(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년09월24일
(11) 등록번호 10-2708156
(24) 등록일자 2024년09월12일

(51) 국제특허분류(Int. Cl.)
B42D 25/24 (2014.01) *B42D 25/21* (2014.01)
B42D 25/28 (2014.01) *B42D 25/305* (2014.01)
B42D 25/405 (2014.01) *B42D 25/48* (2014.01)
G06K 19/10 (2006.01) *G07D 7/00* (2019.01)
G07D 7/0043 (2016.01) *G07D 7/0047* (2016.01)
G09F 3/00 (2006.01)
(52) CPC특허분류
B42D 25/24 (2015.01)
B42D 25/21 (2015.01)
(21) 출원번호 10-2021-7004107
(22) 출원일자(국제) 2019년06월03일
심사청구일자 2022년05월03일
(85) 번역문제출일자 2021년02월09일
(65) 공개번호 10-2021-0031488
(43) 공개일자 2021년03월19일
(86) 국제출원번호 PCT/EP2019/064359
(87) 국제공개번호 WO 2020/011447
국제공개일자 2020년01월16일
(30) 우선권주장
18182697.5 2018년07월10일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
KR1020190094441 A
JP2020515099 A
US20150052615 A1
US20180174157 A1

(73) 특허권자
시크파 홀딩 에스에이
스위스 씨에이치-1008 프릴리 아브뉘 드 플로리상 트 41
(72) 발명자
드꾸, 에릭
스위스 1800 브베 루 드 쥐라 8
질렛, 필리페
스위스 1009 풀리 슈망 드 투어론드 6
(뒷면에 계속)
(74) 대리인
특허법인 광장리앤고

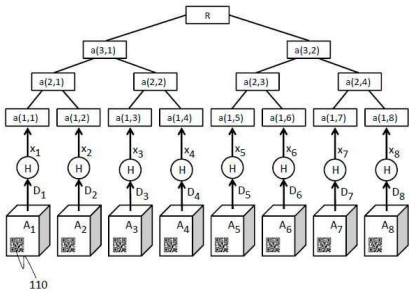
전체 청구항 수 : 총 26 항 심사관 : 정원식

(54) 발명의 명칭 **물품 위조 방지 보호**

(57) 요 약

발명은 물품을 그 연관된 데이터, 특히 물품이 특정 배치에 속하는 것과 관련된 데이터의 위조 및 변조에 대하여 보호하는 것에 관한 것으로서, 보호된 물품의 진정성 및 그 연관된 데이터의 정품 물품의 것에 대한 적합성의 오프라인 및 온라인 검사를 가능하게 한다.

대 표 도 - 도1



(52) CPC특허분류
B42D 25/28 (2015.01)
B42D 25/305 (2015.01)
B42D 25/405 (2015.01)
B42D 25/48 (2015.01)
G06K 19/10 (2021.01)
G07D 7/003 (2017.05)
G07D 7/0043 (2017.05)
G07D 7/0047 (2017.05)
G09F 3/00 (2013.01)
(72) 발명자
데포츠, 필리페
스위스 1305 펜탈라즈 루트 드 데일런스 9
월리스, 엘리자베스
스위스 1009 풀리 슈망 드 라 다마타일 22

명 세 서

청구범위

청구항 1

복수의 원본 물품의 배치(batch)에 속하는 특정한(given) 원본 물품을 위조 또는 변조에 대해 보호하는 방법에 있어서, 각 원본 물품은 그 자체의 연관된 물품 데이터 및 대응하는 물품 디지털 데이터를 가지며, 상기 방법은:

상기 배치의 각 원본 물품에 대하여, 단방향 함수를 사용하여 그 대응하는 물품 디지털 데이터의 연관된 물품 디지털 서명을 계산하는 단계;

상기 배치의 상기 원본 물품에 대한 복수의 계산된 물품 디지털 서명에 기반하고 트리 내의 주어진(given) 노드 순서에 따라 배열된 노드를 포함하는 트리를 형성하는 단계-상기 트리는, 상기 배치 내의 상기 복수의 원본 물품과 각각 연관된 상기 복수의 물품 디지털 서명에 대응하는, 상기 트리의 리프 노드로부터 루트 노드까지의 노드 수준을 포함하며, 상기 트리의 모든 비-리프 노드는 트리 연결 순서에 따라 그 자식 노드의 각 디지털 서명의 연결의 단방향 함수에 의한 디지털 서명에 대응하고, 상기 루트 노드는 상기 트리 연결 순서에 따라 상기 트리 내의 끝에서 두 번째 노드 수준의 노드의 디지털 서명의 연결의 단방향 함수에 의한 디지털 서명인 기준 루트 디지털 서명에 대응함;

상기 특정한 원본 물품에, 상기 리프 노드 수준부터 상기 끝에서 두 번째 노드 수준까지, 상기 특정한 원본 물품의 상기 물품 디지털 서명에 대응하는 상기 리프 노드와 동일한 부모 노드를 갖는 상기 트리 내의 모든 다른 리프 노드, 및 상기 트리 내의 각 다음 수준에서 연속적으로, 이전 수준에서 고려된 이전 동일한 부모 노드와 동일한 부모 노드를 갖는 상기 트리 내의 모든 비-리프 노드의 각 디지털 서명의 시퀀스인, 대응하는 검증 키를 연관시키는 단계;

상기 트리의 상기 기준 루트 디지털 서명을 사용자에게 제공하는 단계; 및

상기 특정한 원본 물품 상에 그 대응하는 물품 디지털 데이터 및 그 대응하는 검증 키의 표현을 포함하는 기계 판독 가능 보안 표지를 적용하여,

물품 데이터가 위조 또는 변조로부터 보호되는 표시된 원본 물품을 획득하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서, 상기 트리의 상기 루트 노드의 상기 기준 루트 디지털 서명은 상기 사용자가 접근할 수 있는 매체에 게시되거나, 상기 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장되거나, 상기 사용자가 접근할 수 있는 블록체인, 또는 블록체인에 의해 보호되는 데이터베이스에 저장되는 방법.

청구항 3

제2항에 있어서, 상기 표시된 원본 물품은 그에 표시되며 상기 사용자가 원본 물품의 상기 배치에 대응하는 상기 트리의 상기 루트 노드의 상기 기준 루트 디지털 서명에 접근할 수 있도록 하는 정보를 포함하는 루트 노드 접근 데이터를 더 포함하며, 상기 정보는 상기 사용자로부터 표시된 원본 물품의 보안 표지로부터 획득된 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 루트 요청을 수신하고, 대응하는 트리의 기준 루트 디지털 서명을 반송하도록 작동 가능한 접근 인터페이스로의 링크이고, 상기 접근 인터페이스는, 각각:

- 상기 기준 루트 디지털 서명이 게시된 상기 매체;

- 상기 기준 루트 디지털 서명이 저장된 상기 검색 가능한 루트 데이터베이스; 및

- 타임스탬프된 상기 기준 루트 디지털 서명이 저장되는 상기 블록체인, 또는 블록체인에 의해 각각 보호되는 데이터베이스 중 하나로의 접근을 허용하는 방법.

청구항 4

제1항에 있어서,

가상 물품이 원본 물품의 상기 배치에 속하는 것으로 계산되고, 상기 가상 물품은 연관된 가상 물품 데이터 및 그 대응하는 가상 물품 디지털 데이터, 및 상기 가상 물품 디지털 데이터의 단방향 함수를 사용하여 획득되는 연관된 가상 물품 디지털 서명을 가지며, 상기 가상 물품은 제조되지 않고 상기 연관된 가상 물품 디지털 서명을 생성하기 위해서만 사용되고;

원본 물품의 상기 배치와 연관된 상기 기준 루트 디지털 서명이, 리프 노드로서, 상기 가상 물품 디지털 서명을 포함하여, 상기 배치의 상기 원본 물품의 모든 상기 물품 디지털 서명을 갖는 트리로부터 계산되는 방법.

청구항 5

제1항에 있어서,

상기 표시된 원본 물품과 연관된 상기 물품 디지털 데이터에 대응하는 추가적인 물품 디지털 데이터가, 표시된 원본 물품의 보안 표지로부터 획득되는 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 정보 요청을 상기 사용자로부터 수신하고, 대응하는 추가적인 물품 디지털 데이터를 반송하도록 작동할 수 있는 정보 데이터베이스 인터페이스를 통해 상기 사용자가 접근할 수 있는 검색 가능한 정보 데이터베이스에 저장되는 방법.

청구항 6

제5항에 있어서, 상기 표시된 원본 물품과 연관된 상기 물품 디지털 데이터에 대응하는 상기 추가적인 물품 디지털 데이터는 상기 물품 디지털 데이터와 연결되는 방법.

청구항 7

제1항에 있어서, 상기 표시된 원본 물품의 상기 물품 디지털 데이터는 상기 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 고유한 물리적 특성의 대응하는 기준 특성 디지털 데이터를 포함하는 방법.

청구항 8

제7항에 있어서, 상기 표시된 원본 물품의 상기 고유한 물리적 특성은 상기 원본 물품 상에, 또는 연관된 객체 상에 적용된 물질 기반 보안 표지의 것인 방법.

청구항 9

제1항에 있어서, 상기 배치의 상기 각 원본 물품의 상기 물품 디지털 데이터는 상기 배치의 모든 상기 물품에 대해 공통인 주어진 필드 사이에 분산되고, 이들 필드에 관련된 디지털 데이터는 상기 물품 디지털 데이터에 포함되지 않고 상기 배치와 연관된 별도의 필드 데이터 블록에 모아지며,

i) 원본 물품의 상기 물품 디지털 서명이 상기 대응하는 물품 디지털 데이터 및 상기 필드 데이터 블록의 상기 디지털 데이터의 연결의 단방향 함수로 계산되고;

ii) 상기 기준 루트 디지털 서명이 상기 연관된 필드 데이터 블록과 함께 상기 사용자에게 제공되는 방법.

청구항 10

제1항의 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 진정성, 또는 그러한 물품의 사본의 적합성을 검증하는 방법에 있어서, 상기 물품 또는 상기 물품의 상기 사본인 시험 객체를 볼 때, 상기 방법은:

이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치에 의해 상기 시험 객체 상의 보안 표지의 디지털 이미지를 획득하는 단계;

상기 시험 객체 상의 상기 보안 표지의 상기 획득된 디지털 이미지 상의 물품 디지털 데이터 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 시험 검증 키를 추출하는 단계;

상기 메모리에 원본 물품의 상기 배치의 트리의 루트 노드의 기준 루트 디지털 서명을 저장하고, 상기 처리 유닛에 디지털 데이터의 및 상기 트리 내의 노드 순서 및 상기 트리 연결 순서에 따른 디지털 서명의 연결의 디지

털 서명을 계산하는 단방향 함수를 프로그래밍하는 단계;

상기 추출된 시험 물품 디지털 데이터 및 연관된 시험 검증 키가 실제로 상기 저장된 기준 루트 디지털 서명과 일치하는지 다음의 단계들을 수행하여 검증하는 단계:

상기 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 상기 시험 객체 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 상기 시험 리프 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고 상기 시험 디지털 서명 및 상기 모든 다른 리프 노드의 상기 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리 내의 각 다음 수준에서 연속적으로 상기 끝에서 두 번째 노드 수준까지, 상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리의 상기 끝에서 두 번째 노드 수준에 대응하는 상기 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 트리의 상기 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

상기 획득된 후보 루트 디지털 서명이 상기 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계를 포함하고,

상기 루트 디지털 서명이 일치하면, 상기 시험 객체 상의 상기 물품 데이터가 정품 물품의 것인 방법.

청구항 11

제10항에 있어서, 상기 표시된 원본 물품은 제9항의 방법에 따라 보호되고, 상기 처리 유닛의 상기 메모리는 상기 연관된 필드 데이터 블록을 더 저장하며,

상기 시험 객체 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 상기 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터 및 저장된 필드 데이터 블록의 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함하는 방법.

청구항 12

제10항에 있어서, 상기 물품은 제2항의 방법에 따라 상기 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스 내에 상기 기준 루트 디지털 서명을 저장함으로써 보호되고, 상기 영상장치는 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하며,

상기 통신 유닛을 사용하여 상기 통신 링크를 통하여 상기 루트 데이터베이스로 요청을 송신하고, 상기 기준 루트 디지털 서명을 수신하고;

상기 수신된 루트 디지털 서명을 상기 영상장치의 상기 메모리 내에 저장하는 예비 단계를 포함하는 방법.

청구항 13

제10항에 있어서, 상기 트리의 상기 루트 노드의 상기 기준 루트 디지털 서명은 상기 사용자가 접근할 수 있는 매체에 게시되거나, 상기 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장되거나, 상기 사용자가 접근할 수 있는 블록체인, 또는 블록체인에 의해 보호되는 데이터베이스에 저장되고, 상기 표시된 원본 물품은 그에 표시되며 상기 사용자가 원본 물품의 상기 배치에 대응하는 상기 트리의 상기 루트 노드의 상기 기준 루트 디지털 서명에 접근할 수 있도록 하는 정보를 포함하는 루트 노드 접근 데이터를 더 포함하며, 상기 정보는 상기 사용자로부터 표시된 원본 물품의 보안 표지로부터 획득된 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 루트 요청을 수신하고, 대응하는 트리의 기준 루트 디지털 서명을 반송하도록 작동 가능한 접근 인터페이스로의 링크이고, 상기 접근 인터페이스는, 각각:

- 상기 기준 루트 디지털 서명이 게시된 상기 매체;

- 상기 기준 루트 디지털 서명이 저장된 상기 검색 가능한 루트 데이터베이스; 및

- 타임스탬프된 상기 기준 루트 디지털 서명이 저장되는 상기 블록체인, 또는 블록체인에 의해 각각 보호되는 데이터베이스 중 하나로의 접근을 허용하고, 상기 영상장치는 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하며,

상기 영상장치로 상기 시험 객체 상에 표시된 상기 루트 노드 접근 데이터를 판독하고;

상기 통신 유닛을 사용하여 상기 통신 링크를 통하여 상기 시험 객체 상의 상기 보안 표지로부터 획득된 상기 물품 디지털 데이터, 또는 상기 물품 디지털 데이터의 디지털 서명을 포함하는 루트 요청을 상기 접근 인터페이스로 송신하고, 연관되는 배치의 대응하는 기준 루트 디지털 서명을 수신하며;

상기 수신된 기준 루트 디지털 서명을 상기 영상장치의 상기 메모리 내에 저장하는 예비 단계를 포함하는 방법.

