(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월13일
(11) 등록번호 10-1424971
(24) 등록일자 2014년07월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(21) 출원번호 10-2007-0034417
(22) 출원일자 2007년04월06일
심사청구일자 2012년04월05일
(65) 공개번호 10-2008-0090935
(43) 공개일자 2008년10월09일
(56) 선행기술조사문헌
JP2006054919 A*
JP2006277420 A
JP2003085495 A
KR100645401 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
김봉선
경기도 성남시 분당구 미금로 246, 주공9단지아파트 903동 411호 (금곡동, 청솔마을)
신준범
경기도 수원시 영통구 봉영로 1526, 살구골7단지아파트 717동 104호 (영통동)
안창섭
서울특별시 서초구 방배로3길 10-3, 101동 202호 (방배동, 삼호한숲아파트)
(74) 대리인
리앤목특허법인

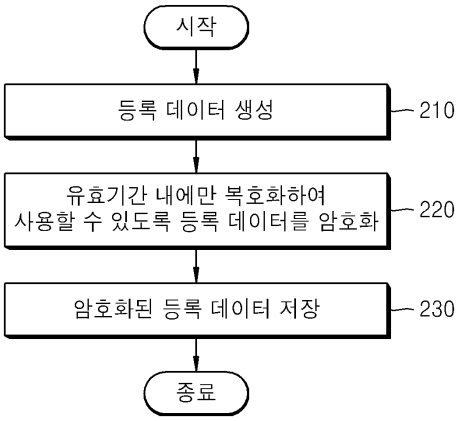
전체 청구항 수 : 총 12 항 심사관 : 양종필

(54) 발명의 명칭 **UMS 기기의 컨텐츠를 시간 정보를 이용하여 보호하는방법 및 이를 위한 장치**

(57) 요 약

본 발명은 UMS 기기에 저장된 디지털 컨텐츠가 무제한적으로 배포되는 것을 방지하는 방법에 관한 것으로, UMS 기기가 시간 정보를 이용하여 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 등록 데이터를 암호화하기 때문에, 본 발명에 따르면 암호화된 등록 데이터가 누출되더라도 정당한 권한이 없는 기기들이 UMS 기기의 등록 데이터를 저장하는 것을 어렵게 하여 UMS 기기의 컨텐츠가 무제한적으로 배포되는 것을 막을 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

UMS기기가 자신의 등록 데이터를 관리하는 방법에 있어서,

상기 등록 데이터를 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 암호화하는 단계; 및

상기 암호화된 결과를 상기 UMS 기기와 접속하는 USB 호스트가 알 수 있는 소정의 위치에 저장하는 단계를 포함하고,

상기 암호화 단계는, 현재의 시간 정보를 이용하여 소정의 알고리즘을 통해 대칭 키를 생성하는 단계; 및

상기 생성된 대칭 키를 이용하여 상기 등록 데이터를 암호화하는 단계를 포함하며,

상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 하는 방법.

청구항 2

제 1항에 있어서,

상기 암호화하는 단계에서,

상기 알고리즘은 상기 현재 시간으로부터 소정 시간 내에 속하는 시간 정보에 대해 동일하게 상기 대칭 키를 생성하는 것을 특징으로 하는 방법.

청구항 3

삭제

청구항 4

제 1항 내지 제 2항 중 어느 한 항에 의한 방법을 실행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

청구항 5

UMS기기의 등록 데이터를 관리하는 장치에 있어서,

상기 등록 데이터를 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 암호화하는 암호화부; 및

상기 암호화된 결과를 상기 UMS 기기와 접속하는 USB 호스트가 알 수 있는 소정의 위치에 저장하는 저장부를 포함하고,

상기 암호화부는 현재의 시간 정보를 이용하여 소정의 알고리즘을 통해 대칭 키를 생성하는 키생성부; 및

상기 생성된 대칭 키를 이용하여 상기 등록 데이터를 암호화하는 등록데이터암호화부를 포함하며,

상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 하는 장치.

청구항 6

제 5항에 있어서,

상기 암호화부에서,

상기 키 생성 알고리즘은 상기 현재 시간으로부터 소정 시간 내에 속하는 임의의 시간 정보에 대해 동일하게 상기 대칭 키를 생성하는 것을 특징으로 하는 장치.

청구항 7

삭제

청구항 8

USB 호스트가 UMS 기기를 등록하는 방법에 있어서,

상기 UMS 기기와 시간을 동기화하는 단계; 및

상기 UMS 기기의 암호화된 등록 데이터를 현재의 시간 정보에 기초하여 복호화함으로써 등록데이터를 선택적으로 획득하는 단계를 포함하며,

상기 획득하는 단계는,

현재의 시간 정보를 소정의 키 생성 알고리즘을 통해 가공하여 대칭 키를 생성하는 단계; 및 상기 생성된 대칭 키를 이용하여 상기 UMS 기기의 소정 위치에 저장된 상기 암호화된 등록 데이터를 복호화 하는 단계를 포함하며,

상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 하는 방법.

청구항 9

제 8항에 있어서,

상기 획득하는 단계에서,

상기 키 생성 알고리즘은 소정 기간 내에 속하는 임의의 시간 정보에 대해 동일한 키를 생성하는 것을 특징으로 하는 방법.

청구항 10

삭제

청구항 11

제 8항에 있어서,

상기 시간을 동기화하는 단계는 외부의 타임 서버로부터 수신된 시간 정보를 이용하여 수행하는 것을 특징으로 하는 방법.

청구항 12

제 8항, 9항, 및 11항 중 어느 한 항에 의한 방법을 실행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 13

UMS 기기와 시간을 동기화하는 시간동기화부; 및

상기 UMS 기기의 암호화 된 등록 데이터를 현재의 시간 정보에 기초하여 복호화함으로써 등록데이터를 선택적으로 처리하는 등록데이터처리부를 포함하며,

상기 등록데이터처리부는,

상기 현재의 시간 정보를 소정의 키 생성 알고리즘을 통해 가공하여 대칭 키를 생성하는 키생성부; 및

상기 생성된 대칭 키를 이용하여 상기 UMS 기기에 저장된, 암호화된 등록 데이터를 복호화하는 복호화부를 포함하며,

상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 하는 USB 호스트 장치.

청구항 14

제 13항에 있어서,

상기 등록데이터처리부에서,

상기 키 생성 알고리즘은 소정 기간 내에 속하는 임의의 시간 정보에 대해 동일한 키를 생성하는 것을 특징으로

하는 USB 호스트 장치.

청구항 15

삭제

청구항 16

제 13항에 있어서,

상기 시간동기화부는 외부의 타임 서버로부터 수신된 시간 정보를 이용하여 상기 UMS 기기와 시간을 동기화하는 것을 특징으로 하는 USB 호스트 장치.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0012] 본 발명은 디지털 컨텐츠의 보호 방법에 관한 것으로, 더욱 상세하게는 UMS기기에 저장된 디지털 컨텐츠가 무제한적으로 배포되는 것을 방지하는 방법에 관한 것이다.

