이용하여 상기 복호화를 수행한 디바이스가 상기 디바이스와 일치하는지의 여부를 판단하는 단계; 및 상기 판단 결과에 기초하여 택일적으로 상기 복호화 키가 외부로 유출되었음을 상기 디바이스에게 통지하는 단계를 수행하는 프로그램을 기록한 기록 매체를 제공한다.

이하에서 첨부된 도면을 참조하여, 본 발명의 바람직한 실시예를 상세히 설명한다.

도 2는 본 발명의 일실시예에 따른 도메인 관리장치에서의 디지털 콘텐츠 관리 방법을 간략히 설명하기 위한 순서도이다.

우선, 본 발명의 일실시예에 따른 도메인 관리장치는 도메인의 외부로부터 디지털 콘텐츠가 유입되면, 도메인 키를 이용하여 디지털 콘텐츠를 암호화한다(210). 즉, 본 실시예에서 도메인 키는 대칭 키임을 가정하며, 따라서 도메인 키를 가지고 있는 도메인의 멤버 디바이스들은 암호화된 콘텐츠를 복호화할 수 있다.

디지털 콘텐츠를 암호화한 후에는 키누출감지모듈을 생성한다(220). 키누출감지모듈은 단계 210에서 사용한 암호화 키가 도메인 외부로 누출되어 단계 210에서 암호화된 디지털 콘텐츠가 복호화된 경우, 복호화를 수행한 디바이스가 도메인의 멤버인지를 판별하고 그 결과를 도메인 관리장치에게 통지함으로써 도메인 관리장치가 암호화 키를 변경할 수 있도록 한다. 키누출감지모듈에 대한 보다 상세한 설명은 후술한다.

키누출감지모듈이 생성되면, 도메인 관리장치는 암호화된 디지털 콘텐츠에 링크 정보를 적재하여(230) 암호화된 디지털 콘텐츠가 복호화되면 자동으로 모듈이 구동되어 복호화를 수행한 디바이스가 도메인의 멤버인지를 판단할 수 있도록 한다.

도 3은 본 발명의 일실시예에 따른 도메인 관리장치에서의 디지털 콘텐츠 관리 방법을 상세히 설명하기 위한 순서도이다.

도메인 관리장치는 도메인 키에 의해서만 복호화되도록 하는 암호화 키인 DAV를 이용하여 디지털 콘텐츠 C를 암호화한다(310). 암호화가 완료되면, 누출감지데이터 α 및 키누출감지프로그램 β 를 생성하고(320), 이들을 패키징(packaging)하여 키누출감지모듈 y를 생성한다(330). 키누출감지데이터 α 는 도메인의 멤버들에 대한 정보로서, 추후에 임의의 디바이스가 도메인의 멤버인지의 여부를 판별하는데 사용된다. 키누출감지프로그램 β 는 암호화된 디지털 콘텐츠가 복호화되면 복호화를 수행한 디바이스로부터 특성값 δ 를 추출하여 키누출감지데이터 α 와 특성값 δ 를 기초로 그 디바이스가 도메인의 멤버인지의 여부를 판별한다.

여기서, 키누출감지데이터 α 와 특성값 δ 는 특정한 종류의 데이터에 한정하지 않는다. 예를 들면, α 는 도메인에 등록된 디바이스들의 공개 키(public key)들의 집합일 수 있고, 특성값 δ 는 복호화를 수행한 디바이스의 공개 키일 수 있다. 이 경우, 키누출감지프로그램 β 는 α 에 δ 가 포함되어 있는지를 판단하게 될 것이다.

다음으로, 도메인 관리장치는 x와 y를 링크시키는데(340), x와 y를 링크시키는 것은 x에 y로 연결되는 링크 정보를 적재하여, 암호화된 디지털 콘텐츠가 복호화되면 키누출감지모듈이 자동으로 구동되도록 하는 것이다. x와 y가 링크되면, x와 y를 패키징하여 γ 를 생성하고(350), 이를 도메인의 멤버들에게 배포한다(360). 본 실시예에서는 x와 y를 패키징하여 생성된 γ 를 도메인에 배포하였지만, x와 y를 반드시 함께 배포할 필요는 없다. x는 이미 y에 링크되어 있으므로, x만 배포된 경우에도 디지털 콘텐츠가 복호화되면 키누출감지모듈 y가 구동될 것이기 때문이다.

