



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년08월10일
(11) 등록번호 10-2288971
(24) 등록일자 2021년08월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/34 (2013.01) G06F 21/10 (2013.01)
G06F 21/46 (2013.01) G06F 21/70 (2013.01)
(52) CPC특허분류
G06F 21/34 (2013.01)
G06F 21/10 (2013.01)
(21) 출원번호 10-2019-0169407
(22) 출원일자 2019년12월18일
심사청구일자 2019년12월18일
(65) 공개번호 10-2021-0077909
(43) 공개일자 2021년06월28일
(56) 선행기술조사문헌
KR1020190128868 A*
(뒷면에 계속)

(73) 특허권자
권오경
서울특별시 마포구 월드컵북로44길 22, 501호 (상
암동, 상암파크빌)
(72) 발명자
권오경
서울특별시 마포구 월드컵북로44길 22, 501호 (상
암동, 상암파크빌)
(74) 대리인
성원찬, 이준영

전체 청구항 수 : 총 7 항

심사관 : 윤혜숙

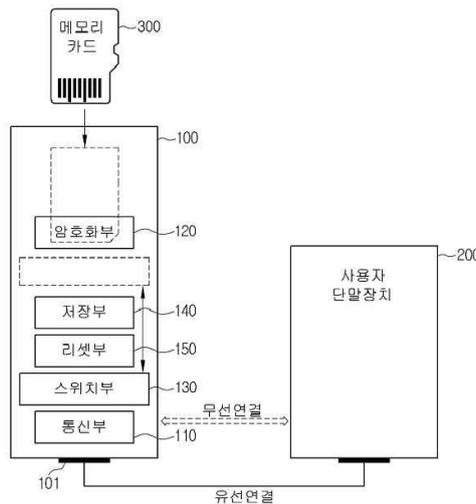
(54) 발명의 명칭 **컨텐츠 월렛 장치 및 이를 이용한 자기주권신원 및 저작권 인증 시스템**

(57) 요약

컨텐츠 월렛 장치가 개시된다. 컨텐츠가 저장된 저장장치가 연결되는 컨텐츠 월렛 장치는, 상기 컨텐츠 월렛 장치 및 사용자 단말 장치 간의 통신을 위한 통신부, 상기 컨텐츠 월렛 장치 및 사용자 단말 장치 간의 인증을 위해 사용자 ID 및 암호를 포함하는 암호화 데이터를 생성하는 암호화부, 상기 저장장치 및 상기 통신부 간의 전기적 연결을 제어하는 스위치부 및 상기 스위치부에 의해 상기 저장장치 및 상기 통신부 간의 전기적 연결이 해제되면 상기 생성된 암호를 초기화 하는 리셋부를 포함한다.

이에 따라, 사용자가 컨텐츠를 판매하는데 있어서, 중앙 관리 시스템에 권한 이양 없이 직접적으로 사용자와 구매자가 컨텐츠를 사고 팔 수 있으며, 사용자가 컨텐츠 소유권을 인증할 때마다 새로운 암호를 생성함으로써, 제 3자의 해킹을 방지하여 컨텐츠의 무단 유출을 막을 수 있다.

대표도 - 도1



(52) CPC특허분류

G06F 21/46 (2013.01)

G06F 21/70 (2013.01)

(56) 선행기술조사문헌

CN107301544 A

US20150039517 A1

US20170161709 A1

KR100669224 B1*

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

컨텐츠가 저장된 저장장치가 연결되는 컨텐츠 월렛 장치에 있어서,

상기 컨텐츠 월렛 장치 및 사용자 단말 장치 간의 통신을 위한 통신부;

상기 컨텐츠 월렛 장치 및 사용자 단말 장치 간의 인증을 위해 사용자 ID 및 암호를 포함하는 암호화 데이터를 생성하는 암호화부;

상기 저장장치 및 상기 통신부 간의 전기적 연결을 제어하는 스위치부; 및

상기 스위치부에 의해 상기 저장장치 및 상기 통신부 간의 전기적 연결이 해제되면 상기 생성된 암호를 초기화하는 리셋부;를 포함하며,

상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면,

상기 통신부는 상기 사용자 단말 장치의 네트워크를 차단하기 위한 신호를 상기 사용자 단말 장치로 전송하는 것인, 컨텐츠 월렛 장치.

청구항 2

제 1항에 있어서,

상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면 상기 암호화부는 제1 랜덤 암호를 생성하고,

상기 스위치부에 의해 상기 저장장치 및 상기 통신부 간의 전기적 연결이 해제되면 상기 리셋부는 상기 제1 랜덤 암호를 초기화시키며,

상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 다시 전기적으로 연결되면 상기 암호화부는 제2 랜덤 암호를 생성하는 것인, 컨텐츠 월렛 장치.

청구항 3

삭제

청구항 4

제 2항에 있어서,

상기 사용자 단말 장치의 네트워크가 차단되면, 상기 암호화부에 의해 생성된 암호화 데이터를 통해 상기 컨텐츠 월렛 장치 및 사용자 단말 장치 간에 인증이 수행되는 것인, 컨텐츠 월렛 장치.

청구항 5

제 1항에 있어서,

상기 암호화부는,

상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면, 상기 컨텐츠를 암호화하여 상기 통신부로 전달하는 것인, 컨텐츠 월렛 장치.

청구항 6

제 1항에 있어서,

상기 암호화부는,

상기 콘텐츠에 사용자 고유의 식별 부호를 삽입하는 것인, 콘텐츠 월렛 장치.

청구항 7

콘텐츠가 저장된 저장장치가 연결되는 콘텐츠 월렛 장치 및 사용자 단말 장치를 포함하는 시스템에 있어서,

상기 콘텐츠 월렛 장치는 상기 콘텐츠 월렛 장치 및 상기 사용자 단말 장치 간의 인증을 위해 사용자 ID 및 암호를 포함하는 암호화 데이터를 상기 사용자 단말 장치에 전송하고,

상기 사용자 단말 장치는 사용자 조작에 따라 입력된 암호가 상기 전송된 암호와 매칭되면 상기 콘텐츠 월렛 장치 및 사용자 단말 장치 간에 인증을 수행하며,

상기 콘텐츠 월렛 장치는,

상기 저장장치 및 상기 콘텐츠 월렛 장치가 전기적으로 연결되면 상기 사용자 단말 장치의 네트워크를 차단하기 위한 신호를 상기 사용자 단말 장치로 전송하고,

상기 사용자 단말 장치는,

상기 전송된 신호에 대응되는 사용자 조작이 입력되면 네트워크를 차단하는 것인, 시스템.

청구항 8

제 7항에 있어서,

상기 콘텐츠 월렛 장치는,

상기 사용자 단말 장치와 인증을 수행할 때마다 상기 인증을 위한 암호를 랜덤하게 생성하여 전송하는 것인, 시스템.

청구항 9

삭제

발명의 설명

기술 분야

[0001] 본 발명은 콘텐츠 월렛 장치 및 이를 이용한 시스템에 관한 것으로서, 보다 상세하게는 자기주권 신원 인증에 필요한 암호를 새롭게 생성함으로써, 콘텐츠 정보의 보안이 강화된 콘텐츠 월렛 장치 및 이를 이용한 시스템에 관한 것이다.

배경 기술

[0002] 온라인 플랫폼을 운영하고자 하는 민간 사업자들은 회원가입 시에 필요한 개인정보 및 플랫폼 이용내역에 관한 데이터 관리, 그리고 해당 정보의 사용권한에 대해 중앙화된 데이터베이스를 운영하고 있는 운영자에게 위탁하여 사업을 운영하는 것이 일반적이다.

[0003] 이렇게 중앙화된 데이터베이스로 운영되는 사실 온라인 플랫폼은 제 3자의 해킹이 있을 경우, 이를 공동으로 이용하는 다른 사용자의 데이터가 쉽게 유출될 수 있는 문제점이 있다.

[0004] 또한, 개인 온라인 플랫폼을 운영하고자 하는 민간 사업자들이 사실 온라인 플랫폼을 이용하게 되면, 이용에 따른 이용료를 높게 지불해야할 뿐만 아니라, 개인 데이터 관리에 문제가 생길 경우에 당사자가 신속하게 대응할 수 없는 문제점 등이 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 목적은 저장장치에 저장된 콘텐츠의 구매를 원하는 구매자에게 중앙 관리서버의 개입 없이 사용자가 직접 전송할 수 있도록 하며, 해킹이나 유출이 쉽게 이루어지지 않도록 사용자 인증 필요할 때마다 새롭게 암호를 생성함으로써, 보안을 강화한 콘텐츠 월렛 장치 및 이를 이용한 시스템을 제공함에 있다.