[0013] 호스트 시스템과 연결되는 주변 기기들은 데이터를 주고 받는 통신 채널로 직렬 포트, 병렬 포트 혹은 USB(Universal Serial Bus) 포트등을 사용할 수 있으며, 이를 위해서 적절한 호스트 시스템 드라이버, 통신 프로토콜, 응용 프로그램이 설치되어야 한다. 그러나, 다양한 장치를 호스트 시스템에 연결시키기 위해서 각각의 드라이버와 관련 프로그램을 설치하는 것은 매우 비효율적이고 불편한 일이며, 일반 사용자들이 꺼리는 작업이기도 하다. 이러한 불편함을 해결하기 위하여, USB 포트의 경우에는 USB 대용량 저장장치(UMS) 클래스를 정의하였고, 윈도우XP 등의 많은 범용 운영체제 시스템에서 이를 기본적으로 제공하게 되었다. 따라서, UMS 규격을 따르는 주변 기기는 별도의 드라이버나 응용 프로그램 설치 없이도 간편하게 시스템에 연결되어 사용될 수 있다.

[0014] 디지털 컨텐츠는 무제한적으로 반복하여 복사될 수 있는 성질을 가지기 때문에, 디지털 컨텐츠를 위한 보안 기술에 대한 관심과 중요도가 점점 증대하고 있다. 호스트 시스템에 저장된 컨텐츠를 보호하기 위해서는 사용 권한을 가지는 주변 기기가 적법한 사용자 혹은 개체임을 증명할 수 있는 인증 정보를 가져야 하며, 이를 위해서는 호스트와 주변 기기가 안전하게 비밀 키를 공유하는 것이 필수적이다. 그러나, UMS 기기는 USB 호스트와 접속되면 단순한 기억장치로서 동작하기 때문에 능동적으로 보안을 위한 기능을 수행할 수 없다. 대표적인 예로, USB 이동식 하드 디스크는 USB 호스트와 접속되면 특정 파일을 암호화하거나 감추는 기능을 제공할 수 없고 단지 큰 용량을 가진 수동적인 저장 장소로만 동작할 뿐이다. 또한, PVR(Personal Video Recorder)의 경우 USB 호스트와 접속되기 전에는 능동적으로 동작할 수 있지만, USB 호스트와 접속되면 펌웨어(Firm-ware)가 종료되며 USB 호스트에게는 수동적인 UMS 기기로만 인식된다. 따라서, UMS 기기에 저장된 컨텐츠는 USB 호스트에 의해 무제한적으로 배포되어 사용되기 쉬우므로, 이를 방지하기 위한 대책이 요구된다.

발명이 이루고자 하는 기술적 과제

[0015] 본 발명은 UMS 기기의 컨텐츠를 사용할 수 있는 인증 정보인 등록 데이터를 암호화하여 보관하고, 암호화된 등록 데이터를 소정의 유효 기간 내에 복호화한 기기에 대하여만 정당한 권한을 부여함으로써 UMS 기기의 컨텐츠를 보호하는 장치 및 방법을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

[0016] 이러한 목적을 달성하기 위한 본 발명은, UMS기기가 자신의 등록 데이터를 관리하는 방법에 있어서, 상기 등록 데이터를 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 암호화하는 단계; 및 상기 암호화된 결과를 상기 UMS 기기와 접속하는 USB 호스트가 알 수 있는 소정의 위치에 저장하는 단계를 포함하며, 상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 한다.

[0017] 상기 암호화하는 단계는, 현재의 시간 정보를 이용하여 소정의 알고리즘을 통해 대칭 키를 생성하는 단계; 및 상기 생성된 대칭 키를 이용하여 상기 등록 데이터를 암호화하는 단계를 포함하며, 상기 알고리즘은 상기 현재

시간으로부터 소정 시간 내에 속하는 시간 정보에 대해 동일하게 상기 대칭 키를 생성하는 것이 바람직하다.

[0018] 한편, 상기 암호화하는 단계는, 소정의 USB 호스트와 공유하는 공유 키를 이용하여 상기 현재의 시간 정보 및 상기 등록 데이터를 암호화할 수도 있다.

[0019] 또한, 본 발명은 상기 등록 데이터 관리 방법을 실행하는 프로그램을 기록한 기록 매체를 제공한다.

[0020] 또한, 본 발명은 UMS기기의 등록 데이터를 관리하는 장치에 있어서, 상기 등록 데이터를 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 암호화하는 암호화부; 및 상기 암호화된 결과를 상기 UMS 기기와 접속하는 USB 호스트가 알 수 있는 소정의 위치에 저장하는 저장부를 포함하며, 상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 한다.

[0021] 또한, 본 발명은 USB 호스트가 UMS 기기를 등록하는 방법에 있어서, 상기 UMS 기기와 시간을 동기화하는 단계; 및 상기 UMS 기기의 등록 데이터를 현재의 시간 정보에 기초하여 선택적으로 획득하는 단계를 포함하며, 상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 한다.

[0022] 상기 획득하는 단계는, 현재의 시간 정보를 소정의 키 생성 알고리즘을 통해 가공하여 대칭 키를 생성하는 단계; 및 상기 생성된 대칭 키를 이용하여 상기 UMS 기기의 소정 위치에 저장된 암호화된 등록 데이터를 복호화하는 단계를 포함하며, 상기 키 생성 알고리즘은 소정 기간 내에 속하는 임의의 시간 정보에 대해 동일한 키를 생성하는 것이 바람직하다.

[0023] 한편, 상기 획득하는 단계는, 상기 UMS 기기와 공유하는 소정의 공유 키를 이용하여 상기 UMS 기기의 소정 위치에 암호화되어 저장된, 상기 등록 데이터 및 시간 정보를 복호화하는 단계; 및 상기 복호화된 시간 정보를 현재의 시간 정보와 비교하여, 비교 결과 상기 현재의 시간 정보에 의한 시간이 상기 복호화된 시간 정보로부터 소정의 유효 기간 내에 속하는 경우에만 상기 복호화된 등록 데이터를 저장하고, 그렇지 않은 경우 상기 복호화된 등록 데이터를 폐기하는 단계를 포함할 수도 있다.

[0024] 상기 시간을 동기화하는 단계는 외부의 타임 서버로부터 수신된 시간 정보를 이용하여 수행하는 것이 바람직하다.

[0025] 또한, 본 발명은 상기 UMS 기기 등록 방법을 실행하는 프로그램을 기록한 기록 매체를 제공한다.

[0026] 또한, 본 발명은 UMS 기기와 시간을 동기화하는 시간동기화부; 및 상기 UMS 기기의 등록 데이터를 현재의 시간 정보에 기초하여 선택적으로 처리하는 등록데이터처리부를 포함하며, 상기 등록 데이터는 상기 UMS기기의 암호화된 컨텐츠를 사용하기 위해 필요한 정보임을 특징으로 한다.

[0027] 이하에서 첨부된 도면을 참조하여, 본 발명의 바람직한 실시예를 상세히 설명한다.