도 4는 본 발명의 일실시예에 따른 도메인 관리장치의 구성도이다.

도 4에 도시된 바와 같이, 본 발명의 일실시예에 따른 도메인 관리장치(400)는 송수신부(410), 암호화부(420), 모듈생성부(430), 정보생성부(440), 정보갱신부(450), 데이터베이스(460), 링크부(470), 도메인키생성부(480) 및 통지부(490)를 포함한다.

송수신부(410)는 도메인 관리장치가 외부와 데이터를 주고 받을 수 있도록 하는 통신 인터페이스이다. 암호화부(420)는 송수신부(410)를 통해 도메인의 외부에서 디지털 콘텐츠가 수신되면, 도메인 키에 대응되는 암호화 키를 이용하여 암호화한다. 모듈생성부(430)는 수신된 디지털 콘텐츠에 대한 키누출감지모듈을 생성한다. 정보생성부(440)는 도메인에 등록된 디바이스들에 대한 정보인 키누출감지데이터 α 를 생성하여 데이터베이스(460)에 저장하고, 키누출감지모듈을 생성하는 모듈생성부(430)에게 α 를 제공한다. 정보갱신부(450)는 도메인의 멤버에 변경이 있을 때, 즉 디바이스가 새로 도메인에 등록하거나, 등록된 디바이스가 도메인을 탈퇴할 경우, 이를 반영하여 α 를 갱신한다.

링크부(470)는 암호화된 디지털 콘텐츠를 키누출감지모듈과 링크시키는 동작을 수행하고, 암호화된 디지털 콘텐츠를 송수신부(410)를 통해 도메인에 배포한다. 전술한 바와 같이, 링크부(470)는 암호화된 디지털 콘텐츠와 키누출감지모듈을 패키징하여 도메인에 배포할 수도 있을 것이다.

배포된 디지털 콘텐츠에 대해 모듈이 동작하여 암호화 키가 누출되었음이 알려지면, 도메인키생성부(480)는 기존의 도메인 키를 폐기하고 새로운 도메인 키를 생성하며, 통지부(490)는 송수신부(410)를 통해 새로운 도메인 키를 도메인의 멤버들에게 통지한다. 물론 이 경우, 암호화부(420)는 이후에 수신되는 디지털 콘텐츠에 대해 새로운 도메인 키에 대응되는 암호화 키를 사용하게 될 것이다.

도 5는 본 발명의 일실시예에 따른 키누출감지모듈의 동작을 설명하기 위한 순서도이다. 키누출감지모듈 y는 키누출감지 프로그램 β 와 키누출감지데이터 α 를 포함하는데, 키누출감지프로그램 β 는 링크된 디지털 콘텐츠가 복호화되었음을 감지하고(510), 복호화를 수행한 디바이스로부터 특성값 δ 를 추출한다(520). 그리고, 키누출감지데이터 α 및 디바이스의 특성값 δ 를 입력값으로 하여(530) 디바이스가 도메인의 멤버인지의 여부에 대한 결과를 출력한다(540). 만약, 디바이스가 도메인의 멤버가 아닌 것으로 판단되면, 도메인 관리장치에 암호화 키가 누출되었음을 통지한다(550). 키누출감지모듈이 이러한 과정을 수행함으로써 도메인 관리장치는 암호화 키가 누출되었는지의 여부를 알 수 있게 된다.

도 6은 본 발명의 일실시예에 따라 디지털 콘텐츠에 대한 암호화 키가 누출되었음을 감지하는 과정을 설명하기 위한 흐름도이다.

도메인 외부로부터 디지털 콘텐츠 C가 유입되면(610), 도메인 관리장치는 도메인 키에 대응되는 암호화 키 DAV로 C를 암호화한 데이터 x를 생성한다(615). 도메인 관리장치는 도메인에 등록된 디바이스 A의 요청에 의해(620) x를 디바이스 A로 전송하고(625), 디바이스 A는 임의의 경로를 통해 디바이스 B에게 x를 전송한다(630). 여기서, 디바이스 B는 디바이스 A와 동일한 도메인에 등록되지 않은 것으로 가정한다.