과제의 해결 수단

- [0006] 이러한 목적을 달성하기 위한 본 발명의 일 실시예에 따른 콘텐츠가 저장된 저장장치가 연결되는 콘텐츠 월렛 장치는, 상기 콘텐츠 월렛 장치 및 사용자 단말 장치 간의 통신을 위한 통신부, 상기 콘텐츠 월렛 장치 및 사용자 단말 장치 간의 인증을 위해 사용자 ID 및 암호를 포함하는 암호화 데이터를 생성하는 암호화부, 상기 저장장치 및 상기 통신부 간의 전기적 연결을 제어하는 스위치부 및 상기 스위치부에 의해 상기 저장장치 및 상기 통신부 간의 전기적 연결이 해제되면 상기 생성된 암호를 초기화 하는 리셋부를 포함할 수 있다.
- [0007] 이때, 상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면 상기 암호화부는 제1 랜덤 암호를 생성하고, 상기 스위치부에 의해 상기 저장장치 및 상기 통신부 간의 전기적 연결이 해제되면 상기 리셋부는 상기 제1 랜덤 암호를 초기화시키며, 상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 다시 전기적으로 연결되면 상기 암호화부는 제2 랜덤 암호를 생성할 수 있다.
- [0008] 또한, 상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면, 상기 통신부는 상기 사용자 단말 장치의 네트워크를 차단하기 위한 신호를 상기 사용자 단말 장치로 전송할 수 있다.
- [0009] 여기서, 상기 사용자 단말 장치의 네트워크가 차단되면, 상기 암호화부에 의해 생성된 암호화 데이터를 통해 상기 콘텐츠 월렛 장치 및 사용자 단말 장치 간에 인증이 수행될 수 있다.
- [0010] 나아가, 상기 암호화부는, 상기 스위치부에 의해 상기 저장장치 및 상기 통신부가 전기적으로 연결되면, 상기 콘텐츠를 암호화하여 상기 통신부로 전달할 수 있다.
- [0011] 또한, 상기 암호화부는, 상기 콘텐츠에 사용자 고유의 식별 부호를 삽입할 수 있다.
- [0012] 한편, 본 발명의 일 실시예에 따른 콘텐츠 월렛 장치 및 사용자 단말 장치를 포함하는 시스템은, 상기 콘텐츠 월렛 장치는 상기 콘텐츠 월렛 장치 및 상기 사용자 단말 장치 간의 인증을 위해 사용자 ID 및 암호를 포함하는 암호화 데이터를 상기 사용자 단말 장치에 전송하고, 상기 사용자 단말 장치는 사용자 조작에 따라 입력된 암호가 상기 전송된 암호와 매칭되면 상기 콘텐츠 월렛 장치 및 사용자 단말 장치 간에 인증을 수행할 수 있다.
- [0013] 여기서, 상기 콘텐츠 월렛 장치는, 상기 사용자 단말 장치와 인증을 수행할 때마다 상기 인증을 위한 암호를 랜덤하게 생성하여 전송할 수 있다.
- [0014] 그리고, 상기 콘텐츠 월렛 장치는, 상기 저장장치 및 상기 콘텐츠 월렛 장치가 전기적으로 연결되면 상기 사용자 단말 장치의 네트워크를 차단하기 위한 신호를 상기 사용자 단말 장치로 전송하고, 상기 사용자 단말 장치는, 상기 전송된 신호에 대응되는 사용자 조작이 입력되면 네트워크를 차단할 수 있다.

발명의 효과

- [0015] 이상과 같은 본 발명에 다양한 실시 예에 따르면, 사용자가 콘텐츠를 판매하는데 있어서, 중앙 관리 시스템에 권한 이양 없이 직접적으로 사용자와 구매자가 콘텐츠를 사고 팔 수 있으며, 사용자가 콘텐츠 소유권을 인증할 때마다 새로운 암호를 생성함으로써, 제 3자의 해킹을 방지하여 콘텐츠의 무단 유출을 막을 수 있다.

도면의 간단한 설명

- [0016] 도 1은 본 발명의 일 실시예에 따른 콘텐츠 월렛 장치의 구성을 도시한 도면이다.
- 도 2는 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치의 구성을 도시한 도면이다.
- 도 3은 도 2에 따른 콘텐츠 월렛 장치를 설명하기 위한 단면도이다.
- 도 4는 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치가 사용자 단말 장치에 내장된 상태를 설명하기 위한 도면이다.
- 도 5는 본 발명의 다른 실시예에 따른 다양한 저장장치가 콘텐츠 월렛 장치에 연결된 상태를 설명하기 위한 도면이다.
- 도 6은 본 발명의 일 실시예에 따른 콘텐츠 월렛 장치를 이용한 시스템을 설명하기 위한 도면이다.
- 도 7은 도 6에 따른 콘텐츠 월렛 장치를 이용한 시스템의 흐름을 설명하기 위한 도면이다.
- 도 8은 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치를 이용한 시스템을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0017] 이하에서는 도면을 참조하여 본 발명을 더욱 상세하게 설명한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관계 등에 따라 달라질 수 있다. 그러므로, 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0018] 본 발명의 저장장치(300)는 콘텐츠를 저장할 수 있는 외장하드, USB, CD, 메모리 카드 등 저장기능을 포함하고 있는 독립된 저장장치일 수 있으며, 이하에서는 메모리 카드(이하, 저장장치의 번호 300으로 기술함)를 가지고 설명하기로 하나, 이에 한정되지 않음은 당연할 것이다.
- [0019] 도 1은 본 발명의 일 실시예에 따른 콘텐츠 월렛 장치의 구성을 도시한 도면이다.
- [0020] 도 1을 참조하면, 콘텐츠 월렛 장치(100)는 콘텐츠가 저장된 메모리 카드(300)가 연결될 수 있으며, 메모리 카드(300)에 저장된 콘텐츠를 사용자 단말 장치(200)에 전송할 수 있다.
- [0021] 이때, 사용자 단말 장치(200)는 모바일 단말 장치일 수 있으나, 이 외에 태블릿 PC, PDA(Personal Digital Assistant), 웨어러블 디바이스, 노트북, 데스크 PC 및 디지털 카메라 등 전기적 통신이 가능한 다양한 전자기기일 수 있다.
- [0022] 또한, 콘텐츠 월렛 장치(100)는 콘텐츠를 전송하기 위해서 통신부(110), 암호화부(120), 스위치부(130), 저장부(140) 및 리셋부(150)를 포함할 수 있다.
- [0023] 통신부(110)는 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간의 통신이 될 수 있도록 하며, 유선에 의한 직접 연결 또는 일정 범위 내 무선에 의한 간접 연결로 통신이 이루어질 수 있다.
- [0024] 예를 들어, 사용자 단말 장치(200) 및 콘텐츠 월렛 장치(100)의 유선에 의한 연결은 일반적으로 사용되는 충전 단자에 연결되는 방식을 이용할 수 있다. 또한, 이 외에도 외장하드, USB, 이어폰 등이 삽입되는 단자 등에 연결되는 방식을 이용하여 직접 연결될 수 있다.
- [0025] 무선에 의한 연결은 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200)가 일정 범위 내에 위치하게 되면, 근거리 무선통신(NFC;Near Field Communication), 주파수 무선통신(RFID;Radio Frequency Identification), 블루투스(Bluetooth) 및 적외선 통신 등을 이용하여 간접 연결될 수 있다.
- [0026] 이렇게 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200)가 통신부(110)에 의해 연결됨으로써, 콘텐츠 월렛 장치(100)에 삽입된 메모리 카드(300)에 저장된 콘텐츠가 사용자 단말 장치(200)로 이동될 수 있고 또한, 콘텐츠 월렛 장치(100)에서 인증을 위해 랜덤하게 생성된 암호가 사용자 단말 장치(200)로 이동될 수 있다.
- [0027] 뿐만 아니라, 통신부(110)는 사용자 단말 장치(100)의 네트워크를 차단하기 위한 신호를 사용자 단말 장치(200)에 전송할 수 있으며, 이하에서 자세히 설명하기로 한다.
- [0028] 암호화부(120)는 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간의 인증을 위해 사용자 ID(Identification) 및 암호(password, pass-code)를 포함하는 암호화 데이터(Encryption data)를 생성할 수 있다.
- [0029] 구체적으로, 암호화부(120)는 메모리 카드(300) 및 통신부(110)가 전기적으로 연결되면 암호화 데이터를 생성할 수 있다.
- [0030] 암호화 데이터에 포함된 사용자 ID는 저장부(140)에 저장되어 있는 사용자 인증 ID일 수 있으며, 예를 들어 분산 ID(DID;Decentralized Identity)에 의한 신원인증 ID일 수 있다.
- [0031] DID는 분산저장 시스템을 기반으로 하는 자기주권 신원 증명 기술로, 분산저장 시스템은 개인의 신원을 구분할 수 있는 정보를 특정 기관이나 기업과 같은 중앙 집중 시스템에 소유권을 위임하지 않고, 신원 검증에 필요한 정보도 네트워크의 말단 구성원들이 나눠 저장, 관리하는 방법이다.
- [0032] 즉, 자기주권 신원 증명 기술은 신원 검증 정보에 대한 주권을 해당 개개인이 스스로 증명하는 방식이다.
- [0033] 이러한 DID를 암호화부(120)는 저장부(140)에서 불러들임으로써, 암호와 함께 암호화 데이터로 생성할 수 있다.
- [0034] 그리고, 생성된 암호화 데이터에 포함된 암호는 숫자, 문자 또는 기호 등을 혼합하여 생성되거나, 터치 횟수,

패턴, 터치 영역 지정 등을 이용하여 생성된 암호일 수 있다.