[0028] 도 1은 본 발명이 적용되는 환경을 도시한 블록도이다. 도 1에 도시된 바와 같이, UMS 기기와 USB 호스트는 USB 포트를 통해 서로 접속된다. UMS 기기는 자신이 보유한 컨텐츠를 암호화하여 저장하고, 미리 정해진 위치에 등록 데이터를 보관한다. 등록 데이터는 UMS 기기의 암호화된 컨텐츠를 정당하게 사용하기 위해 필요한 인증 정보인데, UMS 기기에 USB 호스트가 접속되기 전, 즉 UMS 기기가 능동적인 동작을 할 수 있을 때 사용자의 요청에 의해 미리 생성하여 미리 정해진 위치에 저장한다.

[0029] 예를 들어, UMS 기기가 컨텐츠 키를 이용하여 자신이 보유한 컨텐츠를 암호화한 후 저장하고, 컨텐츠 키를 자신의 디바이스 키로 암호화하는 경우, USB 호스트는 UMS 기기의 디바이스 키를 가지면 컨텐츠 키를 얻을 수 있으므로, UMS 기기의 모든 컨텐츠를 자유롭게 이용할 수 있다. 따라서, 이 경우 UMS 기기의 디바이스 키가 등록 데이터가 될 수 있다.

[0030] 등록 데이터를 가진 기기, 즉 UMS 기기를 등록한 기기는 등록된 UMS 기기의 컨텐츠를 자유롭게 이용할 수 있게 되므로, 등록 데이터는 암호화하여 보관하는 것이 바람직하다. USB 호스트는 암호화된 등록 데이터의 복호화에 성공하면 안전한 장소에 보관한다. 그러나, USB 호스트가 UMS 기기로부터 암호화된 등록 데이터를 가져오는 과정에서 USB 채널을 통해 암호화된 등록 데이터가 누출된 경우, 정당한 권한이 없는 자가 암호화된 등록 데이터를 크래킹하여 등록 데이터를 획득하게 되면 UMS 기기의 컨텐츠가 무제한 배포되는 것을 막기 힘들다.

[0031] 따라서, 본 발명은 등록 데이터를 효과적으로 암호화하여, 암호화된 등록 데이터가 누출되더라도 권한 없는 기기들이 UMS 기기를 무제한 등록하는 것을 막을 수 있도록 한 것이다.

[0032] 도 2는 본 발명의 일실시예에 따른 등록 데이터 관리 방법을 설명하기 위한 순서도이다.

[0033] 단계 210에서, UMS 기기는 사용자의 요청에 따라 등록 데이터를 생성한다. 즉, 사용자는 UMS 기기를 USB 호스트에 등록하고자 하는 경우 UMS 기기의 사용자 인터페이스를 통해 등록 데이터 생성을 요청한다.

[0034] 단계 220에서, UMS 기기는 소정의 유효 기간 내에만 복호화할 수 있도록 등록 데이터를 암호화한다. 즉, 암호화하는 시점에서의 현재 시간 정보를 이용하여 현재 시간을 기준으로 소정 시간 내에만 복호화가 가능하도록 등록 데이터를 암호화한다. 보다 자세한 설명은 도 3 및 도 4에서 후술한다.

[0035] 단계 230에서, UMS 기기는 암호화된 등록 데이터를 미리 정해진 장소, 즉 USB 호스트가 등록 데이터를 읽기 위해 액세스하는 위치에 저장한다.

[0036] 이와 같은 일련의 과정을 통해 등록 데이터를 암호화하여 저장하면, 암호화된 등록 데이터가 암호화된 등록 데이터를 얻게 되더라도 유효 기간이 지난 후에 복호화하면 해당 UMS 기기를 등록할 수 없으므로 UMS 기기를 등록할 수 없게 된다. 따라서, 권한 없는 기기들이 무제한적으로 UMS 기기를 등록하는 것을 막을 수 있다.

[0037] 도 3은 본 발명의 일실시예에 따른 등록 데이터 암호화 방법을 나타낸 순서도이다.

[0038] 단계 310에서는, 현재의 시간 정보를 이용하여 대칭 키를 생성한다. 즉, 현재의 시간 정보를 키 생성 알고리즘의 파라미터로 하여 대칭 키를 생성하는데, 이 때 사용되는 키 생성 알고리즘은 소정의 유효 기간 내에 속하는 임의의 시간 정보를 파라미터로 하여도 모두 동일한 대칭 키를 생성한다. 이러한 키 생성 알고리즘은 다양하게 구현할 수 있으므로 특정 알고리즘으로 한정하지 않는다.

[0039] 단계 320에서는, 생성된 대칭 키를 이용하여 등록 데이터를 암호화한다.

[0040] 이와 같은 과정들을 통해 등록 데이터를 암호화하고, 암호화된 등록 데이터를 복호화하는 기기가 복호화를 위한 대칭 키를 생성해내기 위해 복호화시의 현재 시간을 사용하도록 강제하면, 유효 기간 내에만 암호화된 등록 데이터를 복호화할 수 있게 된다. 이러한 강제성은 UMS 기기와 함께 제공되는 UMS 기기 등록용 소프트웨어 등을 통해 구현할 수 있을 것이다.

[0041] 도 4는 본 발명의 다른 실시예에 따른 등록 데이터 암호화 방법을 나타낸 순서도이다.

[0042] 단계 410에서는, USB 호스트와 공유하는 공유 키를 이용하여 등록 데이터 및 현재 시간 정보를 함께 암호화한다.

[0043] 단계 420에서는, 암호화된 결과를 미리 정해진 위치, 즉 등록 데이터를 위한 저장 위치에 저장한다.

[0044] 본 실시예에 따라 암호화한 경우, 유효 기간과 관계 없이 공유 키를 가지고 있는 모든 기기는 암호화된 등록 데이터를 복호화할 수 있다. 그러나, 복호화를 수행한 기기가 복호화 결과 얻은 시간 정보를 복호화 당시의 현재 시간 정보와 비교하여 유효 기간이 지난 것으로 판단되면 등록 데이터를 저장하지 않도록 강제하면 본 발명의 목적은 달성될 수 있다. 이러한 강제성은 UMS 기기와 함께 제공되는 UMS 기기 등록용 소프트웨어 등을 통해 구현할 수 있을 것이다.

[0045] 도 5는 본 발명의 일실시예에 따른 UMS 기기의 구조를 나타낸 도면이다.

[0046] 도 5에 도시된 바와 같이, 본 발명의 일실시예에 따른 UMS 기기(500)는 암호화부(510), 클록(520) 및 저장부(530)를 포함한다.

[0047] 암호화부(510)는 UMS 기기(500)의 등록 데이터를 소정의 유효 기간 내에만 복호화하여 사용할 수 있도록 암호화하는데, 키생성부(511) 및 등록 데이터 암호화부(512)를 포함한다. 클록(520)은 암호화부(510)에게 시간 정보를 제공하며, USB 호스트(540)와의 시간 동기화를 위해 원격의 타임 서버(도시하지 않음)로부터 시간 정보를 얻을 수 있다.