디바이스 B가 복호화 키 k를 사용하여 디지털 콘텐츠 C를 복호화하면, x에 포함된 링크 정보에 의해 키누출모듈이 동작한다(645). 디지털 콘텐츠 C가 복호화되었음을 감지한 키누출감지프로그램 β 는 디바이스 B의 특성값 δ 를 추출하고(650, 655), 키누출감지데이터 α 및 특성값 δ 를 이용하여 디바이스 B가 유효한 도메인의 멤버인지를 판단한다(660). 디바이스 B가 도메인의 멤버가 아니라고 판단되면(670), 키누출감지프로그램 β 는 도메인 관리장치에게 이를 통지하고, 디지털 콘텐츠 C가 도메인의 멤버가 아닌 디바이스에 의해 복호화되었음을 알게 된 도메인 관리장치는 도메인 키를 업데이트한 후(675), 업데이트된 도메인 키를 디바이스 A에게 통지한다(680). 물론 도메인 관리장치는 이후에 도메인에 배포될 디지털 콘텐츠에 대하여는 업데이트된 도메인 키에 대응하는 암호화 키를 사용할 것이다.

도 7은 본 발명의 다른 실시예에 따른 디지털 콘텐츠 관리 방법을 설명하기 위한 순서도이다. 본 실시예에서는 도메인과 관계없이 일반적인 디지털 콘텐츠 관리 장치에서 자신 이외의 디바이스에서 복호화해서는 안되는 디지털 콘텐츠를 관리하는 경우를 가정한다.

디지털 콘텐츠 관리 장치는 디바이스 키를 이용하여 디지털 콘텐츠를 암호화한다(710). 여기서, 디바이스 키는 암호화의 주체인 디바이스 고유의 암호화 키로서, 암호화하는 디바이스만이 복호화할 수 있도록 디지털 콘텐츠를 암호화하기 위해 사용된다. PKI기반을 가정하면, 개인 키(private key)는 해당 디바이스만 가지게 되므로, 이 경우 디바이스 키는 디바이스의 공개 키(public key)가 될 것이다. 물론 디바이스 키는 대칭 키일 수도 있다.

암호화가 완료되면, 앞서의 예와 같이 키누출감지모듈을 생성한다(720). 여기서의 키누출감지모듈도 역시 키누출감지데이터와 키누출감지프로그램을 포함하고 있어, 암호화된 콘텐츠를 복호화하는 디바이스의 특성값을 추출하여 정당한 디바이스인지를 판단한다. 디바이스의 특성값은 여기서 어느 하나로 특정하지 않으며, 예를 들면 디바이스의 공개 키가 될 수 있다.

키누출감지모듈이 생성되면, 디지털 콘텐츠 관리장치는 암호화된 디지털 콘텐츠에 링크 정보를 적재하여(730) 암호화된 디지털 콘텐츠가 복호화되면 자동으로 모듈이 구동되어 복호화를 수행한 디바이스가 도메인의 멤버인지를 판단할 수 있도록 한다.

도 8은 본 발명의 다른 실시예에 따라 디지털 콘텐츠를 관리하는 장치의 구성도이다. 본 실시예에서의 디지털 콘텐츠 관리장치는 도메인을 가정하지 않은 개별적인 디바이스를 가정한다.

도 8에 도시된 바와 같이, 본 발명에 따른 디지털 콘텐츠 관리장치(800)는 송수신부(810), 암호화부(820), 모듈생성부(830), 키변경부(840) 및 링크부(850)를 포함한다.

송수신부(810)는 디지털 콘텐츠 관리 장치(800)가 외부 디바이스와 데이터를 주고 받을 수 있도록 하는 통신 인터페이스이다. 암호화부(820)는 송수신부(810)를 통해 디지털 콘텐츠가 수신되면, 디바이스 키를 이용하여 수신된 디지털 콘텐츠를 암호화한다. 모듈생성부(830)는 수신된 디지털 콘텐츠에 대한 키누출감지모듈을 생성하고, 링크부(850)는 암호화된 디지털 콘텐츠를 키누출감지모듈과 링크시키는 동작을 수행한다.

암호화된 디지털 콘텐츠가 외부로 전송된 후, 키누출감지모듈이 동작하여 암호화 키가 누출되었음이 알려지면 키변경부(840)는 기존의 디바이스 키를 폐기하고 새로운 디바이스 키를 생성하며, 암호화부(820)는 이후에 수신되는 디지털 콘텐츠의 암호화시 새로운 디바이스 키를 사용하게 될 것이다.