- [0035] 예를 들어, 생성된 암호의 입력 가능한 자리가 10자리 라면, 사용자 단말 장치가 데스크 PC일 경우, 숫자, 문자 또는 기호는 숫자 0에서 9까지 중 숫자만을 혼합하여 암호를 생성하거나, 타자기에 포함된 한글, 영어 그리고 숫자 위에 함께 병기된 기호를 혼합하여 암호를 생성할 수 있다.
- [0036] 또한, 콘텐츠 월렛 장치에서 데스크 PC 화면으로 직선 또는 곡선 등을 사용하여 패턴형태로 암호를 생성할 수 있다.
- [0037] 나아가, 암호화부(120)는 메모리 카드(300)에 저장된 콘텐츠가 사용자 단말 장치(200)로 전송되기 전에 콘텐츠를 암호화하여 통신부(110)로 전달할 수 있다. 이는 스위치부(130)에 의해 메모리 카드(300) 및 통신부(110)가 전기적으로 연결되면 암호화부(120)가 콘텐츠를 암호화하는 것이다.
- [0038] 예를 들어, 암호화부(120)는 미리 저장되어 있는 매커니즘을 이용하여 아날로그 방식으로 콘텐츠를 암호화하거나, 미리 저장되어 있는 논리적 알고리즘을 이용하는 디지털 방식으로 콘텐츠를 암호화할 수 있다.
- [0039] 암호화된 콘텐츠는 공개키 암호화 방식 또는 비밀키 암호화 방식에 따라 암호화되며, 이렇게 암호화된 콘텐츠가 다시 복호화될 수 있도록 암호화부(120)는 복호화 키도 함께 생성하여 통신부(110)로 전달할 수 있다.
- [0040] 또한, 암호화부(120)는 콘텐츠 암호화 과정을 간소화하기 위해 콘텐츠의 원작자를 식별할 수 있도록 콘텐츠의 암호화를 제외하고 콘텐츠에 사용자 고유의 식별 부호만을 삽입할 수 있다.
- [0041] 예를 들어, 사용자 고유의 식별 부호는 워터마크를 통해 이루어질 수 있다. 워터마크는 콘텐츠의 본래 원작자만이 아는 마크(Mark)를 삽입하는 것으로 허용 권한을 받지 않은 제 3자가 콘텐츠를 불법 복제하거나 유통시킨 경우에 콘텐츠에 삽입된 워터마크를 추출함으로써, 원작자의 콘텐츠임을 확인할 수 있을 뿐만 아니라 복제된 경로를 추적하는데도 사용될 수 있다.
- [0042] 스위치부(130)는 메모리 카드(300) 및 통신부(110) 간의 전기적 연결을 제어할 수 있다.
- [0043] 예를 들어, 스위치부(130)는 물리적으로 위치 변화가 가능한 버튼형식으로, 토글 스위치, 푸시 버튼 스위치, 슬라이딩 버튼 스위치 등을 포함할 수 있다.
- [0044] 이렇게 물리적 위치 변화가 가능한 스위치부(130)는 메모리 카드(300)가 삽입된 후에 메모리 카드(300)가 삽입된 방향으로 스위치부(130)를 옮겨 메모리 카드(300) 및 통신부(110)가 전기적으로 연결이 될 수 있도록 할 수 있으며, 이와 반대로 메모리 카드(300)가 삽입된 방향과 반대 방향으로 스위치부(130)의 위치를 옮겨 메모리 카드(300) 및 통신부(110) 간의 전기적 연결을 해지할 수 있다.
- [0045] 다만, 이는 본 발명을 설명하기 위한 실시예이므로, 물리적으로 위치를 조절하여 메모리 카드(300) 및 통신부(110)를 연결하는 방식이 아닌 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간의 통신이 이루어지면, 콘텐츠 월렛 장치(100) 내에서 메모리 카드(300) 및 통신부(110)가 자동으로 연결되는 방식이 실시될 수 있다.
- [0046] 또한, 스위치부(130)에 의해 메모리 카드(300) 및 통신부(110)가 전기적으로 연결되면, 통신부(110)는 사용자 단말 장치(200)의 네트워크를 차단하기 위한 신호를 사용자 단말 장치(200)로 전송할 수 있다.
- [0047] 만일, 사용자 단말 장치(200)가 모바일 단말 장치일 경우에 통신부(110)는 모바일 단말 장치로 비행기 모드 전환 여부를 묻는 메시지를 전송할 수 있으며, 사용자의 조작에 의해 비행기 모드 전환 여부가 선택될 수 있다.
- [0048] 나아가, 사용자 단말 장치(200)의 네트워크가 차단되면, 암호화부(120)에 의해 생성된 사용자 ID 및 암호를 포함하는 암호화 데이터를 통해 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간에 인증이 수행될 수 있다.
- [0049] 계속해서 모바일 단말 장치를 예를 들어 설명하면, 사용자에게 의해 비행기 모드 전환이 선택될 경우 모바일 단말 장치의 네트워크는 차단되고, 암호화부(120)에 의해 생성된 암호화 데이터를 모바일 단말 장치에 전송할 수 있다.
- [0050] 이때, 사용자는 전송된 암호화 데이터에 포함된 암호를 모바일 단말 장치에 입력하고, 콘텐츠 월렛 장치(100)에서 생성된 암호와 일치할 경우, 저장된 콘텐츠에 대해 저작권 식별 정보에 관한 데이터가 부가적으로 콘텐츠 월렛 장치(100)에 기록될 수 있다.
- [0051] 또한, 사용자의 조작에 의해 모바일 단말 장치에 입력된 암호 및 콘텐츠 월렛 장치(100)에서 생성된 암호의 일치 여부를 확인함으로써, 암호화된 콘텐츠에 대한 사용자의 인증이 수행되는 것이며, 이를 통해 자기주권 신원

인증이 이뤄질 수 있다.