[0048] 키 생성부(511)는 클록(520)이 제공하는 시간 정보를 파라미터로 하여 대칭 키를 생성한다. 등록 데이터 암호화부(511)는 키 생성부(511)에 의해 생성된 대칭 키를 이용하여 등록 데이터를 암호화한다.

[0049] 저장부(530)는 암호화된 등록 데이터를 미리 정해진 위치에 저장한다. USB 호스트(540)는 저장부(530)로부터 암호화된 등록 데이터를 획득할 수 있다.

[0050] 도 6은 본 발명의 다른 실시예에 따른 UMS 기기의 구조를 나타낸 도면이다. 도 5에서와 동일한 명칭의 블록들에 대한 설명은 생략한다. 다만, 본 실시예에서는 암호화부(621)가 암호화할 당시의 현재 시간 정보를 파라미터로 사용하여 대칭 키를 생성하는 것이 아니라 USB 호스트(630)와 공유하는 공유 키를 이용하여 등록 데이터 및 암

호화할 당시의 현재 시간 정보를 함께 암호화한다.

[0051] 도 7은 본 발명의 일실시예에 따라 USB 호스트가 UMS 기기를 등록하는 과정을 나타낸 순서도이다.

[0052] 단계 710에서, 등록하려는 UMS 기기와 시간을 동기화한다. 이 때, 원격에서 공인된 시간 정보를 제공하는 외부의 타임 서버가 이용될 수 있다.

[0053] 단계 720에서, USB 호스트는 UMS 기기의 등록 데이터를 현재의 시간 정보에 기초하여 선택적으로 처리한다. 즉, 현재 시간에 따라 UMS 기기를 등록할지의 여부를 결정한다. 이에 대한 상세한 설명은 이하에서 후술한다.

[0054] 도 8은 본 발명의 일실시예에 따라 USB 호스트가 암호화된 등록 데이터를 처리하는 과정을 나타낸 순서도이다.

[0055] 본 실시예는 도 3에 의한 암호화 방법에 의해 암호화된 등록 데이터를 처리하는 과정이다.

[0056] 단계 810에서, USB 호스트는 현재 시간 정보를 이용하여 소정의 키 생성 알고리즘에 따라 대칭 키를 생성한다. 이 때 사용되는 키 생성 알고리즘은 도 3에서 사용된 키 생성 알고리즘과 동일한 것이다. 즉, 소정의 유효 기간 내에 속하는 임의의 시간 정보를 파라미터로 하면 모두 동일한 대칭 키가 생성된다.

[0057] 단계 820 및 단계 830에서, 생성된 대칭 키를 이용하여 암호화된 등록 데이터를 복호화한다.

[0058] 만약 복호화 당시, 정확히 말하면 대칭 키를 생성하는 당시의 현재 시간이 유효 기간 내라면 복호화는 성공할 것이고, 그렇지 않다면 복호화에 실패할 것이다.

[0059] 단계 840에서, 복호화에 성공한 경우 복호화 결과 얻어진 등록 데이터를 한전한 곳에 저장함으로써 등록 절차가 완료된다. 즉, 등록 데이터를 저장한 USB 호스트는 등록된 UMS 기기의 컨텐츠를 자유롭게 이용할 수 있다.

[0060] 도 9는 본 발명의 다른 실시예에 따라 USB 호스트가 암호화된 등록 데이터를 처리하는 과정을 나타낸 순서도이다.

[0061] 본 실시예는 도 4에 의한 암호화 방법에 의해 암호화된 등록 데이터를 처리하는 과정이다.

[0062] 단계 910에서, USB 호스트는 UMS 기기와 공유하는 공유 키를 이용하여 암호화된 데이터를 복호화한다. 이 때의 데이터는 UMS 기기에서 등록 데이터가 저장되는 공간에 위치한 데이터이다.

[0063] 단계 920에서, 복호화의 결과 등록 데이터 및 시간 정보를 획득한다. 이 때 획득한 시간 정보는 암호화 당시의 시간을 나타낸다.

[0064] 단계 930에서, 획득한 시간 정보를 현재의 시간 정보와 비교하여 현재 시간이 유효 기간 내인지를 판단한다. 유효 기간의 길이는 UMS 기기 등록용 소프트웨어 등에서 미리 설정될 수 있다.

[0065] 단계 940에서, 만약 복호화할 때의 현재 시간이 유효 기간 내이면, 등록 데이터를 안전한 곳에 저장하여 등록 절차를 완료한다. 즉, 등록 데이터를 저장한 USB 호스트는 등록된 UMS 기기의 컨텐츠를 향후 자유롭게 이용할 수 있게 된다.

[0066] 단계 950에서, 만약 복호화할 때의 현재 시간이 유효 기간을 지났으면, 등록 데이터를 폐기한다. 즉, 복호화 자체는 성공하였으나, 등록 데이터를 저장하지 않고 폐기하므로 UMS 기기를 등록하지 못한다.

[0067] 도 10은 본 발명의 일실시예에 따른 USB 호스트의 구조를 나타낸 도면이다.

[0068] 본 실시예에 의한 USB 호스트(1000)는 도 3에 의한 방법으로 암호화된 등록 데이터를 복호화하기 위한 구조를 가진다.

[0069] 도 10에 도시된 바와 같이, 본 발명의 일실시예에 따른 USB 호스트(1000)는 시간 동기화부(1030), 클록(1040), 등록 데이터 처리부(1050) 및 저장부(1060)를 포함한다.

[0070] 시간 동기화부(1030)는 UMS 기기와 시간을 동기화하기 위한 수단이다. 이를 위해, 인터넷 등의 네트워크를 통해 원격의 타임 서버(1010)로부터 시간 정보를 수신하는 것이 바람직하다.

[0071] 클록(1040)은 시간 동기화부(1030)로부터 시간 정보를 수신하여 등록 데이터 처리부(1050)에게 시간 정보를 제공한다.

[0072] 등록 데이터 처리부(1050)는 UMS 기기(1020)의 등록 데이터를 복호화를 수행할 때의 시간 정보를 이용하여 복호화하는데, 복호화부(1051) 및 키 생성부(1052)를 포함한다. 키 생성부(1052)는 복호화를 수행할 때의 시간 정보를 클록(1040)으로부터 가져와서, 그 시간 정보를 파라미터로 하여 대칭 키를 생성한다. 이 때 사용되는 키 생

성 알고리즘은 도 3에서 사용된 키 생성 알고리즘과 동일한 것이다. 즉, 이러한 키 알고리즘에 의할 때, 유효 기간 내에 속하는 임의의 시간 정보를 파라미터로 하면 모두 동일한 대칭 키가 생성된다.

[0073] 복호화부(1051)는 UMS 기기(1020)의 암호화된 등록 데이터를 키 생성부(1052)가 생성한 대칭 키를 이용하여 복호화한다. 전술한 바와 같이, 복호화부(1051)가 복호화를 수행할 때의 시각이 유효 기간 내인 경우에만 복호화는 성공할 것이다.