한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 포함한다.

이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

발명의 효과

본 발명에 따르면, 디지털 콘텐츠를 암호화할 때 사용된 암호화 키가 누출되거나 크래킹(cracking)된 경우 해당 디지털 콘텐츠를 암호화한 디지털 콘텐츠 관리 장치가 암호화 키 누출 사실을 자동으로 통지받아 즉시 암호화 키를 변경할 수 있게 됨으로써, 이후의 디지털 콘텐츠에 대하여는 동일한 암호화 키의 사용에 의한 지속적인 디지털 콘텐츠 누출을 방지할 수 있다.

도면의 간단한 설명

도 1은 일반적인 도메인에서 디지털 콘텐츠를 관리하는 방법을 설명하기 위한 도면,

도 2는 본 발명의 일실시예에 따른 도메인 관리장치에서의 디지털 콘텐츠 관리 방법을 간략히 설명하기 위한 순서도,

도 3은 본 발명의 일실시예에 따른 도메인 관리장치에서의 디지털 콘텐츠 관리 방법을 상세히 설명하기 위한 순서도,

도 4는 본 발명의 일실시예에 따른 도메인 관리장치의 구성도,

도 5는 본 발명의 일실시예에 따른 키누출감지모듈의 동작을 설명하기 위한 순서도,

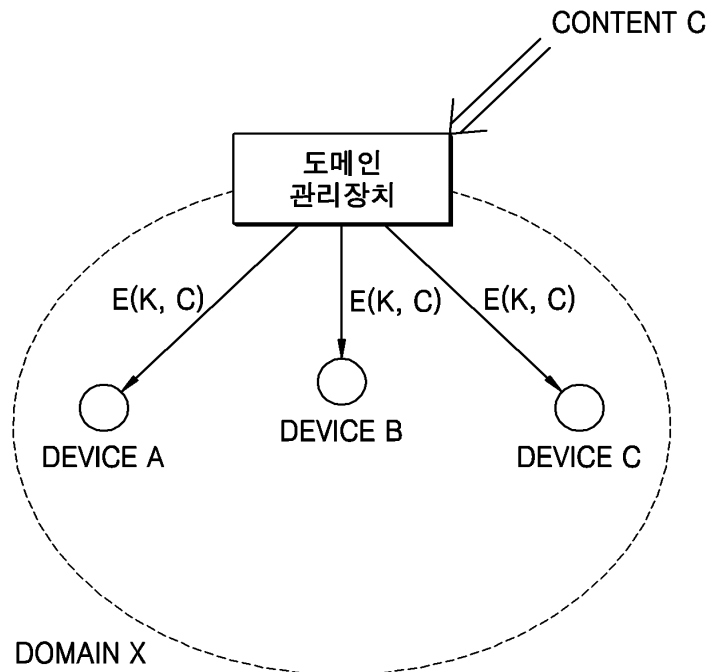
도 6은 본 발명의 일실시예에 따라 디지털 콘텐츠에 대한 암호화 키가 누출되었음을 감지하는 과정을 설명하기 위한 흐름도,

도 7은 본 발명의 다른 실시예에 따른 디지털 콘텐츠 관리 방법을 설명하기 위한 순서도,

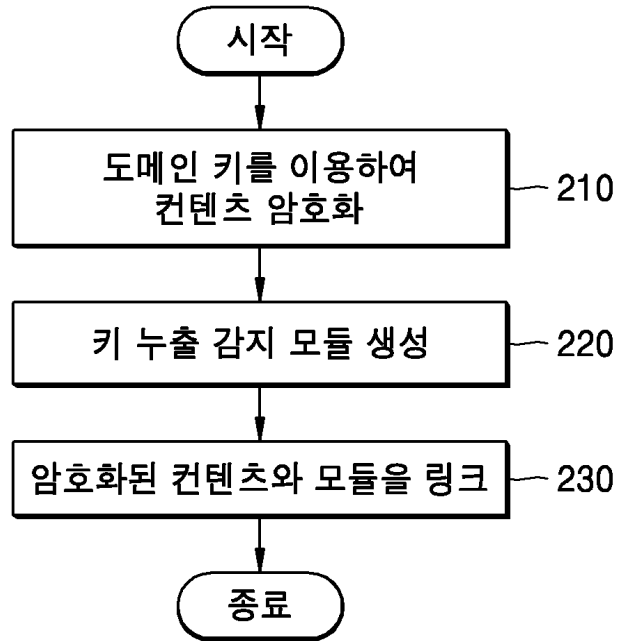
도 8은 본 발명의 다른 실시예에 따라 디지털 콘텐츠를 관리하는 장치의 구성도이다.