청구항 14

제10항에 있어서, 상기 표시된 원본 물품과 연관된 상기 물품 디지털 데이터에 대응하는 추가적인 물품 디지털 데이터가, 표시된 원본 물품의 보안 표지로부터 획득되는 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 정보 요청을 상기 사용자로부터 수신하고, 대응하는 추가적인 물품 디지털 데이터를 반송하도록 작동할 수 있는 정보 데이터베이스 인터페이스를 통해 상기 사용자가 접근할 수 있는 검색 가능한 정보 데이터베이스에 저장되고, 상기 영상장치는 상기 시험 객체 상의 상기 보안 표지로부터 획득된 물품 디지털 데이터, 또는 대응하는 물품 디지털 서명 데이터를 포함하는 정보 요청을 상기 정보 데이터베이스 인터페이스로 송신하고, 대응하는 추가적인 물품 디지털 데이터를 수신하도록 작동할 수 있는 통신 수단을 더 구비하는 방법.

청구항 15

제10항에 있어서, 상기 물품은 제7항의 방법에 따라 보호되고, 상기 영상장치는 각각 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 고유한 물리적 특성을 검출하도록 작동할 수 있는 센서를 더 구비하고, 상기 처리 유닛은 상기 센서로부터 수신된 검출 신호로부터 대응하는 특성 디지털 데이터를 추출하도록 프로그래밍되고, 상기 영상장치는 상기 메모리 내에 각각 상기 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 상기 고유한 물리적 특성에 대응하는 기준 특성 디지털 데이터 CDD를 저장하고, 상기 물품 또는 상기 연관된 객체 또는 개인인 대상을 볼 때, 상기 방법은:

상기 센서로 상기 대상의 고유한 물리적 특성을 검출하고 대응하는 후보 특성 디지털 데이터 CDD^c를 추출하는 단계;

상기 획득한 후보 특성 디지털 데이터 CDD^c를 상기 저장된 기준 특성 디지털 데이터 CDD와 비교하는 단계를 더 포함하며;

상기 후보 특성 디지털 데이터 CDD^c가 상기 저장된 기준 특성 디지털 데이터 CDD로부터 사전 정의된 공차 기준 이내에 있다면, 상기 대상은 각각 정품 물품, 또는 정품 물품과 유효하게 연관된 객체 또는 개인과 대응하는 것으로 간주되는 방법.

청구항 16

제1항의 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여 물품의 물품 디지털 이미지의 적합성을 검증하는 방법에 있어서, 상기 방법은:

이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치에 의해 상기 물품 상의 보안 표지를 나타내는 물품 디지털 이미지를 획득하는 단계;

상기 보안 표지의 상기 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 연관된 시험 검증 키를 추출하는 단계;

상기 메모리에 원본 물품의 상기 배치의 트리의 루트 노드의 기준 루트 디지털 서명을 저장하고, 상기 처리 유닛에 디지털 데이터의 및 상기 트리 내의 노드 순서 및 상기 트리 연결 순서에 따른 디지털 서명의 연결의 디지

털 서명을 계산하는 단방향 함수를 프로그래밍하는 단계;

상기 추출된 시험 물품 디지털 데이터 및 시험 검증 키가 실제로 상기 저장된 기준 루트 디지털 서명과 일치하는지 다음의 단계들을 수행하여 검증하는 단계:

상기 단방향 함수를 사용하여 상기 추출된 시험 물품 디지털 데이터의 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 상기 물품 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 상기 시험 리프 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 상기 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리 내의 각 다음 수준에서 연속적으로 상기 끝에서 두 번째 노드 수준까지, 상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리의 상기 끝에서 두 번째 노드 수준에 대응하는 상기 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 트리의 상기 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

상기 획득된 후보 루트 디지털 서명이 상기 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계를 포함하고,

상기 루트 디지털 서명이 일치하면, 상기 물품 디지털 이미지가 정품 표시된 원본 물품의 것인 방법.

청구항 17

제16항에 있어서, 상기 표시된 원본 물품은 제9항의 방법에 따라 보호되고, 상기 처리 유닛의 상기 메모리는 상기 연관된 필드 데이터 블록을 더 저장하며,

상기 물품 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 단방향 함수를 사용하여 상기 추출된 시험 물품 디지털 데이터 및 상기 저장된 필드 데이터 블록의 상기 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함하는 방법.

청구항 18

제16항에 있어서, 상기 원본 물품은 제2항의 방법에 따라 상기 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스 내에 상기 기준 루트 디지털 서명을 저장함으로써 보호되고, 상기 영상장치는 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하며,

상기 통신 유닛을 사용하여 상기 통신 링크를 통하여 상기 루트 데이터베이스로 요청을 송신하고, 상기 기준 루트 디지털 서명을 수신하고;

상기 수신된 루트 디지털 서명을 상기 영상장치의 상기 메모리 내에 저장하는 예비 단계를 포함하는 방법.

청구항 19

제16항에 있어서, 상기 원본 물품은 제7항의 방법에 따라 보호되고, 상기 영상장치는 각각 표시된 원본 물품과 연관된 객체 또는 개인의 고유한 물리적 특성을 검출하도록 작동할 수 있는 센서를 더 구비하고, 상기 처리 유닛은 상기 센서로부터 수신된 검출 신호로부터 대응하는 특성 디지털 데이터를 추출하도록 프로그래밍되고, 상기 영상장치는 상기 메모리 내에 각각 연관된 객체 또는 개인의 상기 고유한 물리적 특성에 대응하는 기준 특성 디지털 데이터 CDD를 저장하고, 상기 연관된 객체 또는 개인인 대상을 볼 때, 상기 방법은:

상기 센서로 상기 대상의 고유한 물리적 특성을 검출하고 대응하는 후보 특성 디지털 데이터 CDD^c를 추출하는 단계;

상기 획득한 후보 특성 디지털 데이터 CDD^c를 상기 저장된 기준 특성 디지털 데이터 CDD와 비교하는 단계를 더 포함하고;

상기 후보 특성 디지털 데이터 CDD^c가 상기 저장된 기준 특성 디지털 데이터 CDD로부터 사전 정의된 공차 기준 이내에 있다면, 상기 대상은 정품 표시된 원본 물품과 유효하게 연관된 객체 또는 개인과 각각 대응하는 것으로 간주되는 방법.

청구항 20

복수의 원본 물품의 배치에 속하고 제1항 내지 제9항 중 어느 한 항의 방법에 따라 위조 및 변조에 대해 보호되는 물품에 있어서, 상기 배치의 각 원본 물품은 그 자체의 물품 디지털 데이터 및 대응하는 검증 키를 가지고, 상기 배치는 대응하는 기준 루트 디지털 서명을 가지며:

상기 물품 위에 적용되며 그 물품 디지털 데이터 및 그 검증 키의 표현을 포함하는 기계 판독 가능한 보안 표지를 포함하는 물품.

청구항 21

제20항에 있어서, 상기 물품의 상기 물품 디지털 데이터는 상기 물품의, 또는 연관된 객체 또는 개인의 대응하는 고유한 물리적 특성의 기준 특성 디지털 데이터 CDD를 포함하는 물품.

청구항 22

제21항에 있어서, 상기 물품의 상기 고유한 물리적 특성은 상기 물품에 적용된 물질 기반 보안 표지의 것인 물품.

청구항 23

제1항의 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 진정성, 또는 그러한 물품의 사본의 적합성을 검증하는 시스템에 있어서, 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치를 포함하고, 상기 메모리는 원본 물품의 상기 배치에 대응하는 트리의 기준 루트 디지털 서명을 저장하고, 상기 처리 유닛에는 디지털 데이터의 및 상기 트리 내의 노드 순서 및 상기 트리 연결 순서에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수가 프로그래밍되며, 상기 시스템은:

상기 영상장치로 상기 물품 또는 상기 물품의 상기 사본인 시험 객체 상의 보안 표지의 디지털 이미지를 획득하고;

상기 영상장치로 상기 시험 객체 상의 상기 보안 표지의 상기 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 시험 검증 키를 추출하고;

상기 추출된 시험 물품 디지털 데이터 및 연관된 검증 키가 실제로 상기 저장된 기준 루트 디지털 서명과 일치하는지 상기 처리 유닛 상에서 더 프로그래밍된 다음의 단계들을 수행함으로써 검증하도록 작동 가능하고:

상기 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 계산된 디지털 서명으로부터 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 상기 시험 객체 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 상기 시험 리프 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 상기 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리 내의 각 다음 수준에서 연속적으로 상기 끝에서 두 번째 노드 수준까지, 상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리의 상기 끝에서 두 번째 노드 수준에 대응하는 상기 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 트리의 상기 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

상기 획득된 후보 루트 디지털 서명이 상기 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

상기 루트 디지털 서명이 일치하면, 상기 시스템이 상기 시험 객체 상의 상기 물품 데이터가 정품 물품의 것이라는 표시를 전달하도록 구성되는 시스템.

청구항 24

제23항에 있어서, 상기 표시된 원본 물품은 제9항의 방법에 따라 보호되고, 상기 처리 유닛의 상기 메모리는 상기 연관된 필드 데이터 블록을 더 저장하며,

상기 시험 객체 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 상기 단방향 함수를 사용하여 상기 추출된 시험 물품 디지털 데이터 및 상기 저장된 필드 데이터 블록의 상기 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함하는 시스템.

청구항 25

제1항의 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 물품 디지털 이미지의 적합성을 검증하는 시스템에 있어서, 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치를 포함하고, 상기 메모리는 원본 물품의 상기 배치에 대응하는 트리의 기준 루트 디지털 서명을 저장하고, 상기 처리 유닛에는 디지털 데이터의 및 상기 트리 내의 노드 순서 및 상기 트리 연결 순서에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수가 프로그래밍되며, 상기 시스템은:

상기 영상장치를 사용하여 상기 물품 상의 보안 표지를 나타내는 물품 디지털 이미지를 획득하고;

상기 영상장치를 사용하여 상기 보안 표지의 상기 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 연관된 시험 검증 키를 추출하고;

상기 추출된 시험 물품 디지털 데이터 및 시험 검증 키가 실제로 상기 저장된 기준 루트 디지털 서명과 일치하는지 상기 처리 유닛 상에서 더 프로그래밍된 다음의 단계들을 수행함으로써 검증하도록 작동 가능하고:

상기 단방향 함수를 사용하여 상기 추출된 시험 물품 디지털 데이터의 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 상기 물품 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 상기 시험 리프 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 상기 시험 디지털 서명 및 상기 모든 다른 리프 노드의 상기 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리 내의 각 다음 수준에서 연속적으로 상기 끝에서 두 번째 노드 수준까지, 상기 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 상기 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

상기 시험 트리의 상기 끝에서 두 번째 노드 수준에 대응하는 상기 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 시험 트리의 상기 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

상기 획득된 후보 루트 디지털 서명이 상기 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

상기 루트 디지털 서명이 일치하면, 상기 시스템이 상기 물품 디지털 이미지가 정품 표시된 원본 물품의 것이라

는 표시를 전달하도록 구성되는 시스템.

청구항 26

제25항에 있어서, 상기 표시된 원본 물품은 제9항의 방법에 따라 보호되고, 상기 처리 유닛의 상기 메모리는 상기 연관된 필드 데이터 블록을 더 저장하며,

상기 물품 상의 상기 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 상기 단방향 함수를 사용하여 상기 추출된 시험 물품 디지털 데이터 및 상기 저장된 필드 데이터 블록의 상기 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함하는 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 물품 및 그러한 물품에 표시된 데이터에 대한 위조 또는 변조로부터의 보호, 및 그러한 표시된 물품의 디지털 이미지의 원본과의 적합성과 물품의 추적 가능성의 기술 분야에 관한 것이다.

배 경 기 술

[0002] 기계 부품, 전자 구성품, 약품 및 수많은 다른 물품에서 위조 및 변조의 문제는 잘 알려져 있고, 심각하며, 증가하고 있다. 또한 물품과 연관된 데이터의 변조도 심각한 문제이다. 신분증이나 졸업장(물품)과 같은 원본 인쇄 문서에 표시된 데이터를 위조하는 예는 잘 알려져 있으며, 원본(아마도 정품) 문서의 디지털 사본이나 복사본을 고려하면 문제는 더욱 심각하다. 일련번호와 같은 식별자를 추적하는 것은 일반적으로 불충분한 대응인데, 위조자가 이러한 번호 또한 쉽게 복제할 수 있기 때문이다.

[0003] 제조 물품에 대한 다른 많은 보안 체계가 있지만 일반적으로 충분한 수준의 보안을 제공하지 않고, 저장 및 접근하여야 하는 정보의 측면에서 관리 오버헤드가 너무 높으며, 잘 제어된 환경에서 사용하는 것을 제외하고는 종종 비실용적이거나, 또는 단순히 물리적으로 구현되지 않는다. 예를 들어, 문서를 검증 가능한 방식으로 디지털로 보호하기 위한 많은 체계는 많은 물리적인 품목을 수반하는 상황에서 사용하기에 적합하지 않으며 이들에 대응하는 서명들로 표시하는 것이 비실용적이거나 다른 의미에서 바람직하지 않다.

[0004] 물품의 진정성을 보장하거나 연관된 데이터를 보호하기 위한 대부분의 기존 방법의 또 다른 단점은, 예를 들어, 생산 배치(batch)와 같이 잘 정의된 그룹의 일부인 경우에도 물품을 별개로 보는 경향이 있다는 점이다. 이는 중요한 인증 정보를 무시한다.