[0074] 저장부(1060)는 복호화가 성공한 경우, 등록 데이터를 저장한다. 저장된 등록 데이터는 향후 USB 호스트(1000)가 UMS 기기(1020)의 암호화된 컨텐츠를 사용할 때 이용될 것이다.

[0075] 도 11은 본 발명의 다른 실시예에 따른 USB 호스트의 구조를 나타낸 도면이다.

[0076] 본 실시예에 의한 USB 호스트(1100)는 도 4에 의한 방법으로 암호화된 등록 데이터를 복호화하기 위한 구조를 가진다.

[0077] 도 11에 도시된 바와 같이, 본 발명의 일실시예에 따른 USB 호스트(1100)는 시간 동기화부(1130), 클록(1140), 등록 데이터 처리부(1150) 및 저장부(1160)를 포함한다.

[0078] 시간 동기화부(1030)는 UMS 기기와 시간을 동기화하기 위한 수단이다. 이를 위해, 인터넷 등의 네트워크를 통해 원격의 타임 서버(1010)로부터 시간 정보를 수신하는 것이 바람직하다.

[0079] 클록(1140)은 시간 동기화부(1130)로부터 시간 정보를 수신하여 등록 데이터 처리부(1150)에게 시간 정보를 제공한다.

[0080] 등록 데이터 처리부(1150)는 UMS 기기(1120)의 등록 데이터를 복호화를 수행할 때의 시간 정보에 따라 선택적으로 처리하는데, 복호화부(1151) 및 비교부(1152)를 포함한다.

[0081] 복호화부(1151)는 UMS 기기(1120)와 USB 호스트(1100)가 미리 공유하는 공유 키를 이용하여 UMS 기기(1120)의 암호화된 데이터를 복호화한다. 이 때 암호화된 데이터란 UMS 기기(1120)의 등록 데이터가 저장되는 위치에 있는 데이터를 말한다. 복호화가 수행된 결과 등록 데이터와 시간 정보가 얻어지는데, 이 때의 시간 정보는 UMS 기기(1120)로부터 가져온 데이터가 암호화된 시각을 나타낸다.

[0082] 비교부(1152)는 클록(1140)으로부터 현재 시간 정보를 얻어와서 복호화 결과 얻어진 시간 정보와 비교하여 복호화가 수행되는 현재 시각이 유효 기간 내인지의 여부를 판단한다. 전술한 바와 같이, 유효 기간의 길이는 UMS 기기 등록용 소프트웨어 등을 통해 미리 설정될 수 있을 것이다.

[0083] 복호화가 수행된 시각이 유효 기간 내인 경우, 등록 데이터는 저장부(1160)에 저장되어 등록 절차가 완료된다. 만약, 복호화가 수행된 시각이 유효 기간을 도과하였으면, 복호화 결과 얻어진 등록 데이터는 저장되지 않고 폐기된다.

[0084] 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.

[0085] 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.

[0086] 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

[0087] 본 발명에 따르면, 암호화된 등록 데이터가 누출되더라도 UMS 기기를 등록하기 위해서는 유효 기간 내에 암호화된 등록 데이터를 복호화해야 하므로, UMS 기기의 컨텐츠가 권한 없는 기기들에 의해 무제한적으로 배포되는 것을 막을 수 있다.

도면의 간단한 설명

[0001] 도 1은 본 발명이 적용되는 환경을 도시한 블록도,

[0002] 도 2는 본 발명의 일실시예에 따른 등록 데이터 관리 방법을 설명하기 위한 순서도,

[0003] 도 3은 본 발명의 일실시예에 따른 등록 데이터 암호화 방법을 나타낸 순서도,

[0004] 도 4는 본 발명의 다른 실시예에 따른 등록 데이터 암호화 방법을 나타낸 순서도,

[0005] 도 5는 본 발명의 일실시예에 따른 UMS 기기의 구조를 나타낸 도면,

[0006] 도 6은 본 발명의 다른 실시예에 따른 UMS 기기의 구조를 나타낸 도면,

[0007] 도 7은 본 발명의 일실시예에 따라 USB 호스트가 UMS 기기를 등록하는 과정을 나타낸 순서도,

[0008] 도 8은 본 발명의 일실시예에 따라 USB 호스트가 암호화된 등록 데이터를 처리하는 과정을 나타낸 순서도,

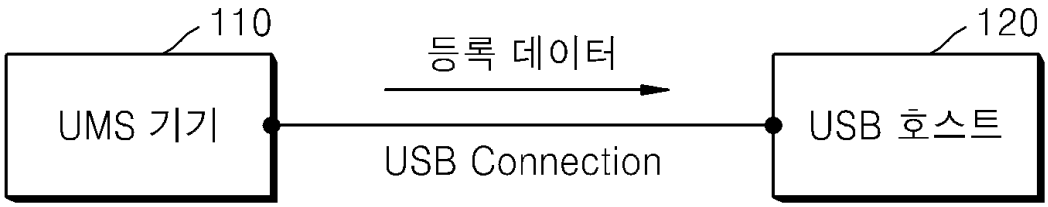
[0009] 도 9는 본 발명의 다른 실시예에 따라 USB 호스트가 암호화된 등록 데이터를 처리하는 과정을 나타낸 순서도,

[0010] 도 10은 본 발명의 일실시예에 따른 USB 호스트의 구조를 나타낸 도면,

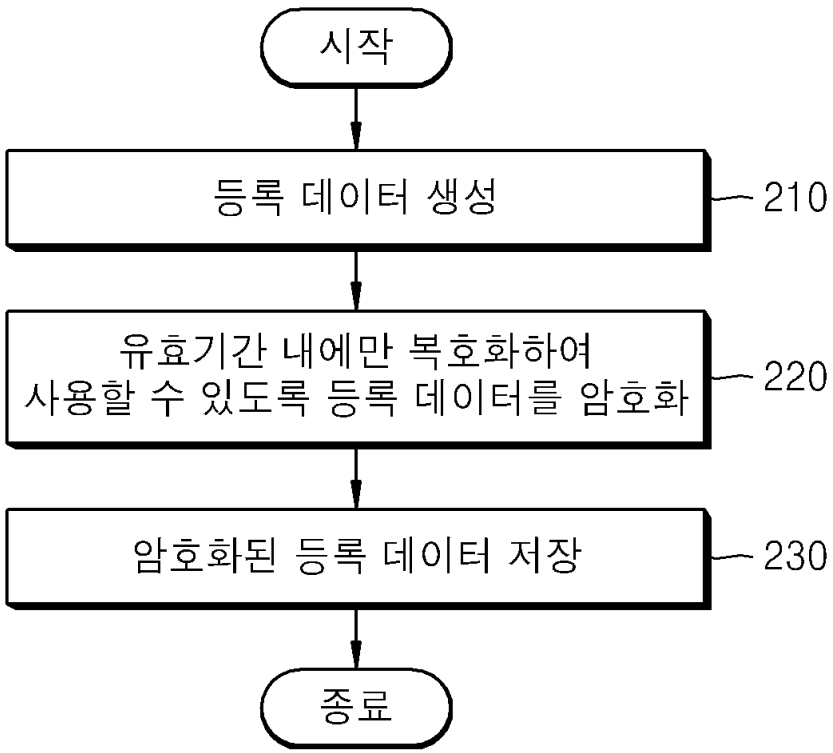
[0011] 도 11은 본 발명의 다른 실시예에 따른 USB 호스트의 구조를 나타낸 도면이다.