도면

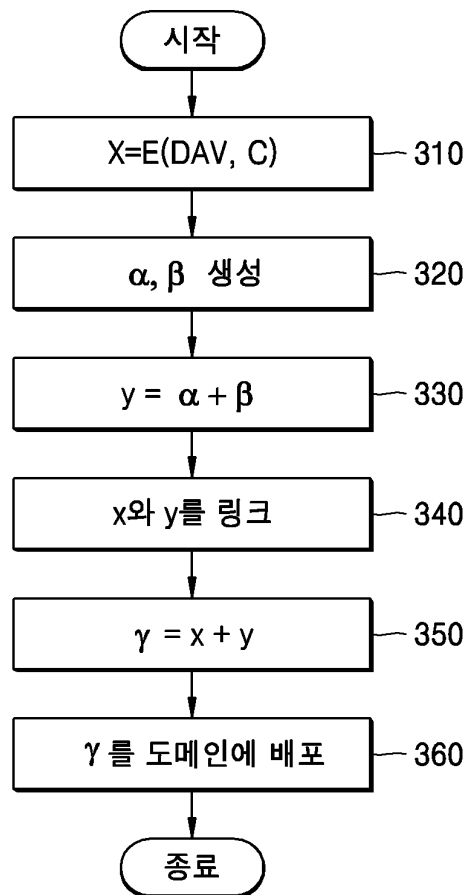
도면1



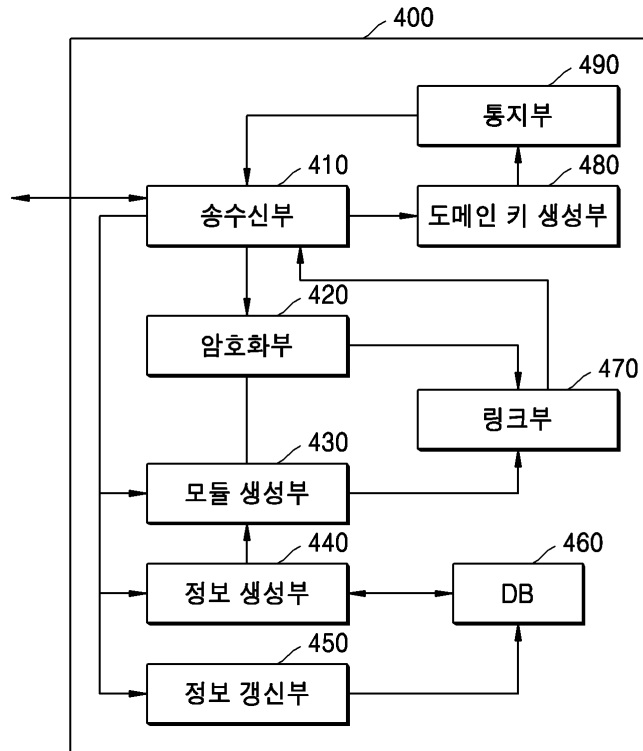
도면2



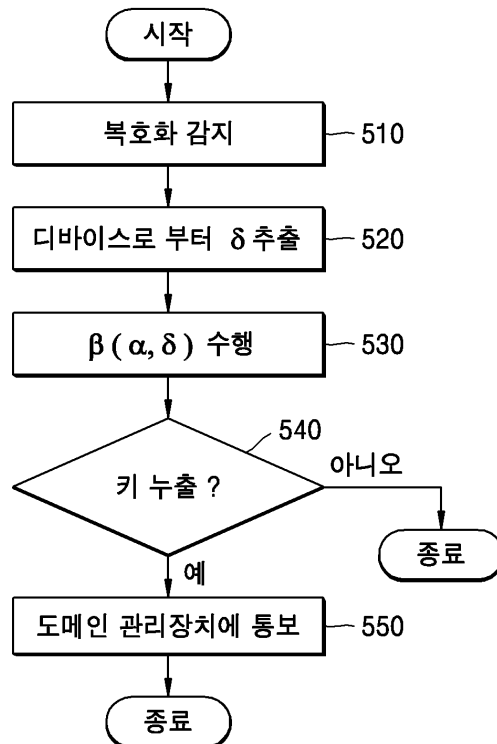