[0005] 물품을 보호하는 기존의 방법은 그 위에 물질 기반 보안 표지(조작 방지 가능), 즉 재현하기 매우 어려운(불가능하지는 않지만) 검출 가능한 고유한 물리적 또는 화학적 특성을 갖는 표지를 적용하는 것이다. 적절한 센서가 표지에서 이 고유한 특성을 감지하면, 이 표지는 높은 수준의 신뢰도로 정품으로 간주되고, 이에 따라 대응하는 표시된 물품 또한 그렇게 간주된다. 이러한 알려진 인증 고유 특성의 많은 예가 있다. 표지는 무작위로 분산될 수 있는 일부 입자를 포함할 수 있거나, 고유한 광학 반사 또는 투과 또는 흡수 또는 심지어 방출(발광, 예를 들어, 또는 편광 또는 회절 또는 간섭…) 특성을 갖는 특정한 층 구조를 가질 수 있으며, 특정 스펙트럼 내용의 "빛"으로 특정 조명 조건에서 감지될 수 있다. 이 고유한 특성은 표지 물질의 특정한 화학적 조성으로 인해 발생할 수 있다. 예를 들어, 발광 안료(시판되지 않을 수 있음)는 물품에 일부 패턴을 인쇄하는 데 사용되는 잉크에 분산될 수 있으며 특정한 빛(예를 들어, UV 스펙트럼 범위의 빛)으로 조명할 때 특정한 빛(예를 들어, 적외선 범위 내의 스펙트럼 윈도우 내의)을 방출하는 데 사용된다. 예를 들어 이는 지폐를 보호하는 데 사용된다. 다른 고유한 특성을 사용할 수도 있다. 예를 들어, 표지 내의 발광 입자는 적절한 여기 광 펄스로 조명한 후 특정한 발광 방출 감쇠 시간을 가질 수 있다. 다른 유형의 고유한 특성은 포함된 입자의 자기 특성, 또는, 예를 들어, 충분한 해상도로 관찰할 때 고유한 특징적인 서명을 추출하는 역할을 할 수 있는, 문서의 특정한 영역에서 종이 기판의 본질적으로 무작위로 분산된 섬유의 상대적 위치와 같은 물품 자체의 "지문" 특성, 또는 충분히 확대하여 볼 때 고유한 서명으로 이어질 수 있는 물품에 인쇄된 데이터의 일부 무작위 인쇄 인공물 등이다. 물품의 고유한 지문 속성에 대한 주요 문제는 노화 또는 마모에 대한 강건성이다. 그러나 물질 기반 보안 표지가 표시된 물품과 연관된 데이터를 항상 보호할 수 있는 것은 아니다. 예를 들어, 문서의 일부 영역에 보안 잉크로 인쇄된 로고와 같은 물질 기반 보안 표지로 문서가 표시된 경우에도, 문서의 나머지 부분에 인쇄된 데이터는 여전히 위조될 수 있다. 또한, 너무 복잡한 인증 서명은 종종 외부 데이터베이스와 관련된 중요한 저장 기능과 그러한 데이터베이스에 질의하기 위한 통신 링크를 필요로 하여, 물품의 오프라인 인증이 불가능하다.

[0006] 따라서 본 발명의 목적은 연관된 데이터, 특히 특정 배치의 물품에 속하는 것과 관련된 데이터의 도용 및 위조로부터 물품을 보호하는 것이다. 본 발명의 다른 목적은 본 발명에 따라 보호되는 객체의 진정성 및 정품 보호된 객체의 데이터에 대해 그 연관된 데이터의 적합성에 대한 오프라인 검사를 허용하는 것이다.

발명의 내용

[0007] 일 양상에 따르면 발명은 복수의 원본 물품의 배치에 속하는 특정한 원본 물품을 위조 또는 변조에 대해 보호하는 방법에 관한 것으로서, 각 원본 물품은 그 자체의 연관된 물품 데이터 및 대응하는 물품 디지털 데이터를 가지며, 방법은:

[0008] - 배치의 각 원본 물품에 대하여, 단방향 함수를 사용하여 그 대응하는 물품 디지털 데이터의 연관된 물품 디지털 서명을 계산하는 단계;

[0009] - 배치의 원본 물품에 대한 복수의 계산된 물품 디지털 서명에 기반하고 트리 내의 주어진 노드 순서에 따라 배열된 노드를 포함하는 트리를 형성하는 단계-상기 트리는, 배치 내의 복수의 원본 물품과 각각 연관된 복수의 물품 디지털 서명에 대응하는, 트리의 리프 노드로부터 루트 노드까지의 노드 수준을 포함하며, 트리의 모든 비-리프 노드는 트리 연결 순서에 따라 그 자식 노드의 각 디지털 서명의 연결의 단방향 함수에 의한 디지털 서명에 대응하고, 루트 노드는 기준 루트 디지털 서명, 즉, 상기 트리 연결 순서에 따라 트리 내의 끝에서 두 번째 노드 수준의 노드의 디지털 서명의 연결의 단방향 함수에 의한 디지털 서명에 대응함;

[0010] - 특정한 원본 물품에, 리프 노드 수준부터 끝에서 두 번째 노드 수준까지, 특정한 원본 물품의 물품 디지털 서명에 대응하는 리프 노드와 동일한 부모 노드를 갖는 트리 내의 모든 다른 리프 노드, 및 트리 내의 각 다음 수준에서 연속적으로, 이전 수준에서 고려된 이전 동일한 부모 노드와 동일한 부모 노드를 갖는 트리 내의 모든 비-리프 노드의 각 디지털 서명의 시퀀스인, 대응하는 검증 키를 연관시키는 단계;

[0011] - 트리의 기준 루트 디지털 서명을 사용자에게 제공하는 단계; 및

[0012] - 특정한 원본 물품 상에 그 대응하는 물품 디지털 데이터 및 그 대응하는 검증 키의 표현을 포함하는 기계 판독 가능 보안 표지를 적용하여,

[0013] 물품 데이터가 위조 또는 변조로부터 보호되는 표시된 원본 물품을 획득하는 단계를 포함한다.

[0014] 트리의 루트 노드의 기준 루트 디지털 서명은 사용자가 접근할 수 있는 매체에 게시되거나, 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장되거나, 사용자가 접근할 수 있는 블록체인, 또는 블록체인에 의해 보호되는 데이터베이스에 저장될 수 있다.

[0015] 따라서, 발명에 따르면, 트리 구조 및 노드 값을 계산하기 위한 강건한 단방향 함수의 사용으로 인하여, 불변으로 만들어진 트리의 루트 디지털 서명과 함께 배치의 모든 물품의 물품 디지털 서명이 얽히고 대응하는 물품 상에 적용된 보안 표지 내에 물품 디지털 데이터 및 그 연관된 검증 키를 포함하여, 데이터의 변조 및 표시된 물품의 위조를 방지하면서 매우 높은 수준의 신뢰성으로 표시된 물품의 조사 및 추적을 가능하게 한다.

[0016] 표시된 원본 물품은 그에 표시되며 사용자가 원본 물품의 배치에 대응하는 트리의 루트 노드의 기준 루트 디지털 서명에 접근하기에 충분한 정보를 포함하는 루트 노드 접근 데이터를 더 포함할 수 있으며, 상기 정보는 사용자로부터 표시된 원본 물품의 보안 표지로부터 획득된 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 루트 요청을 수신하고, 대응하는 트리의 기준 루트 디지털 서명을 반송하도록 작동 가능한 접근 인터페이스로의 링크이고, 접근 인터페이스는, 각각:

[0017] - 기준 루트 디지털 서명이 게시된 매체;

[0018] - 기준 루트 디지털 서명이 저장된 검색 가능한 루트 데이터베이스; 및

[0019] - 타임스탬프된 기준 루트 디지털 서명이 저장되는 블록체인, 또는 블록체인에 의해 각각 보호되는 데이터베이스 중 하나로의 접근을 허용한다.

[0020] 발명에 따르면,

[0021] - 가상 물품이 원본 물품의 배치에 속하는 것으로 계산되고, 상기 가상 물품은 연관된 가상 물품 데이터 및 그 대응하는 가상 물품 디지털 데이터, 및 가상 물품 디지털 데이터의 단방향 함수를 사용하여 획득되는 연관된 가상 물품 디지털 서명을 가지며, 상기 가상 물품은 제조되지 않고 연관된 가상 물품 디지털 서명을 생성하기 위

해서만 사용되고;

[0022] - 원본 물품의 상기 배치와 연관된 기준 루트 디지털 서명이, 리프 노드로서, 가상 물품 디지털 서명을 포함하여, 배치의 원본 물품의 모든 물품 디지털 서명을 갖는 트리로부터 계산되는 것이 또한 가능하다.

[0023] 더 짧은 서명을 갖도록 단방향 함수는 해시 함수일 수 있고 원본 물품의 물품 디지털 서명은 대응하는 물품 디지털 데이터의 해시 값의 비트로부터 선택된 더 낮은 가중치의 특정한 복수의 비트의 시퀀스일 수 있다.

[0024] 위의 방법에서, 표시된 원본 물품과 연관된 물품 데이터에 대응하는 추가적인 물품 디지털 데이터가, 표시된 원본 물품의 보안 표지로부터 획득되는 물품 디지털 데이터, 또는 물품 디지털 데이터의 디지털 서명을 포함하는 정보 요청을 사용자로부터 수신하고, 대응하는 추가적인 물품 디지털 데이터를 반송하도록 작동할 수 있는 정보 데이터베이스 인터페이스를 통해 사용자가 접근할 수 있는 검색 가능한 정보 데이터베이스에 저장될 수 있다. 표시된 원본 물품과 연관된 물품 디지털 데이터에 대응하는 추가적인 물품 디지털 데이터는 상기 물품 디지털 데이터와 또한 연결될 수 있어, 추가적인 물품 디지털 데이터 또한 위조 또는 변조에 대해 보호된다.

[0025] 또한, 표시된 원본 물품은 그에 적용된 대응하는 물품 데이터 표지를 더 포함할 수 있으며, 상기 물품 데이터 표지는 상기 표시된 원본 물품과 연관된 대응하는 물품 데이터를 포함한다.

[0026] 표시된 원본 물품의 위에서 언급된 물품 디지털 데이터는 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 고유한 물리적 특성의 대응하는 기준 특성 디지털 데이터를 포함할 수 있다. 또한, 표시된 원본 물품의 고유한 물리적 특성은 원본 물품 상에, 또는 연관된 객체 상에 적용된 물질 기반 보안 표지의 것일 수 있다.

[0027] 위의 방법에서, 물품 보안 표지 내에 포함된 검증 키의 디지털 서명의 시퀀스는 트리 연결 순서에 의해 정의된 대응하는 노드의 순서와 구분되는 노드의 시퀀스 순서에 따라 배열될 수 있으며, 물품 보안 표지는 상기 시퀀스 순서와 연관된 순서 코드를 더 포함할 수 있다.

[0028] 발명에 따르면, 배치의 각 원본 물품의 물품 디지털 데이터는 배치의 모든 물품에 대해 공통인 주어진 필드 사이에 분산되는 경우, 이들 필드에 관련된 디지털 데이터는 물품 디지털 데이터에 포함되지 않을 수 있고 배치와 연관된 별도의 필드 데이터 블록에 모아질 수 있으며,

[0029] i) 원본 물품의 물품 디지털 서명이 대응하는 물품 디지털 데이터 및 필드 데이터 블록의 디지털 데이터의 연결의 단방향 함수로 계산되고;

[0030] ii) 기준 루트 디지털 서명이 연관된 필드 데이터 블록과 함께 사용자에게 제공된다.

[0031] 발명의 다른 양상은 위의 보호 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 진정성, 또는 그러한 물품의 사본의 적합성을 검증하는 방법에 관한 것으로서, 상기 물품 또는 물품의 상기 사본인 시험 객체를 볼 때, 방법은:

[0032] - 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치에 의해 시험 객체 상의 보안 표지의 디지털 이미지를 획득하는 단계;

[0033] - 시험 객체 상의 보안 표지의 획득된 디지털 이미지 상의 물품 디지털 데이터 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 시험 검증 키를 추출하는 단계;

[0034] - 메모리에 원본 물품의 배치의 트리의 루트 노드의 기준 루트 디지털 서명을 저장하고, 처리 유닛에 디지털 데이터의 및 트리 내의 노드 순서 및 트리 연결 방식에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수를 프로그래밍하는 단계;

[0035] - 추출된 시험 물품 디지털 데이터 및 연관된 시험 검증 키가 실제로 저장된 기준 루트 디지털 서명과 일치하는지 다음의 단계들을 수행하여 검증하여,

[0036] - 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

[0037] - 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 시험 리프 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0038] - 시험 트리 내의 각 다음 수준에서 연속적으로 끝에서 두 번째 노드 수준까지, 시험 검증 키 내의 디지털 서명

의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0039] - 시험 트리의 끝에서 두 번째 노드 수준에 대응하는 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 트리의 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

[0040] - 획득된 후보 루트 디지털 서명이 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

[0041] 상기 루트 디지털 서명이 일치하는 경우, 시험 객체 상의 물품 데이터가 정품 물품의 것이다.

[0042] 표시된 원본 물품이 위에서 언급된 별도의 필드 데이터 블록을 가지면서 보호되면, 처리 유닛의 메모리는 상기 연관된 필드 데이터 블록을 더 저장할 수 있으며, 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터 및 저장된 필드 데이터 블록의 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함할 수 있다.

[0043] 물품이 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스 내에 기준 루트 디지털 서명을 저장함으로써 보호되었으면, 영상장치는 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하며, 위의 검증 방법은:

[0044] - 통신 유닛을 사용하여 통신 링크를 통하여 상기 루트 데이터베이스로 요청을 송신하고, 기준 루트 디지털 서명을 수신하고;

[0045] - 수신된 루트 디지털 서명을 영상장치의 메모리 내에 저장하는 예비 단계를 포함할 수 있다.