도면

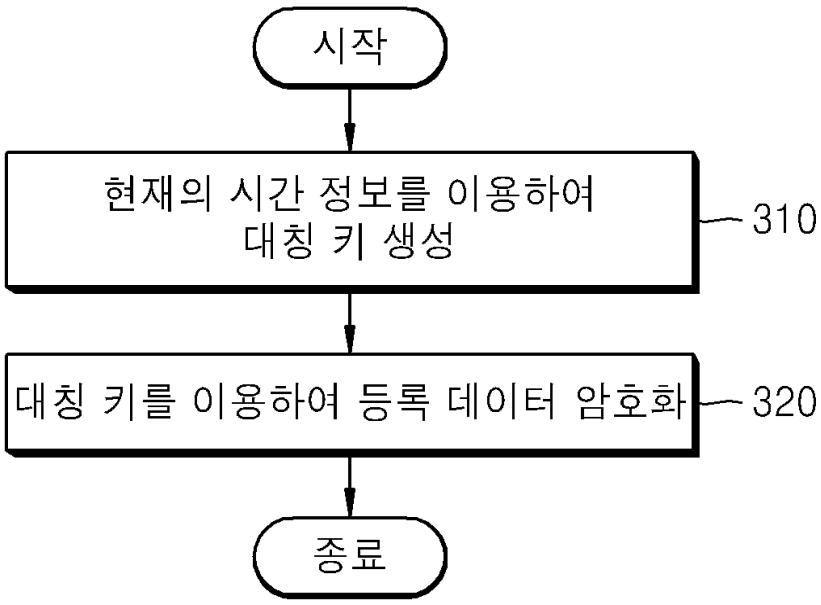
도면1



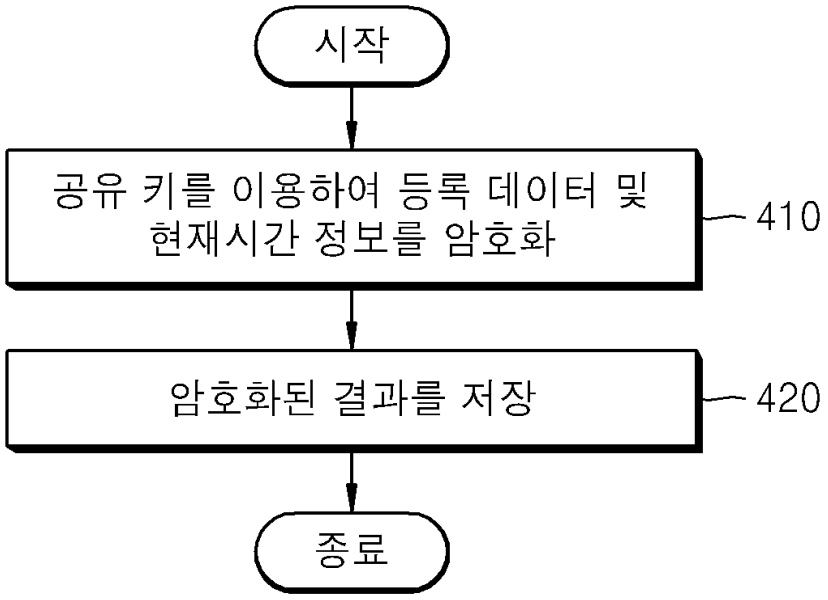
도면2



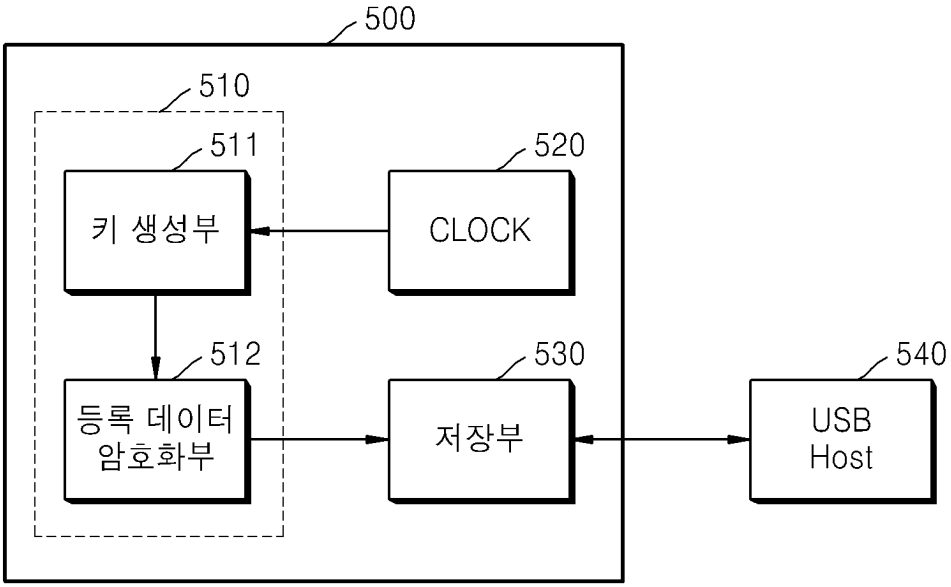
도면3


시작
현재의 시간 정보를 이용하여
대칭 키 생성
310
대칭 키를 이용하여 등록 데이터 암호화
320
종료

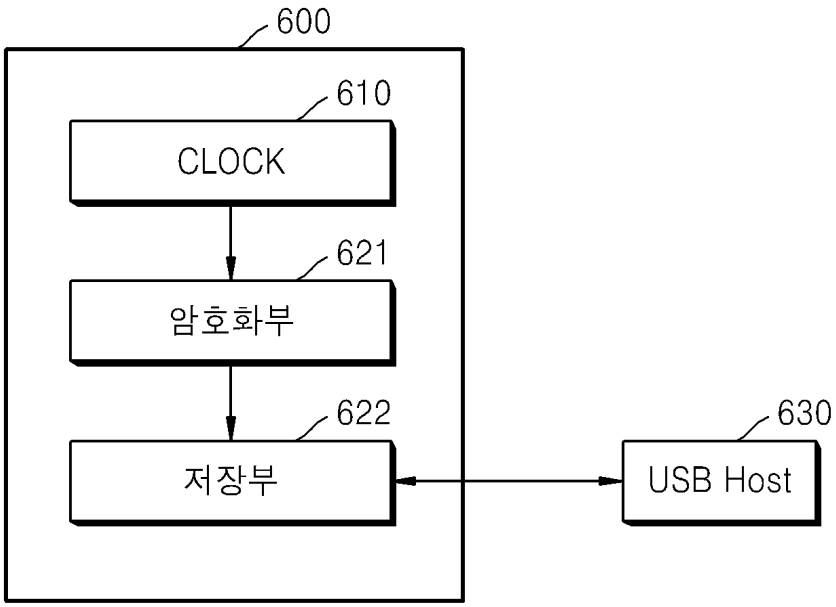
도면4


시작
공유 키를 이용하여 등록 데이터 및
현재시간 정보를 암호화
410
암호화된 결과를 저장
420
종료

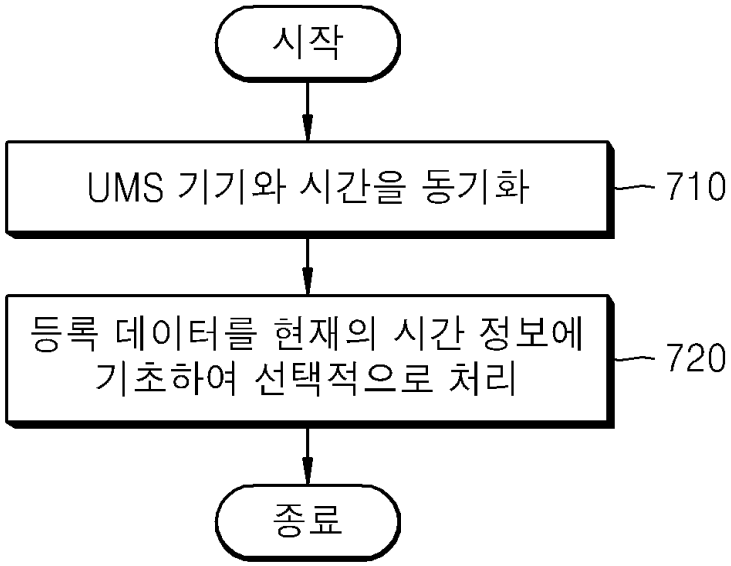
도면5


500
510
511
키 생성부
520
CLOCK