- [0052] 전술한 바와 같이, 사용자 단말 장치가 데스크 PC일 경우, 숫자, 문자 또는 기호는 숫자 0에서 9까지 중 숫자만을 혼합하여 생성된 암호, 타자기에 포함된 한글, 영어 그리고 숫자 위에 함께 병기된 기호를 혼합하여 생성된 암호를 데스크 PC가 전송받아 타자기 또는 그 밖에 입력장치를 통해 전송된 암호와 상응하는 암호를 입력하여 인증을 수행할 수 있다.
- [0053] 또한, 패턴에 의한 암호의 경우에는 사용자 단말 장치의 마우스 또는 터치가 가능한 화면에 전송된 패턴 암호를 따라 그림으로써 암호를 입력하여 인증을 수행할 수 있다.
- [0054] 여기서, 암호화부(120)에 의해 전송된 암호 및 사용자에 의해 사용자 단말 장치(200)에 의해 입력된 암호의 일치여부는 콘텐츠 월렛 장치(100)에 포함된 저장부(140)에서 이루어질 수 있다.
- [0055] 예를 들면, 저장부(140)에 저장된 암호 인증 모듈 또는 암호 인증 프로그램을 통해 암호화부(120)에 의해 전송된 암호 및 사용자에 의해 사용자 단말 장치(200)에 의해 입력된 암호 간의 일치여부가 수행될 수 있다.
- [0056] 저장부(140)는 ROM, RAM, EPROM, EEPROM, 하드디스크 등 적어도 하나를 포함할 수 있으며, 이 외에 저장 가능한 비휘발성 메모리를 포함하는 저장 매체일 수 있다.
- [0057] 이렇게 저장부(140)를 통해 콘텐츠 월렛 장치(100)에서 생성된 암호 및 사용자의 조작에 의해 사용자 단말 장치(200)에 입력된 암호가 서로 일치하게 되면, 사용자 ID의 소유자인 사용자는 사용자 단말 장치(200)를 통해 인증된 콘텐츠 월렛 장치(100)의 메모리 카드(300) 내에 저장된 콘텐츠를 조회할 수 있다.
- [0058] 또한, 다른 외부 단말 장치로 콘텐츠 전송이 필요한 경우, 조회된 콘텐츠를 선택하여 콘텐츠 월렛 장치(100)로부터 사용자 단말 장치(200)로 전송시킨 후에 사용자 단말 장치(200)가 수신한 콘텐츠를 다른 외부 단말 장치로 전송시킬 수 있다.
- [0059] 여기서, 선택된 콘텐츠가 콘텐츠 월렛 장치(100)로부터 사용자 단말 장치(200)로 전송되는 경우, 암호화가 수행되어 전송될 수 있다.
- [0060] 한편, 콘텐츠 월렛 장치(100)는 프로세서(미도시)를 포함할 수 있다. 이 경우 상술한 암호화부(120)의 동작은 프로세서(미도시)가 수행할 수 있으며 이때 암호화부(120)는 프로세서(미도시)로 대체될 수 있다.
- [0061] 프로세서(미도시)는 저장부(140)에 저장된 암호 인증 모듈에 저장된 프로그램을 읽어들이 생성된 암호 및 사용자의 조작에 의해 사용자 단말 장치(200)에 입력된 암호가 서로 일치하는지 여부를 산출할 수 있다.
- [0062] 또한, 프로세서(미도시)는 저장부(140)에 저장된 콘텐츠 암호화 모듈에 저장된 프로그램을 읽어들이 콘텐츠를 상술한 바와 같이 암호화할 수 있다.
- [0063] 리셋부(150)는 스위치부(130)에 의해 메모리 카드(300) 및 통신부(110) 간의 전기적 연결이 해제되면 생성된 암호를 초기화할 수 있다.
- [0064] 예를 들어, 콘텐츠 월렛 장치(100)에 메모리 카드(300)가 삽입되고 삽입된 방향으로 스위치부(130)가 옮겨지게 되면, 메모리 카드(300) 및 통신부(110)가 전기적으로 연결됨으로써 암호화부(120)는 제1 랜덤 암호를 생성할 수 있다.
- [0065] 그 후, 스위치부(130)가 메모리 카드(300)가 삽입된 방향과 반대 방향으로 옮겨지게 되면, 메모리 카드(300) 및 통신부(110) 간의 전기적 연결이 해제되면서 리셋부(150)에 의해 제1 랜덤 암호가 초기화될 수 있다.
- [0066] 물론, 이때 암호화부(120)에 의해 생성된 제1 랜덤 암호는 저장부(140)에 저장되며, 스위치부(130)에 의해 메모리 카드(300) 및 통신부(110) 간의 전기적 연결이 해제되면서 저장부(140)에 저장된 제1 랜덤 암호는 리셋부(150)에 의해 초기화될 수 있다.
- [0067] 만약, 스위치부(130)가 다시 메모리 카드(300)가 삽입된 방향으로 옮겨지게 되면 메모리 카드(300) 및 통신부(110)가 다시 전기적으로 연결이 되면서 암호화부(120)는 초기화된 제1 랜덤 암호와 다른 제2 랜덤 암호를 생성할 수 있으며, 제2 랜덤 암호 역시 저장부(140)에 저장될 수 있다.
- [0068] 이렇게, 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200)가 연결될 때마다, 암호화부(120)는 랜덤하게 암호를 새롭게 생성할 수 있으며, 종전에 랜덤하게 생성된 암호는 리셋부(150)에 의해 초기화됨으로써, 제 3자의 해킹 위험을 방지할 수 있다.

- [0069] 도 2는 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치의 구성을 도시한 도면이며, 도 3은 도 2에 따른 콘텐츠 월렛 장치를 설명하기 위한 단면도이다.
- [0070] 여기서, 통신부(110), 암호화부(120), 스위치부(130), 저장부(140) 및 리셋부(150)는 이미 설명하였으므로 상세한 설명은 생략하기로 한다.
- [0071] 도 2를 참조하면, 콘텐츠 월렛 장치(100)는 입력부(160)를 더 포함할 수 있다.
- [0072] 입력부(160)는 사용자의 조작을 입력받기 위함이며, 콘텐츠 월렛 장치(100)에서 생성된 암호는 사용자의 조작에 의해 입력부(160)에 입력됨으로써 생성될 수 있다.
- [0073] 다시 말해, 일 실시예로써 랜덤하게 생성된 암호는 도 1에 도시된 스위치부(130)에 의해 메모리 카드(300) 및 통신부(110)가 전기적으로 연결되면서 암호화부(120)를 통해 랜덤하게 암호를 생성할 수 있을 뿐만 아니라, 다른 실시예로써 도 2에 도시된 입력부(160)를 통해 사용자 조작에 의한 암호가 입력됨으로써 랜덤하게 생성될 수 있는 것이다.
- [0074] 물론 사용자의 조작에 의해 암호가 생성되므로, 리셋부(150)에 의해 초기화되기 전의 암호와 추가화 된 후의 암호가 동일할 수 있음은 당연할 것이다.
- [0075] 이때, 도 2에 도시된 암호화부(120)는 메모리 카드(300)에 저장된 콘텐츠를 암호화하고, 이를 복호화하기 위한 복호화 키를 생성할 수 있다.
- [0076] 또한, 콘텐츠의 원작자가 식별될 수 있도록 사용자 고유의 식별 부호를 생성할 수 있다.
- [0077] 도 3을 참조하여 콘텐츠 월렛 장치(100)의 작동을 설명하면, 콘텐츠 월렛 장치(100)에 메모리 카드(300)가 삽입될 수 있으며, 삽입된 메모리 카드(300)는 암호화부(120)와 연결될 수 있다.
- [0078] 이때, 스위치부(130)가 메모리 카드(300)가 삽입된 방향으로 위치가 옮겨지게 되면, 메모리 카드(300) 및 통신부(110)가 전기적으로 연결되면서 암호화부(120)는 저장부(140)에 저장된 사용자 ID를 불러들여 사용자 ID를 생성할 수 있다.
- [0079] 그리고, 입력부(160)를 통해 사용자가 임의로 입력한 암호가 랜덤하게 생성될 수 있으며, 동시에 랜덤하게 생성된 암호는 저장부(140)에 저장될 수 있다.
- [0080] 이렇게 입력부(160)를 통해 생성된 암호 및 암호화부(120)를 통해 생성된 사용자 ID는 통신부(110)에 전달될 수 있다.
- [0081] 통신부(110)에 전달된 랜덤하게 생성된 암호는 사용자 단말 장치(200)에 전송될 수 있으며, 사용자 단말 장치(200)를 통해 사용자가 랜덤하게 생성된 암호를 입력하게 되면 콘텐츠 월렛 장치(100)는 통신부(110)를 통해 사용자가 입력한 암호를 전달받게 되고, 저장부(140)는 전달된 암호를 저장하게 된다.
- [0082] 이렇게 저장부(140)는 콘텐츠 월렛 장치(100)에서 랜덤하게 생성된 암호 및 사용자 단말 장치(200)에 입력된 암호의 일치 여부를 확인할 수 있다.
- [0083] 만약, 저장된 암호가 서로 매칭될 경우, 사용자는 사용자 단말 장치(200)를 통해 메모리 카드(300) 내에 저장된 콘텐츠를 조회할 수 있다. 또한, 외부 단말 장치로 콘텐츠를 전송할 경우, 암호화부(120)는 메모리 카드(300)에 저장된 콘텐츠를 암호화하여 통신부(110)에 전달하고, 통신부(110)는 사용자 단말 장치(200)에 암호화된 콘텐츠를 외부 단말 장치로 전송할 수 있다.
- [0084] 스위치부(130)는 메모리 카드(300)가 삽입된 반대 방향으로 위치가 옮겨지게 되면 리셋부(150)에 의해 저장부(140)에 저장된 암호가 초기화 될 수 있다.
- [0085] 그러나, 도 3에 도시된 콘텐츠 월렛 장치(100)는 본 발명을 실시하기 위한 하나의 예시이므로, 콘텐츠 월렛 장치(100)에 포함된 구성요소의 위치는 사용자의 이용 및 편의에 따라 변경될 수 있다.
- [0086] 도 4는 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치가 사용자 단말 장치에 내장된 상태를 설명하기 위한 도면이다.
- [0087] 도 4를 참고하면, 콘텐츠 월렛 장치(100)는 사용자 단말 장치(200)에 내장되는 형태로 실시될 수 있다.
- [0088] 이때, 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200)의 통신은 콘텐츠 월렛 장치(100)가 사용자 단말 장치(300)에 삽입되는 과정에서 이루어지며, 완전하게 콘텐츠 월렛 장치(100)가 사용자 단말 장치(200)에 삽입되면

컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200)는 전기적으로 연결될 수 있다.