[0046] 보호되는 물품이 위에서 설명한 루트 노드 접근 데이터를 포함하고, 영상장치는 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하는 경우, 위의 검증 방법은:

[0047] - 영상장치로 시험 객체 상에 표시된 루트 노드 접근 데이터를 판독하고;

[0048] - 통신 유닛을 사용하여 통신 링크를 통하여 시험 객체 상의 보안 표지로부터 획득된 물품 디지털 데이터, 또는 상기 물품 디지털 데이터의 디지털 서명을 포함하는 루트 요청을 상기 접근 인터페이스로 송신하고, 연관되는 배치의 대응하는 기준 루트 디지털 서명을 수신하며;

[0049] - 수신된 기준 루트 디지털 서명을 영상장치의 메모리 내에 저장하는 예비 단계를 포함할 수 있다.

[0050] 보호되는 물품은 위에서 설명한 추가적인 물품 디지털 데이터를 더 포함할 수 있으며, 영상장치는 시험 객체 상의 보안 표지로부터 획득된 물품 디지털 데이터, 또는 대응하는 물품 디지털 서명 데이터를 포함하는 정보 요청을 정보 데이터베이스 인터페이스로 송신하고, 대응하는 추가적인 물품 디지털 데이터를 수신하도록 작동할 수 있는 통신 수단을 더 구비할 수 있다.

[0051] 보호되는 물품이 위에서 설명한 물품 데이터 표지를 포함하면, 방법은:

[0052] - 영상장치로 시험 객체 상의 물품 데이터 표지 상에 표시된 물품 데이터를 판독하는 단계; 및

[0053] - 물품 데이터 표지로부터 판독된 물품 데이터가 시험 객체 상의 보안 표지로부터 추출된 물품 디지털 데이터에 대응하는지 확인하는 단계를 더 포함할 수 있다.

[0054] 또한, 보호되는 물품이 위에서 설명한 기준 특성 디지털 데이터를 포함하고, 영상장치는 각각 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 고유한 물리적 특성을 검출하도록 작동할 수 있는 센서를 더 구비하고, 처리 유닛은 센서로부터 수신된 검출 신호로부터 대응하는 특성 디지털 데이터를 추출하도록 프로그래밍되면, 영상장치는 메모리 내에 각각 표시된 원본 물품의, 또는 연관된 객체 또는 개인의 상기 고유한 물리적 특성에 대응하는 기준 특성 디지털 데이터 CDD를 저장하고, 상기 물품 또는 상기 연관된 객체 또는 개인인 대상을 볼 때, 위의 방법은:

[0055] - 센서로 대상의 고유한 물리적 특성을 검출하고 대응하는 후보 특성 디지털 데이터 CDD^c를 추출하는 단계;

[0056] - 획득한 후보 특성 디지털 데이터 CDD^c를 저장된 기준 특성 디지털 데이터 CDD와 비교하는 단계를 더 포함할 수 있으며;

[0057] - 특정한 공차 기준 내에서, 후보 특성 디지털 데이터 CDD^c가 저장된 기준 특성 디지털 데이터 CDD와 유사한 경우, 대상은 각각 정품 물품, 또는 정품 물품과 유효하게 연관된 객체 또는 개인과 대응하는 것으로 간주된다.

[0058] 발명의 추가 양상은 위에서 언급된 보호 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여 물품의 물품 디지털 이미지의 적합성을 검증하는 방법에 관한 것으로서, 방법은:

[0059] - 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치에 의해 물품 상의 보안 표지를 나타내는 물품 디지털 이미지를 획득하는 단계;

[0060] - 보안 표지의 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 연관된 시험 검증 키를 추출하는 단계;

[0061] - 메모리에 원본 물품의 배치의 트리의 루트 노드의 기준 루트 디지털 서명을 저장하고, 처리 유닛에 디지털 데이터의 및 트리 내의 노드 순서 및 트리 연결 순서에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수를 프로그래밍하는 단계;

[0062] - 추출된 시험 물품 디지털 데이터 및 시험 검증 키가 실제로 저장된 기준 루트 디지털 서명과 일치하는지 다음의 단계들을 수행하여 검증하여,

[0063] - 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

[0064] - 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 시험 리프 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0065] - 시험 트리 내의 각 다음 수준에서 연속적으로 끝에서 두 번째 노드 수준까지, 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0066] - 시험 트리의 끝에서 두 번째 노드 수준에 대응하는 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 트리의 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

[0067] - 획득된 후보 루트 디지털 서명이 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

[0068] 상기 루트 디지털 서명이 일치하는 경우, 물품 디지털 이미지가 정품 표시된 원본 물품의 것이다.

[0069] 보호되는 표시된 원본 물품의 배치가 위에서 설명한 바와 같이 연관된 필드 데이터 블록을 가지는 경우, 처리 유닛의 메모리는 연관된 필드 데이터 블록을 더 저장하며, 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터 및 저장된 필드 데이터 블록의 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함할 수 있다.

[0070] 원본 물품이 위에서 언급한 바와 같이 접근할 수 있는 검색 가능한 루트 데이터베이스 내에 기준 루트 디지털 서명을 저장함으로써 보호되었고, 영상장치가 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하면, 방법은:

[0071] - 통신 유닛을 사용하여 통신 링크를 통하여 상기 루트 데이터베이스로 요청을 송신하고, 기준 루트 디지털 서명을 수신하고;

[0072] - 수신된 루트 디지털 서명을 영상장치의 메모리 내에 저장하는 예비 단계를 포함할 수 있다.

[0073] 원본 물품이 위에서 언급한 루트 노드 접근 데이터를 포함하고, 영상장치가 통신 링크를 통하여 데이터를 송신 및 수신하도록 작동할 수 있는 통신 유닛을 더 구비하면, 방법은:

[0074] - 영상장치로 물품 디지털 이미지 상에 표시된 루트 노드 접근 데이터를 판독하고;

[0075] - 통신 유닛을 사용하여 통신 링크를 통하여 추출된 시험 물품 디지털 데이터, 또는 계산된 시험 디지털 서명을

포함하는 루트 요청을 접근 인터페이스로 송신하고, 원본 물품의 배치의 트리의 루트 노드의 기준 루트 디지털 서명을 수신하며;

[0076] - 수신된 기준 루트 디지털 서명을 영상장치의 메모리 내에 저장하는 예비 단계를 포함할 수 있다.

[0077] 표시된 원본 물품이 위에서 언급한 검색 가능한 정보 데이터베이스에 저장된 추가적인 물품 디지털 데이터와 연관되었으면, 영상장치는 시험 물품 디지털 데이터, 또는 시험 물품 디지털 서명 데이터를 포함하는 정보 요청을 정보 데이터베이스 인터페이스로 송신하고, 대응하는 추가적인 물품 디지털 데이터를 수신하도록 작동할 수 있는 통신 수단을 더 구비할 수 있다.

[0078] 보호되는 원본 물품이 위에서 언급한 기준 특성 디지털 데이터를 포함하고, 영상장치가 각각 표시된 원본 물품과 연관된 객체 또는 개인의 고유한 물리적 특성을 검출하도록 작동할 수 있는 센서를 더 구비하고, 처리 유닛이 센서로부터 수신된 검출 신호로부터 대응하는 특성 디지털 데이터를 추출하도록 프로그래밍된 경우, 영상장치는 메모리 내에 각각 연관된 객체 또는 개인의 상기 고유한 물리적 특성에 대응하는 기준 특성 디지털 데이터 CDD를 저장하고, 상기 연관된 객체 또는 개인인 대상을 볼 때, 방법은:

[0079] - 센서로 대상의 고유한 물리적 특성을 검출하고 대응하는 후보 특성 디지털 데이터 CDD^c를 추출하는 단계;

[0080] - 획득한 후보 특성 디지털 데이터 CDD^c를 저장된 기준 특성 디지털 데이터 CDD와 비교하는 단계를 더 포함할 수 있으며;

[0081] - 특정한 공차 기준 내에서, 후보 특성 디지털 데이터 CDD^c가 저장된 기준 특성 디지털 데이터 CDD와 유사한 경우, 대상은 정품 표시된 원본 물품과 유효하게 연관된 객체 또는 개인과 각각 대응하는 것으로 간주된다.

[0082] 발명의 다른 양상은 복수의 원본 물품의 배치에 속하고 위에서 언급된 보호 방법에 따라 위조 및 변조에 대해 보호되는 물품에 관한 것으로서, 배치의 각 원본 물품은 그 자체의 물품 디지털 데이터 및 대응하는 검증 키를 가지고, 상기 배치는 대응하는 기준 루트 디지털 서명을 가지며:

[0083] - 물품 위에 적용되며 그 물품 디지털 데이터 및 그 검증 키의 표현을 포함하는 기계 판독 가능한 보안 표지를 포함한다.

[0084] 위의 물품의 물품 디지털 데이터는 물품의, 또는 연관된 객체 또는 개인의 대응하는 고유한 물리적 특성의 기준 특성 디지털 데이터 CDD를 포함할 수 있다. 또한, 물품의 고유한 물리적 특성은 물품에 적용된 물질 기반 보안 표지의 것일 수 있다.

[0085] 발명의 다른 양상은 위에서 언급된 보호 방법에 따라 위조 또는 변조에 대하여 물질 및 디지털 이중 보호로 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 진정성, 또는 그러한 물품의 사본의 적합성을 검증하는 시스템에 관한 것으로서, 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치를 포함하고, 메모리는 원본 물품의 배치에 대응하는 트리의 기준 루트 디지털 서명을 저장하고, 처리 유닛에는 디지털 데이터의 및 트리 내의 노드 순서 및 트리 연결 순서에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수가 프로그래밍되며, 상기 시스템은:

[0086] - 영상장치로 상기 물품 또는 물품의 상기 사본인 시험 객체 상의 보안 표지의 디지털 이미지를 획득하고;

[0087] - 영상장치로 시험 객체 상의 보안 표지의 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 시험 검증 키를 추출하고;

[0088] - 추출된 시험 물품 디지털 데이터 및 연관된 검증 키가 실제로 저장된 기준 루트 디지털 서명과 일치하는지 처리 유닛 상에서 더 프로그래밍된 다음의 단계들을 수행함으로써 검증하도록 작동 가능하고,

[0089] - 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 계산된 디지털 서명으로부터 시험 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

[0090] - 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 시험 리프 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득

하는 단계;

[0091] - 시험 트리 내의 각 다음 수준에서 연속적으로 끝에서 두 번째 노드 수준까지, 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0092] - 시험 트리의 끝에서 두 번째 노드 수준에 대응하는 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 트리의 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

[0093] - 획득된 후보 루트 디지털 서명이 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

[0094] 상기 루트 디지털 서명이 일치하는 경우, 시스템이 시험 객체 상의 물품 데이터가 정품 물품의 것이라는 표시를 전달하도록 구성된다.

[0095] 표시된 원본 물품이 위에서 언급된 필드 데이터 블록을 가지면, 처리 유닛의 메모리는 연관된 필드 데이터 블록을 더 저장하며, 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험 디지털 서명을 계산하는 단계는 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터 및 저장된 필드 데이터 블록의 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함한다.

[0096] 발명의 다른 양상은 위의 보호 방법에 따라 보호되는 원본 물품의 배치에 속하는 표시된 원본 물품에 대하여, 물품의 물품 디지털 이미지의 적합성을 검증하는 시스템에 관한 것으로서, 이미징 유닛, 메모리가 있는 처리 유닛, 및 이미지 처리 유닛을 갖는 영상장치를 포함하고, 메모리는 원본 물품의 배치에 대응하는 트리의 기준 루트 디지털 서명을 저장하고, 처리 유닛에는 디지털 데이터의 및 트리 내의 노드 순서 및 트리 연결 순서에 따른 디지털 서명의 연결의 디지털 서명을 계산하는 단방향 함수가 프로그래밍되며, 상기 시스템은:

[0097] - 영상장치를 사용하여 물품 상의 보안 표지를 나타내는 물품 디지털 이미지를 획득하고;

[0098] - 영상장치를 사용하여 보안 표지의 획득된 디지털 이미지 상의 물품 디지털 데이터의 및 연관된 검증 키의 표현을 판독하고, 상기 판독된 표현으로부터 각각 대응하는 시험 물품 디지털 데이터 및 연관된 시험 검증 키를 추출하고;

[0099] - 추출된 시험 물품 디지털 데이터 및 시험 검증 키가 실제로 저장된 기준 루트 디지털 서명과 일치하는지 처리 유닛 상에서 더 프로그래밍된 다음의 단계들을 수행함으로써 검증하도록 작동 가능하고,

[0100] - 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터의 디지털 서명을 계산하는 단계-상기 시험 디지털 서명은 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응함;

[0101] - 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 시험 리프 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 리프 노드의 디지털 서명을 추출하고, 시험 디지털 서명 및 상기 모든 다른 리프 노드의 추출된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 리프 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0102] - 시험 트리 내의 각 다음 수준에서 연속적으로 끝에서 두 번째 노드 수준까지, 시험 검증 키 내의 디지털 서명의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 시험 트리의 모든 다른 비-리프 노드의 디지털 서명을 추출하고, 상기 각각의 모든 다른 비-리프 노드의 디지털 서명 및 상기 이전 동일한 부모 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0103] - 시험 트리의 끝에서 두 번째 노드 수준에 대응하는 비-리프 노드의 획득된 디지털 서명의 연결의 디지털 서명을 계산하여, 시험 트리의 루트 노드의 후보 루트 디지털 서명을 획득하는 단계; 및

[0104] - 획득된 후보 루트 디지털 서명이 저장된 기준 루트 디지털 서명과 일치하는지 확인하는 단계,

[0105] 상기 루트 디지털 서명이 일치하는 경우, 시스템이 물품 디지털 이미지가 정품 표시된 원본 물품의 것이라는 표시를 전달하도록 구성된다.