512
등록 데이터
암호화부
530
저장부
540
USB
Host

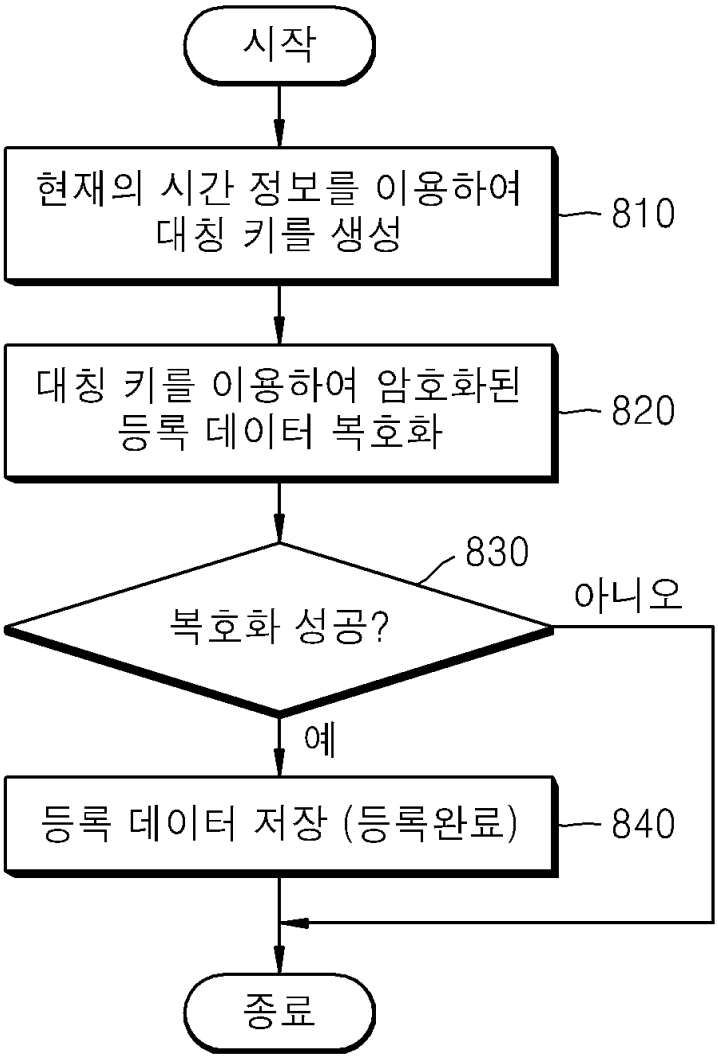
도면6


600
610
CLOCK
621
암호화부
622
저장부
630
USB Host

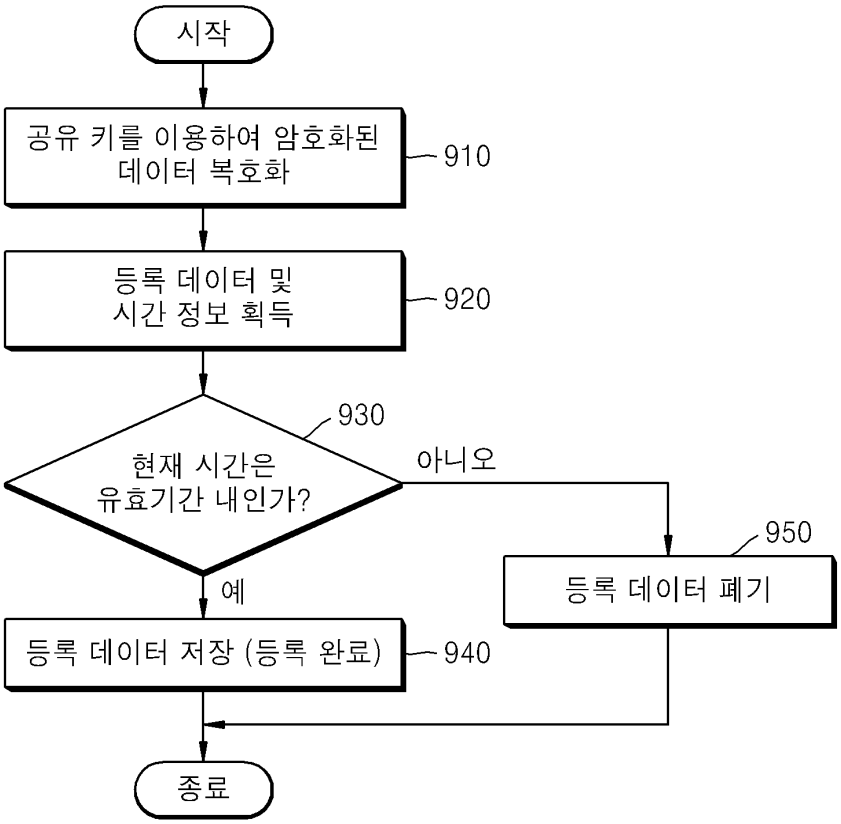
도면7


시작
UMS 기기와 시간을 동기화
710
등록 데이터를 현재의 시간 정보에 기초하여 선택적으로 처리
720
종료

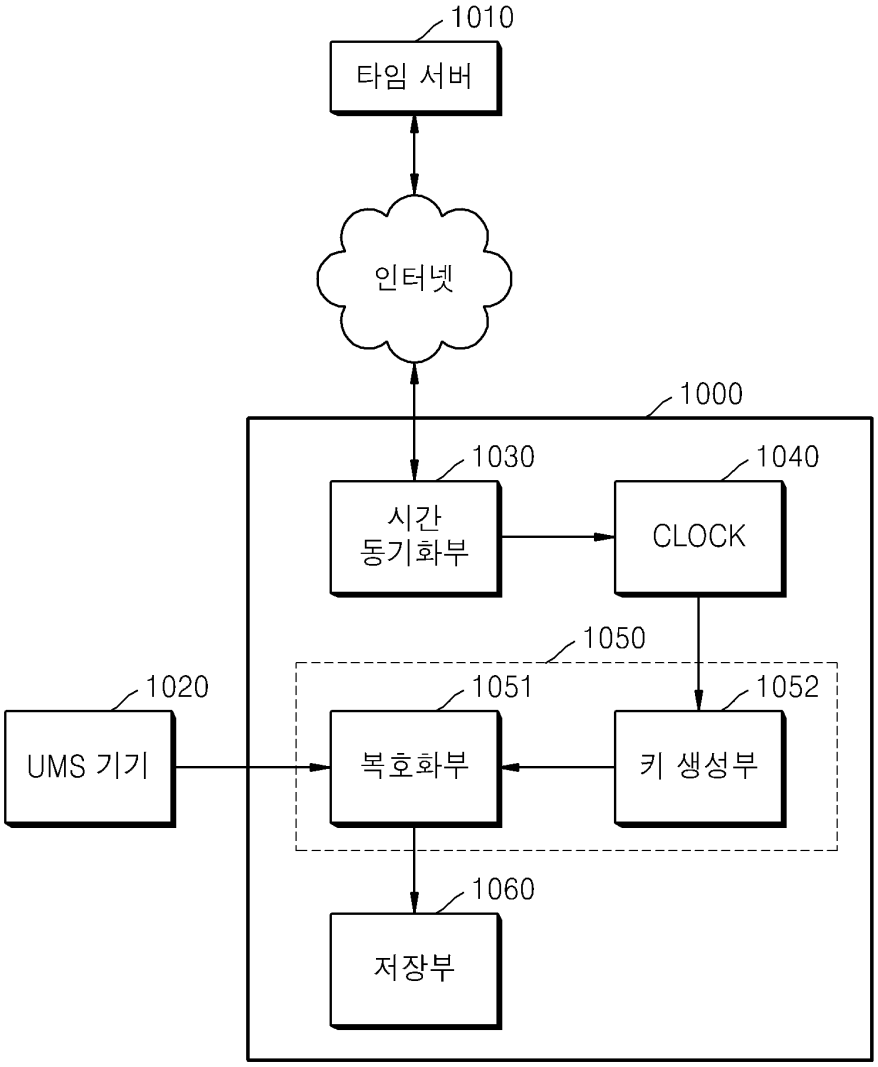
도면8


시작
현재의 시간 정보를 이용하여 대칭 키를 생성
810
대칭 키를 이용하여 암호화된 등록 데이터 복호화
820
830
복호화 성공?
아니오
예
등록 데이터 저장 (등록완료)
840
종료