- [0089] 이렇게 전기적으로 연결됨과 동시에 컨텐츠 월렛 장치(100)는 사용자 단말 장치(200)에 외부 통신망을 중단하는 메시지를 전송하게 된다.
- [0090] 만일, 사용자가 사용자 단말 장치(200)에 외부 통신망을 중단하는 선택을 입력하게 되면, 컨텐츠 월렛 장치(100)는 랜덤하게 암호를 생성하고, 컨텐츠 월렛 장치(100)에 저장되어 있던 사용자 ID를 불러들여 생성된 암호와 함께 사용자 단말 장치(200)로 전송할 수 있다.
- [0091] 그러면, 사용자 단말 장치(200)에 전송된 암호가 사용자에게 의해 입력되고, 컨텐츠 월렛 장치(100)는 입력된 암호와 컨텐츠 월렛 장치(100)에서 랜덤하게 생성된 암호를 매칭하여 일치여부를 확인한 후, 메모리 카드(300)에 저장된 컨텐츠를 암호화하여 사용자 단말 장치(200)에 전송하게 되는 것이다.
- [0092] 암호화된 컨텐츠가 사용자 단말 장치(200)에 전송이 모두 완료되면 삽입된 컨텐츠 월렛 장치(100)는 사용자 단말 장치(200)에서 외부로 분리될 수 있다.
- [0093] 이때, 컨텐츠 월렛 장치(100)가 사용자 단말 장치(200)에서 분리되면서 랜덤하게 생성되었던 암호는 초기화될 수 있다.
- [0094] 컨텐츠 월렛 장치(100)가 사용자 단말 장치(200)에 내장되어 실시되는 다른 예로는, 컨텐츠 월렛 장치(100)가 사용자 단말 장치(200)에 삽입이 되면, 삽입되지 않고 외부로 노출되어 있는 일 면에 위치변화가 가능한 스위치 유닛(미도시)을 포함시킬 수 있다.
- [0095] 이러한 스위치유닛은 토글 스위치, 푸시 버튼 스위치, 슬라이딩 버튼 스위치 등일 수 있으며, 이를 이동시킴으로써 컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200)의 전기적으로 연결을 제어할 수 있다.
- [0096] 도 5는 본 발명의 다른 실시예에 따른 다양한 저장장치가 컨텐츠 월렛 장치에 연결된 상태를 설명하기 위한 도면이다.
- [0097] 도 5를 참고하면, 컨텐츠 월렛 장치(100)는 다수개의 입·출력 포트를 포함할 수 있으며, 포트를 통해 다양한 저장장치를 연결할 수 있다.
- [0098] 이때, 다수개의 입·출력 포트를 포함하고 있는 월렛 장치(100)는 USB 또는 썬더볼트 등과 같이 도킹스테이션이 가능한 장치일 수 있다.
- [0099] 도 6은 본 발명의 일 실시예에 따른 컨텐츠 월렛 장치를 이용한 시스템을 설명하기 위한 도면이다.
- [0100] 도 6을 참조하면, 컨텐츠 월렛 장치를 이용한 시스템(10)은 컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200)를 포함할 수 있다.
- [0101] 컨텐츠 월렛 장치(100)는 컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간의 인증을 위해 사용자 ID 및 랜덤하게 생성된 암호를 포함하는 암호화 데이터를 사용자 단말 장치(200)에 전송할 수 있다.
- [0102] 사용자 단말 장치(200)는 사용자 조작에 따라 입력된 암호가 전송된 암호와 매칭이 되면, 컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200)간에 인증을 수행할 수 있다.
- [0103] 예를 들어, 컨텐츠 월렛 장치(100)는 랜덤하게 생성된 암호를 사용자 단말 장치(200)에 전송할 수 있으며, 전송된 암호를 사용자가 사용자 단말 장치(200) 통해 입력함으로써, 입력된 암호를 전송받은 컨텐츠 월렛 장치(100)는 랜덤하게 생성된 암호와 매칭하여 일치여부를 확인할 수 있다.
- [0104] 여기서, 랜덤하게 생성된 암호는 컨텐츠 월렛 장치(100) 및 사용자 단말 장치(200)가 인증을 수행할 때마다 새롭게 생성될 수 있으며, 컨텐츠 월렛 장치(100)는 인증 시마다 새롭게 생성된 암호의 일치여부를 확인할 수 있다.
- [0105] 만일, 매칭된 암호가 서로 일치하게 되면 컨텐츠 월렛 장치(100)는 컨텐츠 및 사용자 ID를 사용자 단말 장치(200)에 전달하게 되고 이를 구입하고자 하는 다른 사용자의 사용자 단말 장치(200-1)에 암호화된 컨텐츠를 복호화 키와 함께 컨텐츠 및 사용자 ID를 직접 전송할 수 있다.
- [0106] 이때, 사용자 단말 장치(200)는 컨텐츠 월렛 장치(100)에서 전송된 사용자 ID를 다른 사용자의 사용자 단말 장치(200-1)로 전송함으로써, 서로 DID(Decentralized Identity)에 의한 신원인증을 수행할 수 있다.
- [0107] 예를 들어, 컨텐츠를 공급하려는 사용자 단말 장치(200)에서 컨텐츠 월렛 장치(100)에서 전송된 비활성화된 사

용자 ID(DID) 및 암호화된 콘텐츠를 다른 사용자 단말 장치(200-1)로 전송하게 되면, 다른 사용자 단말 장치(200-1)에서 자가 신원 인증 값(SSI;Self-Sovereign Identity)을 전송함으로써, 공급자에게 해당 개별 수요에 대한 사용자 신원인증을 수행할 수 있다.

- [0108] 물론, 이와 반대로 다른 사용자는 자신의 콘텐츠 월렛 장치(100-1)를 통해 랜덤하게 생성된 암호를 사용자 단말 장치(200-1)에 입력함으로써, 콘텐츠 월렛 장치(100-1)에서 전달된 암호 및 사용자 단말 장치(200-1)의 사용자에게 의해 입력된 암호가 일치되면 자신이 소유하고 있는 콘텐츠를 사용자 단말 장치(200-1)에 전송할 수 있으며, 다른 사용자 단말 장치(200)에 직접 전송할 수 있다.
- [0109] 이렇게 서로 다른 사용자가 소유하고 있는 콘텐츠를 콘텐츠 월렛 장치(100,100-1) 및 사용자 단말 장치(200,200-1)를 통해 랜덤하게 생성된 암호를 통해 정당한 사용자임을 증명한 후, 사용자 ID 및 콘텐츠를 직접 전송함으로써 제 3자의 해킹 및 콘텐츠의 불법 유출을 방지할 수 있다.
- [0110] 도 1 및 도 6를 참조하면, 콘텐츠 월렛 장치(100)를 포함하고 있는 시스템(10)은 메모리 카드(300) 및 콘텐츠 월렛 장치(100)가 전기적으로 연결되면 사용자 단말 장치(200)의 네트워크를 차단하기 위한 신호를 사용자 단말 장치(200)로 전송하고, 사용자 단말 장치(200)는 전송된 신호에 대응되는 사용자 조작이 입력되면 네트워크를 차단할 수 있다.
- [0111] 이때, 차단되는 네트워크는 사용자 단말 장치(200)의 외부 통신망일 수 있으며, 예를 들어 근거리 네트워크(LAN;Local Area Network), 도시권 네트워크(MAN;Metropolitan Area Network), 광역 네트워크(WAN;Wide Area Network) 등을 포함할 수 있다.
- [0112] 구체적으로 예를 들면, 사용자 단말 장치(200)가 모바일 단말 장치일 경우에 통신부(110)는 모바일 단말 장치로 비행기 모드 전환 여부를 묻는 메시지를 전송할 수 있으며, 사용자의 조작에 의해 비행기 모드 전환 여부가 선택될 수 있다.
- [0113] 이때, 사용자가 비행기 모드 전환을 선택하게 되면, 모바일 단말 장치의 외부 통신망인 네트워크는 차단되고, 유선에 의한 직접 연결 또는 일정 범위 내 무선에 의한 간접 연결로 콘텐츠 월렛 장치(100) 및 사용자 단말 장치(200) 간의 통신만이 수행될 수 있다.
- [0114] 도 7은 도 6에 따른 콘텐츠 월렛 장치를 이용한 시스템의 흐름을 설명하기 위한 도면이다.
- [0115] 도 7을 참조하면, 콘텐츠 월렛 장치를 이용한 시스템(10)은 메모리 카드가 콘텐츠 월렛 장치에 삽입되는 단계(S100), 삽입된 메모리 카드와 콘텐츠 월렛 장치의 연결 여부를 판단하는 단계(S200), 콘텐츠 월렛 장치에서 사용자 단말 장치로 네트워크 차단을 위한 신호를 전송하는 단계(S300), 사용자 단말 장치의 네트워크 차단 여부를 판단하는 단계(S400), 콘텐츠 월렛 장치에서 사용자 단말 장치로 암호화 데이터를 전송하는 단계(S500), 콘텐츠 월렛 장치 및 사용자 단말 장치 간의 랜덤하게 생성된 암호의 일치 여부를 확인하는 단계(S600), 콘텐츠 월렛 장치에서 콘텐츠를 암호화하여 사용자 단말로 전송하는 단계(S600)를 순차적으로 진행할 수 있다.
- [0116] 메모리 카드가 콘텐츠 월렛 장치에 삽입되는 단계(S100)는 콘텐츠가 저장된 메모리 카드가 콘텐츠 월렛 장치에 삽입되는 단계이며, 그 후 삽입된 메모리 카드와 콘텐츠 월렛 장치의 연결 여부를 판단하는 단계(S200)를 진행할 수 있다.
- [0117] 이때, 삽입된 메모리 카드와 콘텐츠 월렛 장치의 연결 여부를 판단하는 단계(S200)는 물리적인 변화에 의해 전기적으로 메모리 카드와 콘텐츠 월렛 장치가 연결되었는지 여부를 확인하는 단계일 수 있다.
- [0118] 만약 메모리 카드와 콘텐츠 월렛 장치가 전기적으로 연결되지 않았을 경우에는 콘텐츠 월렛 장치를 이용한 시스템은 콘텐츠를 사용자 단말에 전송하는 절차를 진행하지 않는다.
- [0119] 반대로, 메모리 카드와 콘텐츠 월렛 장치가 전기적으로 연결된 경우에는 콘텐츠 월렛 장치에서 사용자 단말 장치로 네트워크 차단을 위한 신호를 전송하는 단계(S300)로 진행할 수 있다.
- [0120] 콘텐츠 월렛 장치에서 사용자 단말 장치로 네트워크 차단을 위한 신호를 전송하는 단계(S300)는 사용자 단말 장치가 다른 전자기기와 통신을 위해 사용하고 있는 외부 통신망인 네트워크를 차단하는 신호를 전송하는 단계일 수 있다.
- [0121] 네트워크를 차단하는 신호가 사용자 단말 장치에 정상적으로 전달되면, 사용자의 조작에 의해 네트워크 차단 여부를 선택할 수 있다.