[0106] 표시된 원본 물품이 위에서 언급된 연관된 필드 데이터 블록을 가지면, 처리 유닛의 메모리는 연관된 필드 데이터 블록을 더 저장하며, 시험 객체 상의 보안 표지에 대응하는 시험 트리 내의 시험 리프 노드에 대응하는 시험

디지털 서명을 계산하는 단계는 단방향 함수를 사용하여 추출된 시험 물품 디지털 데이터 및 저장된 필드 데이터 블록의 디지털 데이터의 연결의 디지털 서명을 계산하는 것을 포함할 수 있다.

[0107] 본 발명은 첨부 도면을 참조하여 이하에서 더욱 완전하게 설명될 것이며, 상이한 도면에 걸쳐 유사한 도면 부호는 유사한 요소를 표현하며, 발명의 두드러진 양상 및 특징이 예시된다.

도면의 간단한 설명

[0108] 도 1은 본 발명에 따른 물품 배치를 보호하는 일반적인 개념의 개략도이다.

도 2a는 본 발명에 따라 보호되는 생체 식별 문서의 예로서 보호되는 생체 여권을 도시한다.

도 2b는 도 2a의 보호되는 생체 여권을 갖는 개인을 정규 관리가 통제하는 것을 도시한다.

도 3은 본 발명에 따라 보호되는 항공기 부품 배치를 도시한다.

도 4는 본 발명에 따라 보호되는 제약 제품 배치를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0109] 본 개시는 도면에 예시된 비제한적인 실시예를 참조하여 여기에서 상세하게 설명된다.

[0110] 도 1은 물품 배치의 보호 및 각 물품과 연관될 수 있는 검증 정보의 인코딩을 계산하는 방법에 관한 본 발명의 일반적인 개념을 도시한다. 도 1은 물품의 그룹 또는 "배치(batch)" 및 그 연관된 트리를 도시하며, 간단하게, 8개의 물품 A_1, …,A_8만이 도시되어 있고, 이는 물리적인 기계 판독 가능한 보안 표지(110)(여기에서는 2D 바코드로 예시되지만, 1D 바코드 또는 RFID 표지 등일 수 있음)을 갖거나 포함할 수 있거나, 또는 물리적 보안 표지를 다시 갖거나 포함할 수 있는 어떤 것을 가질 수 있는 임의의 것일 수 있다. 물품은 제조된 품목 또는 그 포장, 물리적 문서 또는 이미지, 여러 품목이 포함된 패키지(예컨대 약품의 블리스터 팩) 또는 제품 상자 팔레트가 들어있는 컨테이너 등이 될 수 있다. 사람이나 동물도 본 발명의 실시예의 의미에서 "물품"일 수 있는데, 예를 들어, 행사의 승인된 참석자 또는 그룹 구성원, 또는 떼(flock)나 무리(herd)의 구성원이 어떤 형태의 ID 배지를 소지하거나 (특히 동물의 경우) 물리적으로 표시될 수 있다.

[0111] 배치는, 예를 들어, 공통의 제조 조업(run), 특정 공급업체가 제공한 품목, 특정 기간 동안 제조 또는 배송된 품목, 관련된 이미지 세트, 사람 그룹, 떼 또는 무리, 또는 그밖에 데이터 A_i를 정의할 수 있는 모든 객체에 대한 사용자 정의 그룹이 될 수 있다. 도 1에 나타난 임의의 물품은 선택한 데이터의 인코딩을 활성화하기 위해 포함될 수 있는 선택적 소프트웨어 구성인 "가상 물품" A_v일 수 있다. 이에 대해서는 아래에서 자세히 설명한다. 예를 들어, 8개의 물품 중 하나, 예를 들어, 물품 A_8이 실제로 8개의 물품의 배치에 속하는 것으로 계산되는 가상 물품 A_v일 수 있으며, 이는 (실제 객체에 해당하지 않지만) 실질적으로 동일한 방식으로 처리될 수 있으므로, 다른 7개의 실제 물품 중 임의의 것과 동일하게 처리된다. 디지털 데이터를 인코딩하고 더 강력한 물품 디지털 서명을 생성하기 위하여 복수의 가상 물품 A_{v1}, A_{v2},…, A_{vk}를 사용할 수 있음은 물론이다(아래 참조).

[0112] 배치의 각 물품 A_1, A_2, …, A_7, A_v ($A_8 \equiv A_v$)에 대하여, 임의의 적합한 방법을 사용하여 각각의 물품 디지털 데이터 D_1, D_2, …, D_7, D_v ($D_8 \equiv D_v$)가 연관되거나 추출된다(또는, 가상 물품 A_v의 경우, 생성된다). 이 데이터는 물리적 특성의 일부 수치, 완성된 양식 또는 제품 정보와 같은 텍스트 데이터, 일련번호 또는 기타 식별자, 콘텐츠 표시, 이미지의 디지털 표현 또는 시스템 설계자가 물품과 연관시키기로 선택한 임의의 다른 정보일 수 있다. 물품 디지털 데이터 D_i는 대응하는 디지털 데이터 파일을 생성할 수 있는 판독기에 의해 물품에 표시(예를 들어 물품에 인쇄되거나 물품에 부착된 라벨에 인쇄)된 사람이 판독할 수 있는 데이터(예를 들어, 영숫자 데이터)로부터 추출될 수 있다. 추가적인 디지털 데이터(예를 들어, 물품 사용 지침 또는 안전 지침 등)가 추출된 데이터와 연관되어 물품 디지털 데이터 D_i를 구성할 수 있다.

[0113] 가상 물품 A_v의 경우, 연관된 디지털 데이터는, 예를 들어, 배치 식별 번호, 배치의 물품 수, 데이터 엔트로피를 증가시켜 보안을 증가시키고자 하는 (의사) 난수, 날짜 및/또는 또는 시간 정보 등을 포함할 수 있다. 다른 형태의 연관된 데이터는 허용 또는 허용되지 않는 작업 규칙, 유효기간 등의 표시일 수 있다. 간단히 말해서, 디지털 데이터 D_v는 디지털 형식으로 표현할 수 있는 모든 것이 될 수 있다.

[0114] 배치의 각 물품에 대하여, 그 각각의 디지털 물품 데이터 D_1, D_2, …, D_7, D_v는 바람직하게는 그것이 본질적으로 은폐되는 방식으로 수학적으로 변환되지만, 이는 임의의 실시예에 대한 절대적인 요구사항은 아니다. 물품 A_i의 물품 디지털 데이터 D_i에 적용되는 이 변환은 대응하는 디지털 서명 x_i를 생성하는 역할을 한다. 이 디지털 서명은 단방향 함수, 즉, 계산하기 쉽지만 반전하기 어려운 함수(S. Goldwasser 및 M. Bellare "암호화에 대한 강의 노트", MIT, 2008년 7월, http://www-cse.ucsd.edu/users/mihir 참조)를 사용하여 생성된다.

[0115] 이러한 유리한 변환 중 하나는, 예를 들어, 일반적으로 입력 크기에 관계없이 알려진 비트 길이의 출력을 반환하는 속성이 있는 해시 함수 H() = hash()를 물품 디지털 데이터에 적용하는 것이며, 그 기술적 효과는 연관된 물품 디지털 데이터의 크기와 배치의 크기에 관계없이, 물품과 연관된 디지털 데이터의 디지털 서명을 생성하는 데 특히 유용하다. 해시 함수는 단방향 함수의 잘 알려진 예이다. SHA(Secure Hash Algorithm) 계열 함수, 예를 들어, SHA-256와 같은 암호화 해시 함수를 사용하는 경우, 함수는 실질적으로 반전 불가능 및 충돌 저항성의 추가 이점이 있다. 즉, 두 개의 상이한 입력이 동일한 출력으로 이어질 확률은 무시할 수 있다. 이하의 설명으로부터 이해되는 바와 같이, 이는 다른 응용에서와 동일한 이유로 유리하지만, 또한 본 발명의 요구사항은 아니다. 도 1에 나타난 바와 같이, x_1, x_2, x_3,…, x_8 값은 각 물품 데이터 세트의 해시 값, 즉 연관된 물품 디지털 서명이며, 즉, j = 1…,8 에 대해 $x_j = H(D_j)$이다($A_8 \equiv A_v$인 경우, $D_8 \equiv D_v$ 및 $x_8 \equiv x_v = H(D_v)$이다).

[0116] 서명을 단축하기 위해, 물품 A_j의 물품 디지털 서명 x_j는 해시 값 $H(D_j)$의 비트로부터 선택된 더 낮은 가중치의 일정한 복수 비트의 시퀀스일 수도 있다. 예를 들어, SHA-2 계열의 SHA-256 해시 함수를 사용하는 경우, 256 비트 서명에서 더 낮은 가중치의 128 비트만 유지하더라도 코드브레이킹 공격과 관련하여 강건한 서명을 유지할 수 있다.

[0117] 도 1은 각각 그 위에 적용된 대응하는 보안 표지(110)를 갖는 8개의 표시된 원본 물품 A_1, …,A_8 의 배치를 나타내고, 물품 디지털 서명의 트리를 사용하여 물품 및 각 연관된 물품 디지털 데이터 D_1, …, D_8을 보호하는 방법을 도시한다. 디지털 서명과 연관된 트리는 공지되어 있으며(이진 해시 트리, n-항(n-ary) 해시 트리 또는 머클(Merkle) 트리), 이들은 일반적으로 기본 노드 또는 리프(leaf) 노드를 가지고, 이들이 리프 노드의 특정 그룹에 따라 리프 노드와 연관된 디지털 서명의 연결에 디지털 서명하여 다음 (중간) 수준 노드를 구축하는 데 사용된다. 이진 트리의 경우, 제1 중간 수준 노드와 연관된 디지털 서명은 두 개의 연속 리프 노드와 연관된 디지털 서명의 연결에 디지털 서명(예를 들어, 단방향 해시 함수 H 또는 단방향 타원 곡선 함수 등을 사용하여)함으로써 각각 계산된다. N-항 트리의 경우, 제1 중간 수준 노드의 값은 n개의 연속된 리프 노드 값을 연결하여 얻는다. 트리는 더 복잡한 구조(혼합 트리)를 가질 수 있으며, 리프 노드의 연결이 특정 리프 노드에 대한 연속 노드 쌍, 다른 연속 리프 노드의 세 노드의 한 벌(triplet)에 의해 수행될 수 있는 등이다. 단순하게 하기 위하여, 8개의 리프 노드를 갖는 단순한 이진 트리가 도 1에 나타나 있다. 트리의 8개의 리프 노드 a(1,1),…, a(1,8)의 각 값은 각각 물품 디지털 서명 $x_1 = H(D_1)$,…, $x_8 = H(D_8)$에 해당한다. 모든 리프 노드에 대하여, 제1 인덱스의 값, 즉 "1"은 트리의 제1 수준(또는 기본 수준)을 표시하며, 1에서 8까지 이어지는 제2 인덱스는 트리의 (리프) 노드 순서를 나타낸다. 다음 수준 (비-리프) 노드, 즉 수준 2의 4개의 노드 a(2,1), a(2,2), a(2,3) 및 a(2,4)의 값이, 리프 노드 쌍, 즉 트리에서 그들의 자식 노드 쌍의 값의 연결(기호로는 연산자 "+"로 표시됨)에, 여기에서는 해시 함수를 통해, 디지털 서명함으로써 획득된다. 다음 수준의 노드 값을 얻기 위한 이 자식 노드 그룹은 트리 연결 순서를 정의한다. 표기를 단순화하기 위하여, 그 연관된 값(즉, 그 연관된 디지털 서명)을 또한 나타내기 위하여 노드 기호 a(i, j)를 사용한다. 여기에서 트리는 리프 노드 수준 위에 두 개의 중간 수준만을 가지고, 최상위 수준에는 루트 노드가 있다. 루트 노드 수준은 실제로 트리의 마지막 비-리프 노드 수준이다. 따라서, 다음 중간 수준의 4개의 비-리프 노드의 값은 다음과 같다.

[0118] $a(2,1) = H(a(1,1)+a(1,2))$, 즉 $a(2,1) = H(H(D_1)+ H(H(D_2))$, (a(1,1) 및 a(1,2)가 노드 a(2,1)의 자식 노드이므로)

[0119] $a(2,2) = H(a(1,3)+a(1,4))$

[0120] $a(2,3) = H(a(1,5)+a(1,6))$

[0121] $a(2,4) = H(a(1,7)+a(1,8))$

[0122] 다음으로, 끝에서 두 번째(penultimate) 노드 수준(여기서는 수준 3)에는 두 개의 노드 값이 있다.

[0123] a(3,1) = H(a(2,1)+a(2,2))

[0124] a(3,2) = H(a(2,3)+a(2,4)).

[0125] 각 비-리프 노드에 대하여 상이한 트리 연결 순서를 선택할 수 있음을 언급한다. 예를 들어 a(2,4) = H (a(1,7) + a(1,8)) 대신, 다른 노드 값을 제공하는 a(2,4) = H (a(1,8) + a(1,7))을 정의할 수 있다.

[0126] 마지막으로 트리의 루트 노드 R의 값 또는 기준 루트 디지털 서명은 R = H (a(3,1) + a(3,2))로 획득된다.

[0127] 트리와 관련된 연결 연쇄로 인하여, 노드(특히 리프 노드)에서 디지털 데이터의 비트가 변경되면 루트 값을 검색하는 것이 사실상 불가능하다. 또한, 일부 가상 물품이 배치에 포함되면(가상 물품 디지털 데이터는 트리의 리프 노드의 디지털 서명을 생성한 시스템에만 알려짐), 위조자는 배치의 모든 생산(및 표시) 물품의 디지털 데이터를 알고 있더라도 루트 디지털 서명을 검색할 수 없다.