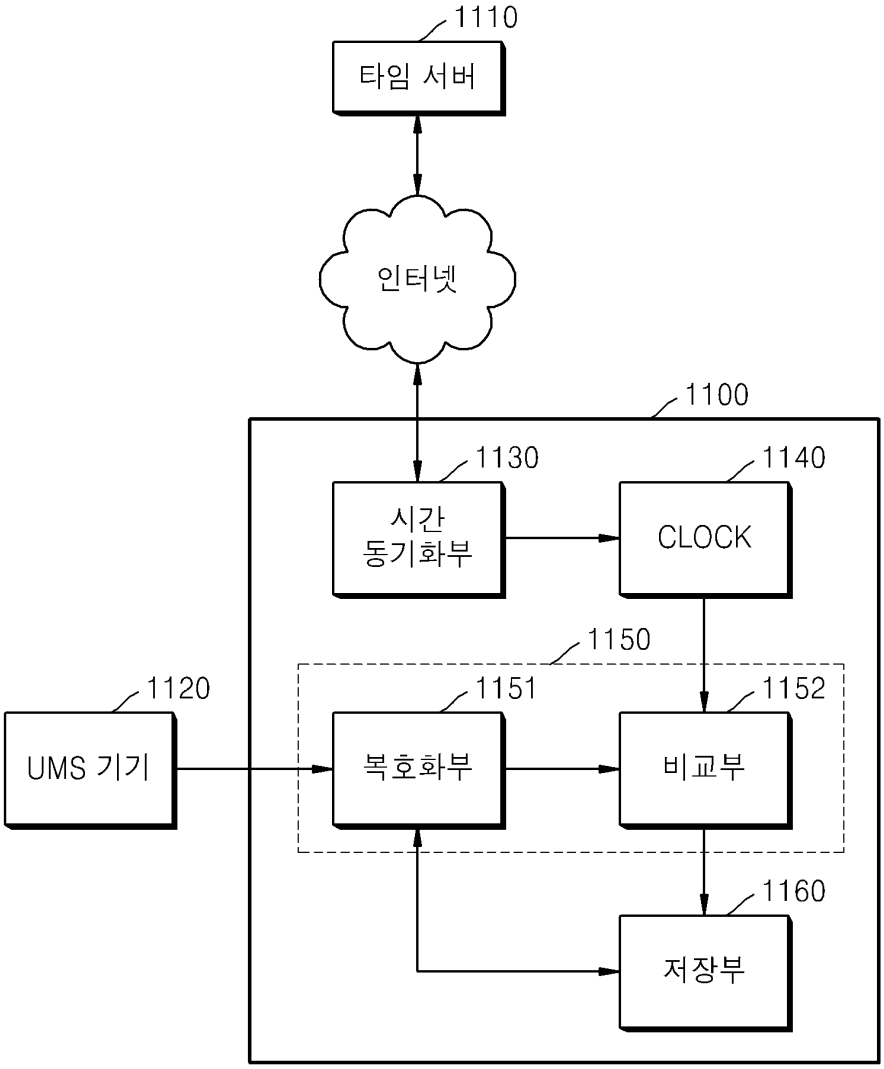
도면9


시작
공유 키를 이용하여 암호화된 데이터 복호화
910
등록 데이터 및 시간 정보 획득
920
930
현재 시간은 유효기간 내인가?
아니오
950
등록 데이터 폐기
예
등록 데이터 저장 (등록 완료)
940
종료

도면10


1010
타임 서버
인터넷
1000
1030
시간
동기화부
1040
CLOCK
1050
1020
UMS 기기
1051
복호화부
1052
키 생성부
1060
저장부

도면11



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제14항 및 제16항

【변경전】

"~ 특징으로 하는 장치"

【변경후】

"~ 특징으로 하는 USB 호스트 장치"