- [0122] 사용자 단말 장치의 네트워크 차단 여부를 판단하는 단계(S400)는 사용자의 조작에 의해 네트워크 차단이 선택된다면, 사용자 단말 장치의 네트워크가 정상적으로 차단되었는지 여부를 판단하는 단계일 수 있다.
- [0123] 만약, 사용자 단말 장치의 네트워크가 정상적으로 차단되지 않았다면, 삽입된 메모리 카드와 콘텐츠 월렛 장치의 연결 여부를 판단하는 단계(S200)로 회귀하여 메모리 카드와 콘텐츠 월렛 장치의 전기적 연결이 되었는지를 판단할 수 있다.
- [0124] 반대로, 사용자 단말 장치의 네트워크가 정상적으로 차단되었다면, 콘텐츠 월렛 장치에서 사용자 단말 장치로 암호화 데이터를 전송하는 단계(S500)로 진행할 수 있다.
- [0125] 이때, 암호화 데이터는 사용자 ID 및 랜덤하게 생성된 암호를 포함하는 데이터일 수 있다.
- [0126] 콘텐츠 월렛 장치에서 사용자 단말 장치로 랜덤하게 생성된 암호를 전송하는 단계(S500)는 메모리 카드 및 콘텐츠 월렛 장치 간의 연결이 정상적으로 이루어지게 되면 콘텐츠 월렛 장치에 포함되어 있는 암호화부가 랜덤하게 암호를 생성하고, 랜덤하게 생성된 암호를 사용자 단말 장치로 전송하는 단계일 수 있다.
- [0127] 이때, 랜덤하게 생성된 암호 뿐만 아니라 사용자 ID도 함께 사용자 단말 장치로 전송될 수 있다.
- [0128] 이렇게 랜덤하게 생성된 암호가 사용자 단말 장치에 전송되면, 콘텐츠 월렛 장치 및 사용자 단말 장치 간의 랜덤하게 생성된 암호의 일치 여부를 확인하는 단계(S600)를 진행할 수 있다.
- [0129] 콘텐츠 월렛 장치 및 사용자 단말 장치 간의 랜덤하게 생성된 암호의 일치 여부를 확인하는 단계(S600)는 사용자 단말 장치에 전송된 랜덤하게 생성된 암호가 사용자의 조작에 의해 사용자 단말 장치에 입력되면, 입력된 암호는 콘텐츠 월렛 장치에 전송되고, 전송된 암호 및 콘텐츠 월렛 장치에서 랜덤하게 생성된 암호를 매칭하게 된다.
- [0130] 매칭된 암호가 일치하지 않는다면, 삽입된 메모리 카드와 콘텐츠 월렛 장치의 연결 여부를 판단하는 단계(S200)로 진행하게 되고, 메모리 카드와 콘텐츠 월렛 장치의 전기적 연결이 새롭게 이루어 지면서 충전에 랜덤하게 생성된 암호는 초기화되고 다른 암호를 랜덤하게 생성할 수 있다.
- [0131] 반대로, 매칭된 암호가 일치한다면, 콘텐츠 월렛 장치에서 콘텐츠를 암호화하여 사용자 단말로 전송하는 단계(S700)를 진행할 수 있다.
- [0132] 콘텐츠 월렛 장치에서 콘텐츠를 암호화하여 사용자 단말로 전송하는 단계(S700)는 메모리 카드에 저장되어 있는 콘텐츠를 암호화함과 동시에 콘텐츠의 원작자가 전송하고자 하는 다른 사용자 또는 정상적으로 콘텐츠를 구매한 사용자가 콘텐츠를 이용할 수 있도록 암호화된 콘텐츠를 복호화할 수 있는 복호화 키를 함께 전송하는 단계일 수 있다.
- [0133] 이때, 암호화된 콘텐츠는 콘텐츠의 원작자를 구별하기 위해서 사용자 고유의 식별부호가 삽입되어 전송될 수 있다.
- [0134] 도 8은 본 발명의 다른 실시예에 따른 콘텐츠 월렛 장치를 이용한 시스템을 설명하기 위한 도면이다.
- [0135] 도 8을 참조하면, 콘텐츠 월렛 장치를 이용한 시스템(10)은 사용자 단말 장치(200, 200-1, 200-2, 200-3, 200-4, 200-5)를 소유하고 있는 사용자 간에 직접 콘텐츠를 무료 또는 유료로 전송할 수도 있지만, 다수의 사용자 단말 장치(200, 200-1, 200-2, 200-3, 200-4, 200-5)에 콘텐츠 월렛 장치(100, 100-1, 100-2, 100-3, 100-4, 100-5)를 이용함으로써, 사용자는 원하는 콘텐츠를 용이하게 전송받을 수 있다.
- [0136] 이때, 다수의 사용자 단말 장치(200, 200-1, 200-2, 200-3, 200-4, 200-5) 중 어느 하나의 사용자 단말 장치(200)에서 콘텐츠 월렛 장치(100)를 통해 사용자 인증을 수행한 후에 암호화된 콘텐츠를 네트워크에 전송하게 되면, 네트워크는 암호화된 콘텐츠의 미리보기 혹은 관련정보를 제공할 수 있다.
- [0137] 그러면, 다수의 사용자는 소유하고 있는 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)를 통해 암호화된 콘텐츠의 미리보기 혹은 관련정보를 보고 구매를 원할 경우, 암호화된 콘텐츠에 관한 비용을 지불하고 비용이 모두 지불되면, 암호화된 콘텐츠를 소유하고 있는 원작자가 다른 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)에 암호화된 콘텐츠 및 복호화 키를 함께 전송할 수 있다.
- [0138] 여기서, 콘텐츠 월렛 장치(100, 100-1, 100-2, 100-3, 100-4, 100-5)를 사용하는 사용자 단말 장치(200, 200-1, 200-2, 200-3, 200-4, 200-5)간의 구매 이력 및 전송 이력 등은 분산원장에 이루어질 수 있다.