[0128] 발명에 따르면, 물품 배치의 기준 루트 디지털 서명 R은 물품(또는 그 연관된 데이터)의 진정성을 확인하여야 하는 사용자가 접근할 수 있는 (공용) 매체에 게시되거나, 또는 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장되거나, 바람직한 모드에서는, 사용자가 접근할 수 있는 블록체인(또는 블록체인으로 보호되는 데이터베이스)에 저장됨으로써 불변으로 만들어지고 따라서 위조 방지된다. 그런 다음 사용자는 이러한 이용 가능한 소스로부터 획득한 기준 값 R을 저장할 수 있다.

[0129] 배치의 각 물품 A_i에 대하여, 연관된 트리의 대응하는 물품 검증 키 k_i(또는 검증 경로)는, 리프 노드 수준으로부터 끝에서 두 번째 노드 수준까지, 트리 내에서 물품 디지털 서명에 대응하는 리프 노드와 동일한 부모 노드를 갖는 모든 다른 리프 노드의, 및 트리의 각 다음 수준에서 연속적으로, 이전 수준에서 이전의 동일한 부모 노드가 고려된 트리 내의 동일한 부모 노드를 갖는 모든 비-리프 노드의 각 디지털 서명의 시퀀스로 계산된다. 도 1의 예에서, 배치의 8개의 물품 $A_1,\cdots,A_8$ 및 그 대응하는 8개의 리프 노드 a(1,1),…,a(1,8)에 각각 대응하는 8개의 검증 키 $k_1,\cdots,k_8$가 있다.

[0130] 1) 물품 A_1에 대응하는 리프 노드 $a(1,1) = x_1 = H(D_1)$에 대하여, 검증 키는 k_1 = {a(1,2),a(2,2),a(3,2)}이며, 이로부터 다음의 단계를 통하여 루트 디지털 서명 값 R이 검색될 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨)

[0131] i) 리프 노드 $a(1,1) = x_1$ 및 k_1 내의 리프 노드 $a(1,2) = x_2$ (a(1,2)는 물품 디지털 서명 x_1에 대응하는 리프 노드, 즉 노드 a(1,1)과 동일한 부모 노드, 즉 노드 a(2,1)를 갖는 다른 리프 노드임)로부터, 부모 노드 값 a(2,1)이 a(2,1) = H(a(1,1)+a(1,2))에 의해 획득된다(즉, $a(2,1) = H(x_1 + x_2)$),

[0132] ii) 획득된 a(2,1) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(2,1)과 트리에서 동일한 부모 노드, 즉 노드 a(3,1)를 갖는 비-리프 노드인, 다음 비-리프 노드 수준의 k_1 내의 다음 노드 값, 즉 a(2,2)로부터, 부모 노드 값 a(3,1)이 a(3,1) = H(a(2,1)+a(2,2))에 의해 획득된다,

[0133] iii) 획득된 a(3,1) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(3,1)과 트리에서 동일한 부모 노드, 즉 루트 노드를 갖는 비-리프 노드인, 끝에서 두 번째 노드 수준의 k_1 내의 다음 노드 값, 즉 a(3,2)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0134] 비고: 이 예에서, 트리가 루트 노드 수준 아래로 3개의 수준을 가지고, 따라서 검증 키가 3개의 노드 값을 포함하므로 3개의 단계 i), ii) 및 iii)이 있다.

[0135] 따라서, 트리의 루트 노드 값은 R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))로 획득된다.

[0136] 2) 물품 A_2에 대응하는 리프 노드 $a(1,2) = x_2 = H(D_2)$에 대하여, 검증 키는 k_2 = {a(1,1),a(2,2),a(3,2)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0137] i) $a(1,2) = x_2$ 및 k_2 내의 $a(1,1) = x_1$(a(1,1)는 물품 디지털 서명 x_2에 대응하는 리프 노드, 즉 노드 a(1,2)과 동일한 부모 노드, 즉 노드 a(2,1)를 갖는 다른 리프 노드임)로부터, 부모 노드 값 a(2,1)이 a(2,1) = H(a(1,1)+a(1,2))에 의해 획득된다,

[0138] ii) 획득된 a(2,1) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(2,1)과 트리에서 동일한 부모

노드, 즉 노드 a(3,1)를 갖는 비-리프 노드인, 다음 비-리프 노드 수준의 k_2 내의 다음 노드 값, 즉 a(2,2)로부터, 부모 노드 값 a(3,1)이 a(3,1) = H(a(2,1)+a(2,2))에 의해 획득된다,

[0139] iii) 획득된 a(3,1) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(3,1)과 트리에서 동일한 부모 노드, 즉 루트 노드를 갖는 비-리프 노드인, 끝에서 두 번째 노드 수준의 k_2 내의 다음 노드 값, 즉 a(3,2)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0140] 따라서, 트리의 루트 노드 값은 R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))로 획득된다.

[0141] 3) 물품 A_3에 대응하는 리프 노드 a(1,3) = x_3 = H(D_3)에 대하여, 검증 키는 k_3 = {a(1,4),a(2,1),a(3,2)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0142] i) a(1,3) = x_3 및 k_3 내의 a(1,4) = x_4(a(1,4)는 물품 디지털 서명 x_3에 대응하는 리프 노드, 즉 노드 a(1,3)과 동일한 부모 노드, 즉 노드 a(2,2)를 갖는 다른 리프 노드임)로부터, 부모 노드 값 a(2,2)이 a(2,2) = H(a(1,3)+a(1,4))에 의해 획득된다,

[0143] ii) 획득된 a(2,2) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(2,2)과 트리에서 동일한 부모 노드, 즉 노드 a(3,1)를 갖는 비-리프 노드인, 다음 비-리프 노드 수준의 k_3 내의 다음 노드 값, 즉 a(2,1)로부터, 부모 노드 값 a(3,1)이 a(3,1) = H(a(2,1)+a(2,2))에 의해 획득된다,

[0144] iii) 획득된 a(3,1) 및 이전 수준에서 이전 동일한 부모 노드가 고려된, 즉 노드 a(3,1)과 트리에서 동일한 부모 노드, 즉 루트 노드를 갖는 비-리프 노드인, 끝에서 두 번째 노드 수준의 k_3 내의 다음 노드 값, 즉 a(3,2)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0145] 따라서, 트리의 루트 노드 값은 R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2))로 획득된다.

[0146] 4) 물품 A_4에 대응하는 리프 노드 a(1,4) = x_4 = H(D_4)에 대하여, 검증 키는 k_4 = {a(1,3),a(2,1),a(3,2)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0147] i) a(1,4) = x_4 및 k_4 내의 a(1,3) = x_3으로부터, 부모 노드 값 a(2,2)이 a(2,2) = H(a(1,3)+a(1,4))에 의해 획득된다,

[0148] ii) 획득된 a(2,2) 및 다음 비-리프 노드 수준의 k_4 내의 다음 노드 값, 즉 a(2,1)로부터, 부모 노드 값 a(3,1)이 a(3,1) = H(a(2,1)+a(2,2))에 의해 획득된다,

[0149] iii) 획득된 a(3,1) 및 끝에서 두 번째 노드 수준의 k_4 내의 다음 노드 값, 즉 a(3,2)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0150] 따라서, 트리의 루트 노드 값은 R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2))로 획득된다.

[0151] 5) 물품 A_5에 대응하는 노드 a(1,5) = x_5 = H(D_5)에 대하여, 검증 키는 k_5 = {a(1,6),a(2,4),a(3,1)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0152] i) a(1,5) = x_5 및 k_5 내의 a(1,6) = x_6으로부터, 부모 노드 값 a(2,3)이 a(2,3) = H(a(1,5)+a(1,6))에 의해 획득된다,

[0153] ii) 획득된 a(2,3) 및 다음 비-리프 노드 수준의 k_5 내의 다음 노드 값, 즉 a(2,4)로부터, 부모 노드 값 a(3,2)이 a(3,2) = H(a(2,3)+a(2,4))에 의해 획득된다,

[0154] iii) 획득된 a(3,2) 및 끝에서 두 번째 노드 수준의 k_5 내의 다음 노드 값, 즉 a(3,1)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0155] 따라서, 트리의 루트 노드 값은 R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4)))로 획득된다.

[0156] 6) 물품 A_6에 대응하는 노드 a(1,6) = x_6 = H(D_6)에 대하여, 검증 키는 k_6 = {a(1,5),a(2,4),a(3,1)}이며, 이로

부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0157] i) $a(1,6) = x_6$ 및 k_6 내의 $a(1,5) = x_5$으로부터, 부모 노드 값 a(2,3)이 a(2,3) = H(a(1,5)+a(1,6))에 의해 획득된다,

[0158] ii) 획득된 a(2,3) 및 다음 비-리프 노드 수준의 k_6 내의 다음 노드 값, 즉 a(2,4)로부터, 부모 노드 값 a(3,2)이 a(3,2) = H(a(2,3)+a(2,4))에 의해 획득된다,

[0159] iii) 획득된 a(3,2) 및 끝에서 두 번째 노드 수준의 k_6 내의 다음 노드 값, 즉 a(3,1)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0160] 따라서, 트리의 루트 노드 값은 R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4)))로 획득된다.

[0161] 7) 물품 A_7에 대응하는 노드 $a(1,7) = x_7 = H(D_7)$에 대하여, 검증 키는 k_7 = {a(1,8),a(2,3),a(3,1)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0162] i) $a(1,7) = x_7$ 및 k_7 내의 $a(1,8) = x_8$으로부터, 부모 노드 값 a(2,4)이 a(2,4) = H(a(1,7)+a(1,8))에 의해 획득된다,

[0163] ii) 획득된 a(2,4) 및 다음 비-리프 노드 수준의 k_7 내의 다음 노드 값, 즉 a(2,3)로부터, 부모 노드 값 a(3,2)이 a(3,2) = H(a(2,3)+a(2,4))에 의해 획득된다,

[0164] iii) 획득된 a(3,2) 및 끝에서 두 번째 노드 수준의 k_7 내의 다음 노드 값, 즉 a(3,1)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0165] 따라서, 트리의 루트 노드 값은 R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8))))로 획득된다.

[0166] 8) 물품 A_8에 대응하는 노드 $a(1,8) = x_8 = H(D_8)$에 대하여, 검증 키는 k_8 = {a(1,7),a(2,3),a(3,1)}이며, 이로부터 다음의 단계를 통해 루트 값 R을 검색할 수 있다(트리의 노드 순서 및 트리 연결 순서에 따라 실행됨).

[0167] i) $a(1,8) = x_8$ 및 k_8 내의 $a(1,7) = x_7$으로부터, 부모 노드 값 a(2,4)이 a(2,4) = H(a(1,7)+a(1,8))에 의해 획득된다,

[0168] ii) 획득된 a(2,4) 및 다음 비-리프 노드 수준의 k_8 내의 다음 노드 값, 즉 a(2,3)로부터, 부모 노드 값 a(3,2)이 a(3,2) = H(a(2,3)+a(2,4))에 의해 획득된다,

[0169] iii) 획득된 a(3,2) 및 끝에서 두 번째 노드 수준의 k_8 내의 다음 노드 값, 즉 a(3,1)로부터, 루트 노드 값 R이 R = H(a(3,1)+a(3,2))에 의해 획득된다.

[0170] 따라서, 트리의 루트 노드 값은 R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8))))로 획득된다.

[0171] 일반적으로 주어진 리프 노드 값과 주어진 리프 노드와 연관된 검증 키에 지정된 노드 값에서 시작하여 (후보) 루트 노드 값을 검색하기 위하여, 다음 단계가 수행된다.

[0172] - 검증 키의 노드 값 시퀀스에서 주어진 리프 노드의 것과 동일한 부모 노드를 갖는 트리의 모든 다른 리프 노드의 노드 값(즉, 디지털 서명 값)을 추출하고 주어진 노드 값 및, 각각 트리의 노드 순서 및 트리 연결 순서에 따라, 모든 다른 리프 노드의 추출된 노드 값의 연결의 디지털 서명을 계산하여, 주어진 리프 노드의 동일한 부모 노드의 디지털 서명을 획득하는 단계;

[0173] - 트리의 각 다음 수준 및 끝에서 두 번째 노드 수준까지 연속적으로:

[0174] . 검증 키 내의 노드 값의 시퀀스로부터, 이전 단계에서 고려된 이전 동일한 부모 노드의 것과 동일한 부모 노드를 갖는 트리의 모든 다른 비-리프 노드의 노드 값을 추출하고,

[0175] . 각 모든 다른 비-리프 노드의 노드 값의 연결의 디지털 서명 및, 트리의 노드 순서 및 트리 연결 순서에 따라, 상기 이전 동일한 부모 노드의 획득된 디지털 서명을 계산하여, 상기 이전 동일한 부모 노드의 상기 동일한 부모 노드의 노드 값을 획득하는 단계; 및

[0176] - 트리의 노드 순서 및 트리 연결 순서에 따라 트리의 끝에서 두 번째 노드 수준에 대응하는 비-리프 노드의 획

득된 노드 값의 연결의 디지털 서명을 계산하여, 트리의 루트 노드의 루트 디지털 서명을 획득하는 단계.

[0177] 위의 예에서 분명한 바와 같이, 루트 노드 값 R은 임의의 주어진 리프 노드 값으로부터 이 리프 노드 값과 대응하는 검증 키 내에 지정된 노드 값만의 연결의 디지털 서명에 의하여 최종적으로 검색될 수 있다. 따라서, 루트 노드 값을 검색하는 데 필요한 검증 정보 내의 데이터량은 기준 루트 노드 값을 계산하는 데 필요한 데이터량보다 분명히 훨씬 적다(즉 트리의 중간 수준의 모든 비-리프 노드 값을 계산함으로써 리프 노드 값에만 기반한다). 이는 (2차원 바코드와 같은) 보안 표지에 사용할 수 있는 크기가 제한되는 제약 조건의 관점에서 발명의 이점이다.