도면3



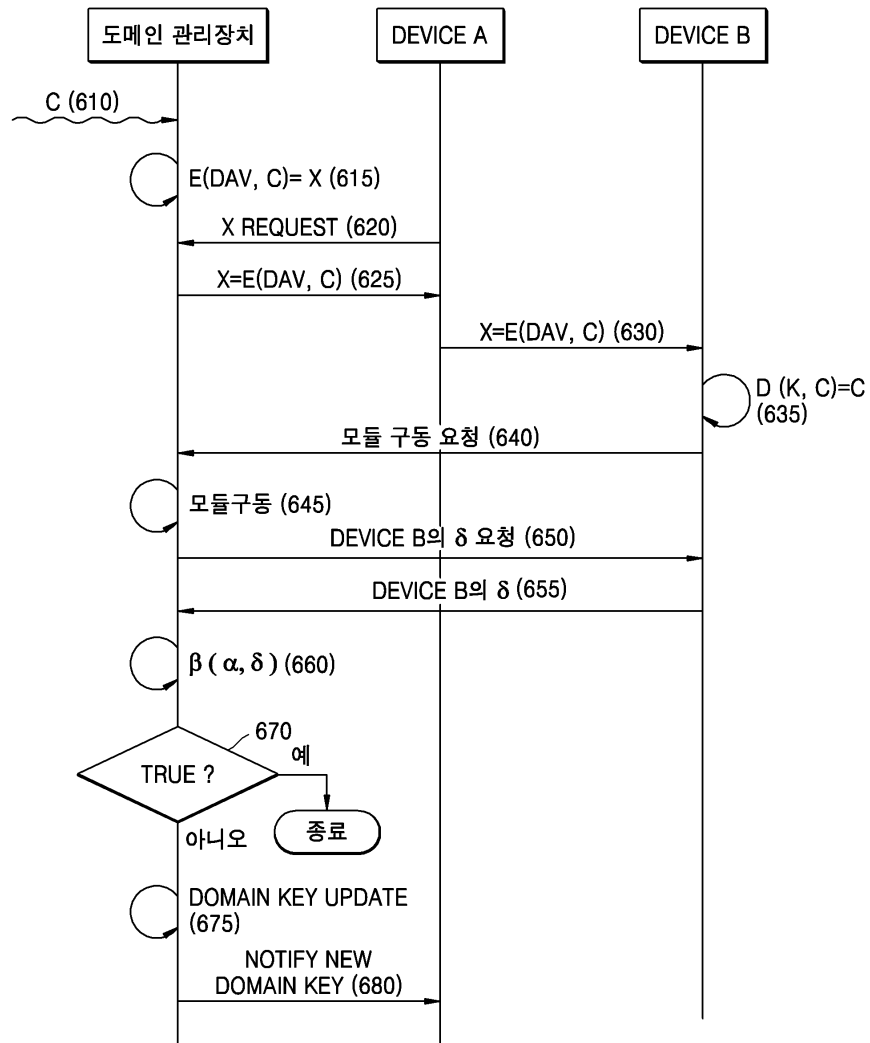
도면4



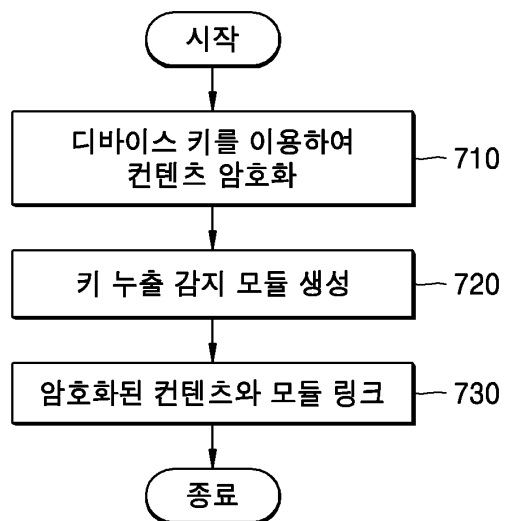
도면5



도면6



도면7



도면8