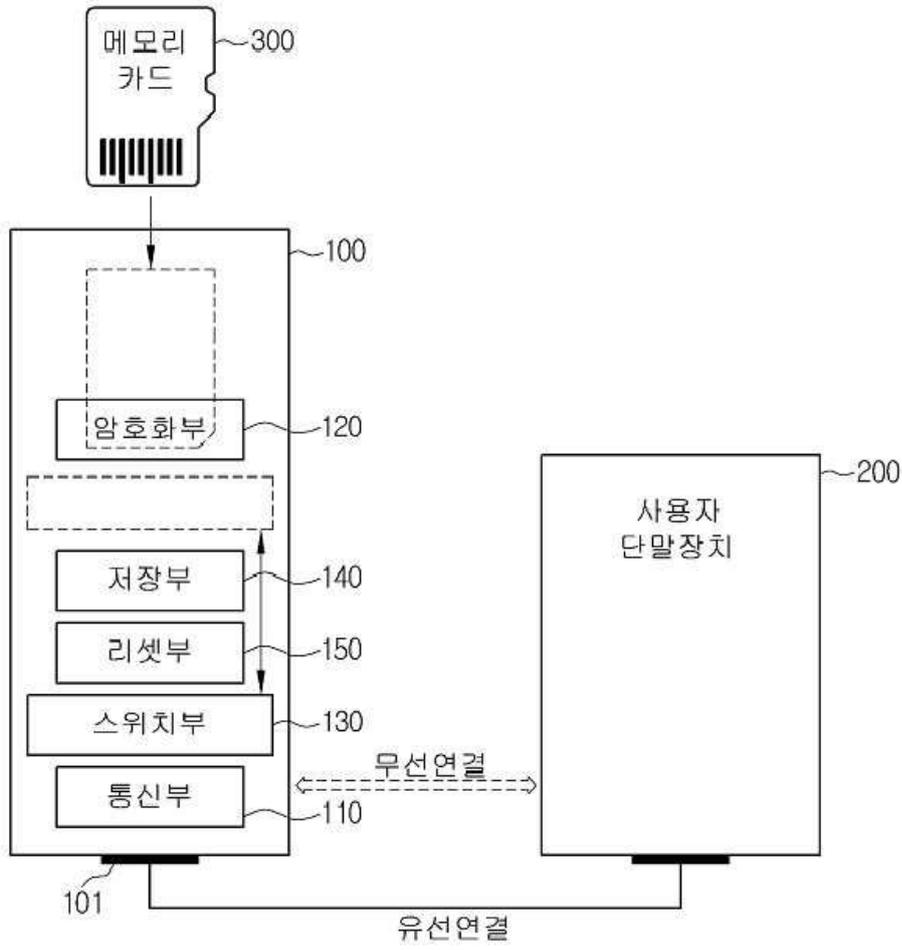
- [0139] 분산원장은 일반적으로 사용되는 블록체인에 의한 것일 수 있으며, 이를 사용함으로써 본 발명의 콘텐츠 월렛 장치(100)를 이용하여 콘텐츠를 주고받은 모든 이력이 저장될 수 있다.
- [0140] 또한, 분산원장은 각 콘텐츠 월렛 장치(100, 100-1, 100-2, 100-3, 100-4, 100-5)에서 전송된 사용자 ID를 통해 구매이력 및 전송 이력 등이 어떤 사용자에게 의해 이루어졌는지 저장할 수 있다.
- [0141] 이때, 사용되는 사용자 ID는 각 콘텐츠 월렛 장치(100, 100-1, 100-2, 100-3, 100-4, 100-5)의 사용자가 자신이 소유하고 있는 사용자 인증 ID, 즉 분산 ID(DID)임을 전술한 바 있다.
- [0142] 이에 따라, 각 사용자들은 분산원장에 의해 저장된 모든 이력을 열람할 수 있으며, 어떤 사용자에게 의해 구매 및 전송 등이 이루어졌는지를 용이하게 알 수 있어 투명화된 거래가 가능한 이점이 있다.
- [0143] 또한, DID를 사용함으로써, 중앙 서버에 의해 신원 정보가 관리되던 사용자 인증 방법을 사용자 본인이 직접 관리할 수 있는 이점이 있다.
- [0144] 다시 말해, 예를 들어 메모리 카드에 저장된 콘텐츠가 동영상이라고 한다면, 이를 공급하고자 하는 사용자 단말 장치(200)에서 구매하려는 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)로 사용자의 신원 인증에 필요한 분산 ID(DID)가 전송될 수 있다.
- [0145] 그런 후, 구매하려는 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)에서 신원 인증 값(SSI)을 전송하여 사용자 신원인증이 성립되면, 동영상이 완전히 공개되지 않은 형태로 암호화되어 복호화키와 함께 구매하려는 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)로 전송될 수 있다.
- [0146] 이러한 과정에서 동영상을 공급한 사용자 단말 장치(200)의 공급기록, 구매하려는 사용자 단말 장치(200-1, 200-2, 200-3, 200-4, 200-5)의 구매이력 등이 모두 각 사용자 단말 장치(200, 200-1, 200-2, 200-3, 200-4, 200-5)의 분산원장 데이터에 저장될 수 있다.
- [0147] 이상에서는 본 발명의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

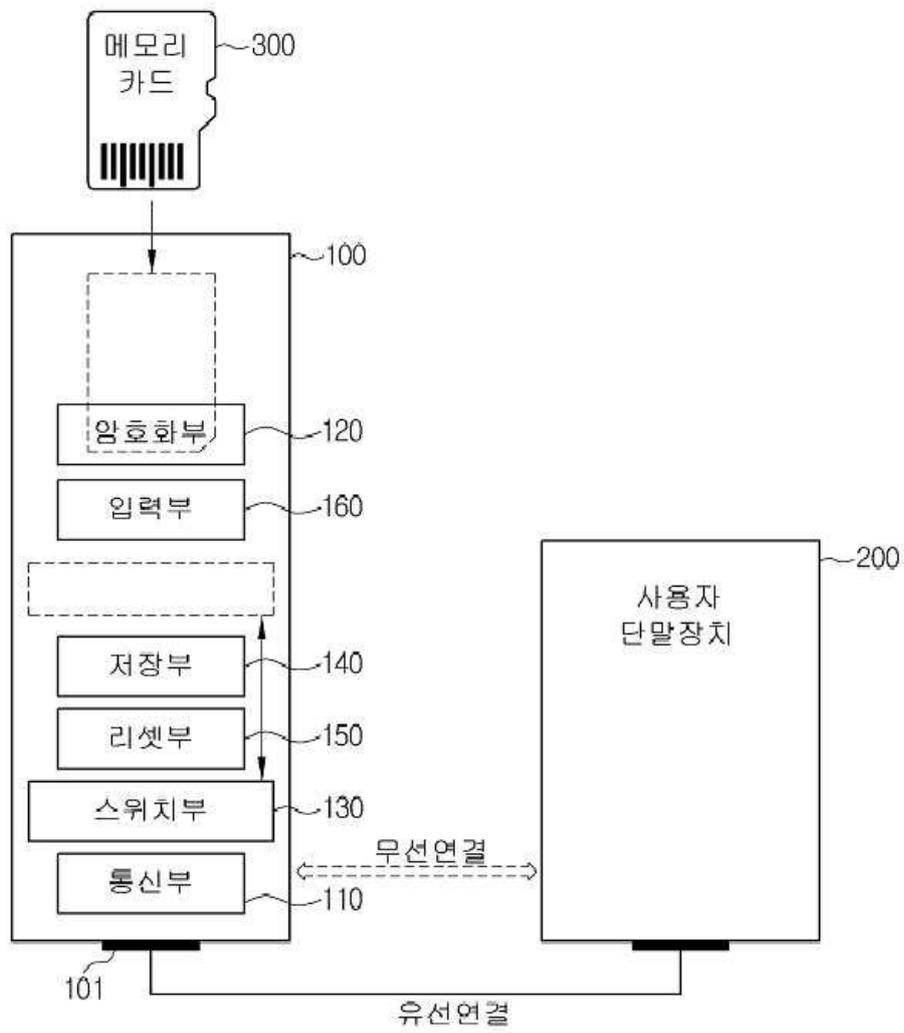
- [0148] 100 : 콘텐츠 월렛 장치
- 110 : 통신부
- 120 : 암호화부
- 130 : 스위치부
- 140 : 저장부
- 150 : 리셋부
- 160 : 입력부
- 200 : 사용자 단말 장치
- 300 : 저장장치

도면

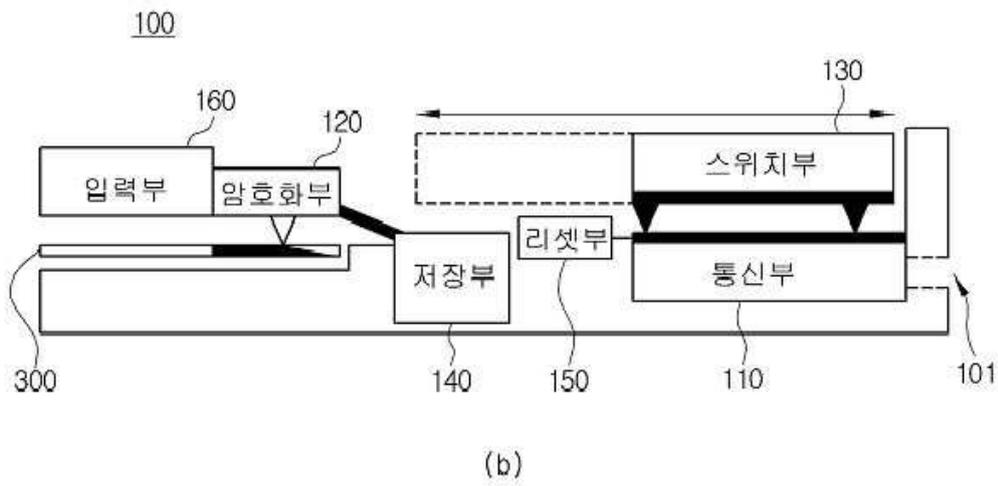
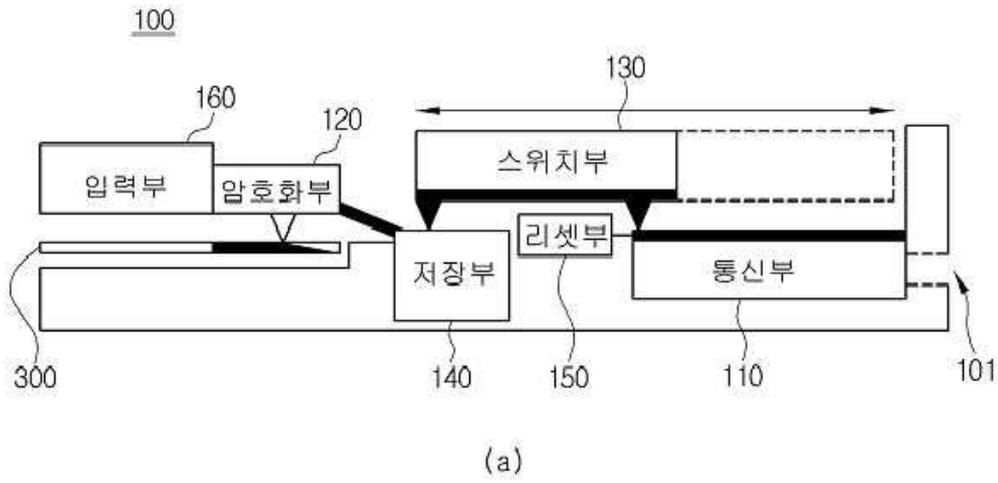
도면1