[0178] 발명에 따르면, 검증 정보 V_i의 디지털 표현의 비트 크기를 종래의 판독기로 쉽게 판독할 수 있는 2차원 기계 판독 가능 바코드의 데이터 콘텐츠와 호환되는 수준으로 유지하면서 물품 데이터 D_i와 표시된 물품 A_i이 정품 물품의 주어진 배치에 속하는 것 사이에 고유하고, 변경 불가능하며 변조 방지된 링크를 제공함으로써, 물품 배치의 물품 A_i에 적용된 보안 표지(110)(변조 방지 가능)가 표시된 물품의 진정성 또는 정품 표시된 물품의 것에 대한 그 연관된 데이터의 적합성, 또는 정품 표시된 물품의 것에 대한 물품의 이미지의 적합성까지 온라인 및 오프라인 검사 작업을 허용하는 검증 정보 V_i를 포함한다. 이 검증 정보는 물품 디지털 데이터 D_i 및 대응하는 검증 키 k_i, $V_i = (D_i,k_i)$를 포함한다. 이 확인 작업은 물품 A_i 상의(각각, A_i의 이미지 상의) 기계 판독 가능 보안 표지(110) 상의(또는 보안 표지의 이미지 상의) 물품 디지털 데이터 D_i 및 대응하는 검증 키 k_i를 먼저 판독하고, 판독된 물품 디지털 데이터 D_i의 단방향 함수를 사용하여 $X_i = H(D_i)$로서 후보 물품 디지털 서명 X_i를 계산하고, 위에서 설명한 바와 같이 X_i 및 검증 키 k_i에 표시된 노드 값의 시퀀스에 따른 트리의 노드 값의 연결의 디지털 서명으로부터 후보 루트 디지털 서명 R^c을 계산함으로써 배치와 연관된 트리의 배치 값, 또는 기준 루트 디지털 서명 R을 검색하는 것을 포함한다. 데이터 암호화 및 따라서 암호화/복호화 키 관리(특히 보안 표지에 암호화 키가 포함되지 않음)가 필요하지 않다는 이점을 갖는 이 보호 방식은 (예를 들어, RSA "Rivest-Shamir-Adleman" 시스템과 같은) 공개 암호화 키-비공개 복호화 키를 사용하는 기존 데이터 암호화에 비해 코드브레이킹 공격에 대해 훨씬 더 강건하다. 결과적으로, 발명에 따라 보안 표지에 표현되는 디지털 데이터의 크기는 작고 기존의 2D 바코드(예를 들어, QR 코드) 및 따라서 기존의 바코드 판독기(또는 단순히 카메라를 갖는 프로그래밍된 스마트폰)의 사용을 허용하면서도, 코드브레이킹 공격에 대해 매우 높은 수준의 강건성을 제공한다. 또한, 이 보안 표지는 표시된 물품의 진정성 및 정품 물품의 것에 대한 그 데이터의 적합성의 (코드 판독기와 통신하는 서버를 통한) 온라인 및 (프로그래밍된 코드 판독기를 통한) 오프라인 확인 양자와 호환될 수 있다. 또한, 발명에 따르면 디지털 데이터 D_i 및 키 데이터 k_i의 표현이 상이할 수 있으며, 데이터 연결 방식 및/또는 단방향 함수가 트리의 노드 수준에 의존할 수 있어, 코드브레이킹 공격에 대해 추가적인 수준의 강건성을 제공한다.

[0179] 바람직하게는, 보안 표지 내에 포함될 디지털 데이터(즉, 검증 정보 V)의 크기를 더욱 줄이기 위하여, 배치의 각 원본 물품 A_i의 물품 디지털 데이터 D_i가 배치의 모든 물품에 대해 공통인 주어진 필드 사이에 분산되며, 이들 필드에 관한 디지털 데이터는 각 물품 디지털 데이터 Di에 포함되지 않고 물품 배치와 연관된 별도의 필드 데이터 블록 FDB 내에 모아지고,

[0180] - 그런 다음 배치의 원본 물품 A_i의 물품 디지털 서명 x_i이 대응하는 물품 디지털 데이터 D_i 및 필드 데이터 블록 FDB의 디지털 데이터의 연결의 단방향 함수 H, 즉 $x_i = H(D_i+FDB)$로 계산되며;

[0181] - 기준 루트 디지털 서명 R이 연관된 필드 데이터 블록 FDB와 함께 사용자에게 제공된다(필드 데이터 블록 또한 변경 불가능하게 함).

[0182] 발명의 변형에서, 필드 데이터 블록 FDB은 기준 루트 디지털 서명과 독립적으로 사용자가 접근할 수 있다.

[0183] 배치의 물품과 연관된 대부분의 데이터가 데이터 구조화를 위한 일부 필드에 따라 구분되기 때문에, 위의 크기 축소는 대부분의 경우에 가능하다. 제약 제품에 대하여, 예를 들어, "일련번호", "유효기간" 등의 표시, 이들 필드와 연관된 데이터만이 Di에 포함되는 한편(예를 들어, 12603, 2020년 5월 등), 필드의 공통 명칭 "일련번호", "유효기간" 등은 필드 데이터 블록 FDB에 있다.

[0184] 검증 키와 물품 디지털 데이터(또는 임의의 다른 데이터)를 인코딩하기 위하여 사용될 수 있는 상이한 유형의 물리적 (보안) 표지가 있다. 그러나, 작은 품목에 사용하기에 실용적인 많은 표지 시스템이나 고해상도의 물리적 표지를 수용할 수 없는 서비스는 많은 양의 데이터를 인코딩할 수 없다.

[0185] 이 문제를 해결하는 한 가지 방법은 각각 검증 벡터의 요소 중 하나 이상을 포함하는 여러 표지를 포함하는 것이다. 많은 경우, 이것은 물리적 공간이 부족하거나 표시 표면이 적합하지 않기 때문에 또는 단순히 미적으로 받아들일 수 없기 때문에 비실용적이다.

[0186] 물리적 표면에 적용할 수 있는 방식으로 정보를 인코딩하는 알려진 방법이 많이 있다. 이러한 임의의 방법은 본 발명의 임의의 실시예의 구현에 사용될 수 있다. 물리적 표지의 일반적인 형태 중 하나는 잘 알려진 QR 코드이다. 잘 알려진 바와 같이, 주어진 영역에 대해 QR 코드가 인코딩할 수 있는 데이터가 많을수록 모듈 밀도(대략 흑백 "정사각형"의 밀도)가 높아지고 인쇄 및 판독에 필요한 해상도가 높아진다. 밀도(제곱 모듈 수) 외에도 QR 코드는 일반적으로 포함된 오류 수정 수준에 따라 분류된다. 현재 네 가지 상이한 표준 "레벨", L, M, Q 및 H는 각각 "손상"의 정도, 즉 QR 코드 이미지를 유지하고 복구할 수 있는 데이터 손실을 나타낸다. 레벨 L, M, Q 및 H는 각각 대략 7%, 15%, 25% 및 30%의 피해를 견딜 수 있다.

[0187] 다음 표는 상이한 QR 코드 버전에 대한 적어도 근사하는 값을 보여준다.

표 1

[0188]

버전	크기(모듈)	인코딩 가능한 비트 수	
		ECC 레벨 L	ECC 레벨 H
10	57 X 57	2192	976
25	117 X 117	10208	4304
40	177 X 177	23648	10208

[0189] 그러나 일부 모듈은 스캔 대상, 마스크 패턴 및 오류 수정 모듈에 사용되기 때문에, 모든 비트가 데이터 "로드"를 인코딩하는 데 사용되는 것은 아니다. 따라서 QR 코드(또는 표지(110)로 사용되는 모든 것)가 인코딩할 수 있는 정보의 양과 검증 정보(V)에 포함되고 인코딩되어야 하는 정보의 양 사이에는 트레이드오프가 있다.제한된 인코딩 용량을 갖는 선택된 유형의 보안 표지(110)(예컨대 QR 코드)에 대하여, 적절한 단방향 함수 H도 따라서 선택되어야 한다. 요구되는 비트의 측면에서 출력이 너무 큰 함수는 사용이 전혀 불가능하고, 범위가 너무 작은 함수는 보안이 충분하지 않을 수 있다. 또한 많은 응용에서 확장성이 문제가 될 수 있다. 예를 들어, 일부 데이터 보안 체계는 배치의 구성원 수가 증가함에 따라 증가하는 서명을 포함하고, 보안 표지(110)가 인코딩할 수 있는 비트 수의 관점에서 배치의 크기를 허용 가능하지 않게 제한할 수 있다. 이것이 발명의 바람직한 모드에 따라 선택된 함수 유형이 SHA-2 계열의 단방향 해시 함수인 이유이다.

[0190] 배치의 물품의 물품 디지털 데이터를 디지털 서명하기 위한 계산을 수행하고, 상이한 물품에 대한 검증 키를 결정하고, 대응하는 트리의 기준 루트 디지털 서명을 계산하기 위하여 제공되는 코드를 실행하기 위하여 계산 모듈(미도시)이 보안 시스템 내에 포함되는 것이 바람직하다. 보안 시스템은 또한 가상 물품(들) A_v의 디지털 데이터 D_v에 대응하는 (사전 프로그래밍된) 값을 입력하기 위한 적절한 모듈을 포함할 수 있다. 물품 관련 해싱 계산을 외부에서(예를 들어, 연결된 원격 서버 상에서), 예를 들어, 물품이 만들어질 때마다, 또한 수행할 수 있으며, 이는, 우려되는 경우, 그 사이트(또는 사이트들)로부터 보안 시스템으로 네트워크를 통해 미가공 물품 데이터 D_i를 전송하는 것을 피할 수 있게 한다.

[0191] 각 물품 A_i에 대하여, 대응하는 검증 정보 V_i가 컴파일되고 그 다음 각 물품에 물리적으로 적용되거나 다른 방식으로 연관되는 어떤 형태의 기계 판독 가능 보안 표지(110)로 인코딩(표현)된다. 예를 들어, V_i는 물품에 부착되거나 물품에 직접 또는 포장에 인쇄될 수 있는 광학 또는 자기 판독 가능한 라벨, RFID 태그 등으로 인코딩될 수 있다. 다른 옵션으로, 표지는 적절한 경우 물품 또는 포장 내부에 직접 적용하거나, 예를 들어, 포장 내부에 있는 문서의 일부 형식에 포함될 수 있다.

[0192] 임의의 "가상" 물품 A_v에 대하여, 그 대응하는 검증 정보 $V_v = (D_v, k_v)$는 보안 시스템에 의해 내부적으로 연관될 수 있다. 검증 정보는 일반적으로 적어도 물품 배치의 임의의 물품 A_i에 대하여 대응하는 물품 디지털 데이터 D_i 및 대응하는 검증 키 k_i 를 포함하며, 즉 $V_i = (D_i, k_i)$이다.

[0193] 추가적인 물품 데이터가 물품과 더 연관될 수 있으며, 예를 들어, 배치 값, 즉 기준 루트 디지털 서명 R, 또는 품목 일련번호, 배치 ID, 날짜/시간 정보, 제품명, 개별 항목(예컨대, 물품 이미지, 라벨링 또는 포장재 등) 또는 배치와 연관된 다른 온라인 정보를 가리키는 URL, 공급자/제조업체, 검증을 위해 전화할 수 있는 전화번호

등과 같이 시스템 설계자(또는 시스템 관리자)가 포함하기로 선택한 기타 정보를 포함할 수 있다. 추가적인 물품 데이터는 (정보 데이터베이스 인터페이스를 통해) 사용자가 접근할 수 있는 검색 가능한 정보 데이터베이스에 저장될 수 있다.

[0194] 원본 물품 A_i의 검증 키 k_i가 계산되고 (즉, 인코딩 또는 임의의 선택된 데이터 표현을 통해) 대응하는 물품 디지털 데이터 D_i와 함께, 물품 A_i에 적용된 기계 판독 가능 물품 보안 표지(110)에 포함되면, 결과적인 표시된 원본 물품 및 그 연관된 물품 데이터는 실제로 위조 및 변조로부터 보호된다.

[0195] 예를 들어 A_1과 같은 물품의 수신자인 사용자는 영상장치로 A_1 상의 보안 표지를 스캔(또는 다른 방식으로 판독)하고 물품 디지털 데이터 D_1 및 검증 키 k_1(및 표지 내로 인코딩된 임의의 다른 정보)를 추출한다. 표시된 물품 A_1의 검증을 위하여, 사용자는 먼저 A_1 상의 보안 표지(110)로부터 검증 정보 $V_1 = (D_1, k_1)$을 검색하고, 추출된 물품 디지털 데이터 D_1로부터 디지털 서명 x_1을 계산하여야 한다. 이를 위하여 사용자는 물품 디지털 서명을 계산하는 데 사용할 단방향 함수, 여기에서는 단방향 함수 H()(예를 들어, SHA-256 해시)를 알고 있어야 하며, 대응하는 후보 루트 디지털 서명 R^c를 계산하기 위하여 필요한 전체 데이터 (x_1, k_1)를 얻기 위하여 $x_1 = H(D_1)$ 연산을 수행하여야 한다. 예를 들어 사용자는 단방향 함수를 안전하게 수신하거나(예를 들어, 공개/개인 키 쌍을 사용하여), 이를 물품 제공자 또는 서명과 키를 생성한 엔티티에게 요청하거나, 또는 사용자의 영상장치의 처리 유닛에 이미 프로그래밍되어 있도록 할 수 있다.