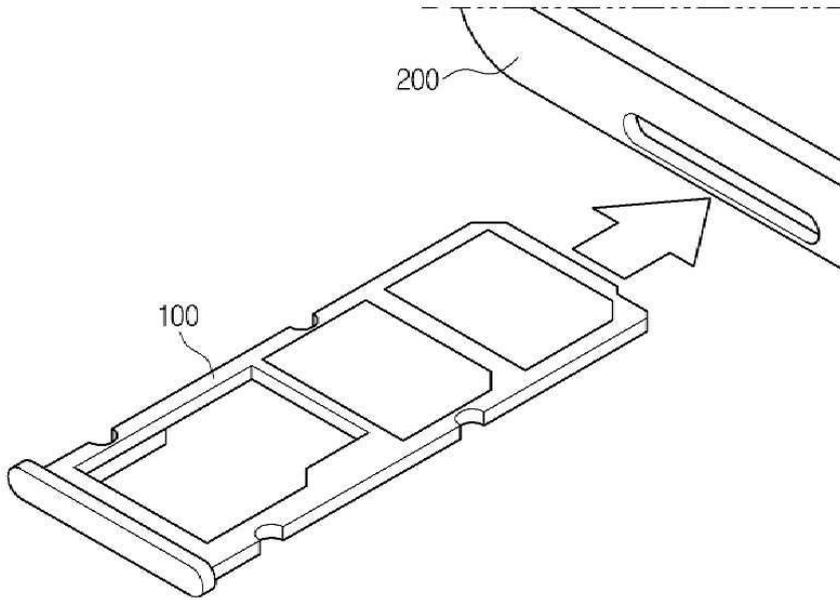
도면2



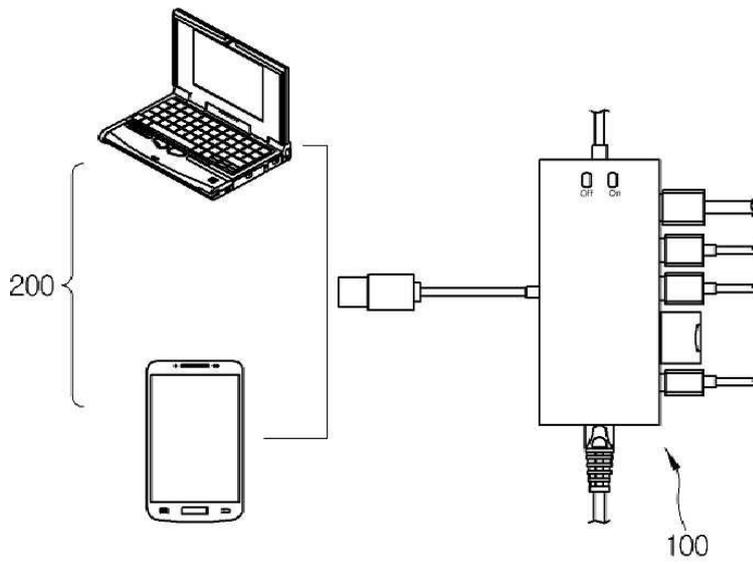
도면3



도면4

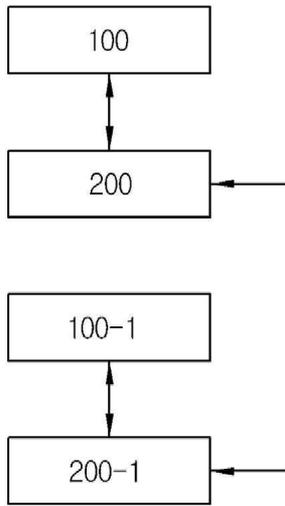


도면5

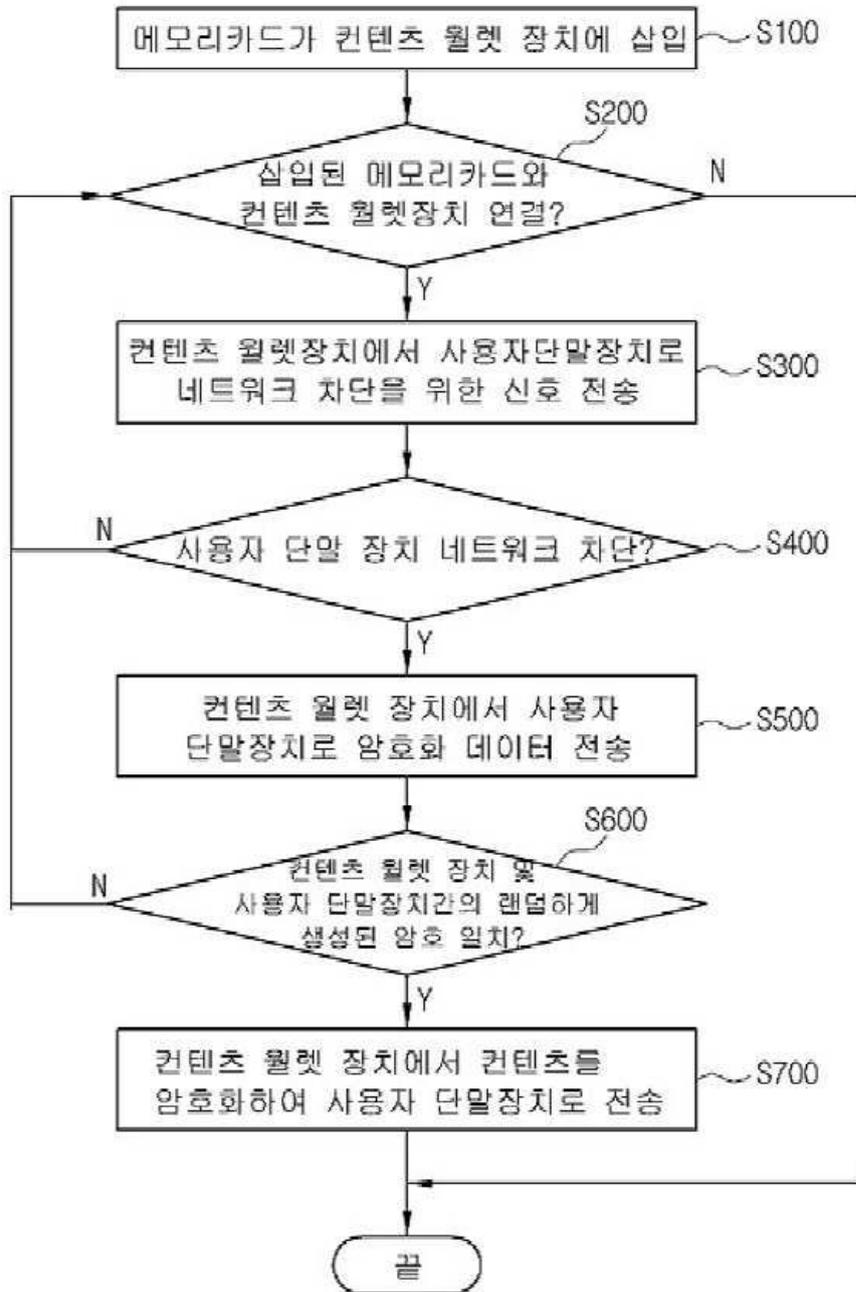


도면6

10



도면7



도면8