[0196] 다음으로, 이러한 후보 루트 디지털 서명 R^c를 계산하기 위하여, 사용자는 이를 위해 (H(a(i,j)+a(i,k)를 통해 노드 값을 연결하기 위하여) 사용할 데이터 연결 방식의 유형을 추가로 알아야 한다. 사용자는 임의의 알려진 방식으로 이 정보를 안전하게(예를 들어, 공개/개인 키 쌍을 사용하여), 또는 이를 물품 제공자 또는 검증 데이터를 생성한 엔티티에게 요청함으로써 간단히 수신하거나, 또는 사용자의 처리 유닛에 이미 프로그래밍되어 있도록 할 수 있다. 그러나 연결 방식은 실제로 두 노드 값에 각각 대응하는 두 개의 디지털 데이터 블록의 단순한 종단간 연결에 대응할 수 있다. 이 경우 특정 방식이 사용자에게 전송되지 않아야 한다. 일부 변형에서, 연결 방식은 트리에서 연결된 디지털 데이터 블록의 등급 또는 수준에 지정된 데이터를 포함할 수 있는 연결 블록을 추가로 삽입할 수 있으며, 그 결과로 코드브레이킹 공격을 훨씬 더 어렵게 만든다.

[0197] 데이터 연결 방식을 알면, 사용자는 위에서 설명한 바와 같이, 트리 내의 노드 순서 및 트리 연결 순서에 따라 실행되는, 노드 a(1,1)에 관련한 위의 항목 1)을 참조하면, 물품 디지털 서명 x_1 및 검증 키 k_1 내에 지정된 노드 시퀀스에 따른 노드 값의 연결에 단계적으로 디지털 서명함으로써 (예를 들어, 적합하게 프로그래밍된 영상장치를 통하여) 후보 루트 디지털 서명 R^c을 계산할 수 있다. 여기에서, 후보 루트 디지털 서명은 다음과 같이 획득된다(트리 내의 노드 순서는 수준의 각 인덱스 (i,j) 및 수준 내의 등급에 의해 주어진다):

[0198] $R^c = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))$.

[0199] 이 계산된 후보 루트 디지털 서명 R^c는 사용 가능한(또는 게시된) 기준 R 값과 같아야 한다. 이 값은 사용자에 의해 미리 획득되었을 수 있거나 및/또는 영상장치의 처리 유닛의 메모리에 이미 저장되었을 수 있으며, 이는 또한 임의의 알려진 방식으로 수신인이 요청하고 시스템 관리자로부터 수신한 값일 수 있다. 후보 R^c 및 사용 가능한 기준 루트 디지털 서명 R이 일치하면, 이 계산은 보안 표지(110) 내의 정보를 검증하고 물품 A_1이 올바른 배치로부터 온 것임을 확인한다. 바람직하게는 보안 표지가 임의의 복사하기 어렵고 및/또는 제거하기 어려운 (변조 방지) 방식으로 이루어지거나 및/또는 물품에 적용되어야 한다. 이 경우 루트 디지털 서명의 일치는 물품이 진정한 것일 가능성이 높음을 사용자에게 표시할 수 있다. 이는 물품 A_1의 인증이 그 실질적인, 즉, A_1의 고유한 물리적 특성을 통하거나 A_1에 적용된 물질 기반 보안 표지를 통한 물질 인증을 필요로 하지 않기 때문에 특히 흥미롭다.

[0200] 물품 A_1에 대응하는 배치에 대한 기준 루트 디지털 서명 R에 접근하는 링크가 보안 표지(110)에 포함될 수 있지만(예를 들어, R가 대응하는 웹사이트에서 검색될 수 있는 경우 웹 주소), 이는 선호되는 변형은 아니다.

[0201] 일부 구현에서, 물품 A_i의 수신자는 물품으로부터 직접 디지털 물품 데이터 D_i에 대응하는 물품 데이터를 "시각적으로" 추출할 수 있다. 예를 들어, 물품 데이터는 일련번호 또는 설명 문구 내의 텍스트와 같은 텍스트이거나

물품 또는 포장의 어느 곳에 위치한 영숫자 인코딩이고 물품 자체 또는 그에 첨부되거나 포함된 것으로부터 사람이 읽을 수 있는 것일 수 있다. 물품 수신자에게는 스마트폰과 같은 영상장치 디바이스 내의 모듈과 같은 적절한 소프트웨어가 제공될 수 있으며, 이는 데이터를 입력하거나 전화 카메라를 통해 광학적으로 데이터를 판독하고, 사용 가능한 물품에 대한 $x_i = H(D_i)$를 계산한다. 예를 들어, 물품 A_1의 보안 표지(110)가 표준 QR 코드인 경우, 사용자는 영상장치에서 실행되는 표준 QR 코드 판독기 애플리케이션을 사용하여 영상장치로 QR 코드를 스캔하여 디지털 데이터 D_1 및 k_1을 쉽게 얻을 수 있으며, 사용자의 영상장치의 검증 애플리케이션은 x_1 및 R^c 을 계산할 수 있고, 위에서 설명한 대로 이 값을 사용 가능한 기준 배치 값 R와 비교한다.

[0202] 바람직하게는, 기준 루트 디지털 서명(즉, "배치 값") R는 위의 스마트폰 예의 경우에서와 같이, 통신 유닛이 장착된 영상장치를 통해 사용자가 (통신 링크를 통해) 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장된다. 물품 A_1을 검증하여야 하는 사용자는 스마트폰으로 루트 요청을, 데이터베이스의 접근 인터페이스를 통해, 데이터베이스의 주소로 보낼 수 있으며, 요청은 대응하는 기준 배치 값 R를 검색하도록 허용하는 A_1의 보안 표지(110)에서 판독한 물품 데이터 D_1(또는 계산된 디지털 서명 $x_1 = H(D_1)$)을 포함할 수 있고, 접근 인터페이스는 기준 루트 디지털 서명 R를 스마트폰으로 반환한다. 데이터베이스는 저장된 루트 디지털 서명의 불변성을 강화하기 위해 블록체인으로 보호될 수 있다. 본 발명의 이점은 물리적 객체, 즉 원본 물품과 그 속성, 즉 연관된 물품 데이터 및 그것이 특정한 물품 배치에 속하는 것 사이에 대응하는 루트 디지털 서명을 통해 실질적으로 불변의 링크를 만드는 것이다.

[0203] 위에서 언급한 물품 A_i의 검증 프로세스는 또한 A_i에 적용된 대응하는 물품 데이터 표지 상에 A_i 상에 추가로 표시되거나, A_i의 포장 또는 전단지에 인쇄된 사람이 읽을 수 있는 물품 데이터를 인증하는 역할을 할 수 있다. 실제로, 사용자는 물품 A_i의 보안 표지에서 판독되고 영상장치에 의해 디코딩된 대응하는 물품 디지털 데이터 D_i를, 예를 들어, 영상장치의 디스플레이에서 읽을 수 있으며, 표시된 정보가 물품 데이터 표지 상의 물품 데이터와 일치하는지 시각적으로 확인할 수 있다.

[0204] 바람직한 실시예에서, 물품 데이터 또는 그 대응 물품 디지털 데이터 D_i는 A_i를 (실질적으로) 인증하는 데 사용될 수 있는 표시된 원본 물품 A_i의 고유한 물리적 특성의 고유한 특성 디지털 데이터(characteristic digital data; CDD)를 더 포함한다. 따라서, 물품 A_i의 물리적 특성에 대응하는 특성 디지털 데이터가 CDD_i인 경우, 대응하는 고유한 물리적 서명 데이터 UPS_i는 CDD_i의 (바람직하게는 단방향 함수에 의한) 인코딩에 의해, 예를 들어, 디지털 데이터 CDD_i의 해시를 취함으로써, 즉 $UPS_i = H(CDD_i)$로 획득될 수 있다. 그러나 임의의 다른 공지의 인코딩을 대신 사용할 수 있다. 예를 들어, 짧은 서명을 갖기 위해 타원 곡선 디지털 서명 알고리즘을 사용할 수 있다. 물품 A_i의 고유한 물리적 특성에 대응하는 특성 디지털 데이터 CDD_i의 매우 단순화된 예의 예시로서 물품 A_i(또는 A_i의 특정 영역)를 영상화하여 얻은 단순한 디지털 이미지를 고려하면, 대응하는 고유한 물리적 서명 데이터 UPS_i는, 예를 들어, 디지털 이미지의 해시, $UPS_i = H(CDD_i)$이다. 서명 UPS_i를 생성한 특성 디지털 데이터 CDD_i는 A_i에 대한 기준 특성 디지털 데이터를 구성하고, 획득된 서명 UPS_i는 A_i에 대한 대응하는 기준 고유한 물리적 서명 데이터이다. 바람직하게는, UPS_i, 즉 물품 A_i에 대한 기준 물리적 서명 데이터는 (예를 들어, 물품 A_i의 보안 표지에서 판독된 물품 디지털 데이터 D_i 또는 그 대응하는 디지털 서명 x_i를 포함하는 요청을 통해) 사용자가 접근할 수 있는 검색 가능한 데이터베이스 또는 블록체인(또는 블록체인에 의해 보호되는 데이터베이스)에 저장된다. 따라서 저장된 UPS_i는 변경 불가능한 특성을 획득한다. CDD_i의 사본은 사용자의 영상장치의 메모리에 추가로 저장될 수 있다. 실시예의 변형에서, UPS_i의 사본 또한 (오프라인 검사 동작을 허용하기 위하여) 사용자의 영상장치의 메모리에 추가로 저장될 수 있다.

[0205] 물품 A_i의 진정성 확인은 물품 A_i 상의 보안 표지 상에서 (여기에서는 예를 들어 스마트폰일 수 있는 영상장치에서 실행되는 디코딩 애플리케이션을 사용하여) 판독된 디지털 데이터 D_i에서 후보 특성 디지털 데이터 CDD_i^c를 추출하고, 이를 영상장치의 메모리에 저장된 기준 특성 디지털 데이터 CDD_i와 비교하여 수행할 수 있다. $CDD_i^c = CDD_i$로 일치하는 경우, 물품 A_i는 정품으로 간주된다(그 디지털 콘텐츠는 정품으로 표시된 원본 물품에

대응한다). 기준 특성 디지털 데이터 CDD_i가 영상장치의 메모리에 저장되지 않고, 대신 기준 고유한 물리적 서명 데이터 UPS_i가 영상장치의 메모리에 저장되는 경우(CDD_i에 비해 훨씬 적은 메모리를 차지한다는 이점이 있음), 디지털 데이터 D_i에서 추출한 후보 고유한 물리적 특성 디지털 데이터 CDD_i^c의 해시 값을 계산하여 얻은 후보 고유한 물리적 서명 데이터 UPS_i^c를 검증하여 A_i의 진정성을 확인할 수 있다. 즉, $UPS_i^c = H(CDD_i^c)$이면 메모리에 저장된 기준 고유한 물리적 서명 데이터 UPS_i와 일치한다.

[0206] 사용자는 이러한 측정을 수행할 수 있는 센서(여기에서는, 영상장치의 이미징 유닛)를 통해, A_i에서 상기 고유한 물리적 특성을 검출하고 검출된 특성(여기서에는, 영상장치가 촬영한 디지털 이미지)으로부터 후보 특성 디지털 데이터 CDD_i^c를 얻어서, 오프라인 (자체 검증) 프로세스를 통해 수신된 물품 A_i의 진정성을 추가로 확인할 수 있다. 그런 다음, 사용자는 획득한 CDD_i^c를 (영상장치의 메모리에 저장된) 기준 CDD_i의 사본과 (영상장치의 이미지 처리 유닛을 통해, 또는 영상장치의 디스플레이 상에서 시각적으로) 비교할 수 있다. "합리적인" 일치 $CDD_i^c \approx CDD_i$ (즉, 두 디지털 데이터가 약간의 주어진 공차 또는 유사성 기준 내에서 일치함)의 경우 A_i 물품은 정품으로 간주된다.

[0207] 또한, 사용자는 또한 영상장치의 메모리에 저장된 기준 CDD_i의 사본에서 대응하는 후보 물리적 서명 데이터를 $UPS_i^c = H(CDD_i)$로 계산하고, 이를 영상장치의 메모리에 저장된 기준 물리적 서명 데이터 UPS_i와 비교할 수 있다. $UPS_i^c = UPS_i$로 일치하는 경우, 물품 A_i는 더 높은 신뢰도로 정품임이 확인된다. 또한, 일치의 경우, A_i 상의 보안 표지 상에서 판독된 검증 정보 (D_i k_i)로부터 대응하는 기준 배치 값 R를 검색하여, 전술한 바와 같이, 정품 물품의 것과 대응되는 것으로 검증된 A_i와 연관된 물품 디지털 데이터 D_i가 또한 인증된다. 바람직한 모드에서, 기준 특성 디지털 데이터 CDD_i의 사본은, 사용자의 영상장치의 메모리에 저장되는 대신, 물품 A_i의 보안 표지에 포함된 물품 디지털 데이터 Di의 일부이며 (영상장치로) 보안 표지 상에서 판독함으로써 얻을 수 있다. 그러나 변형(오프라인 검증과 여전히 호환됨)에서는 기준 특성 디지털 데이터 CDD_i의 사본이 물품 A_i에 적용된 물품 데이터 표지에 대신 포함될 수 있다(사용자의 영상장치가 읽을 수 있음).

[0208] 실시예의 변형에서, 사용자에 의한 물품 A_i의 진정성 확인은 온라인 프로세스를 통해 수행될 수 있다. 이 경우, 기준 데이터 CDD_i 및/또는 UPS_i는 사용자가 접근할 수 있는 검색 가능한 데이터베이스에 저장되며, 여기서 물품 A_i와 관련된 기준 데이터는 각각 대응하는 물품 디지털 데이터 D_i(A_i의 보안 표지에 포함됨) 또는 대응하는 물품 디지털 서명 x_i(데이터 D_i가 $x_i = H(D_i)$ 연산을 통해 보안 표지에서 추출되면 사용자에 의해 계산될 수 있음)와 연관되어 저장되며 각각 D_i 또는 x_i를 포함하는 질의를 데이터베이스에 전송하여 요청할 수 있다.

[0209] 물론, 물품 A_i의 특성 디지털 데이터 CDD_i 및 대응하는 고유한 물리적 서명 데이터 UPS_i를 얻기 위해 다른 알려진 고유의 물리적/화학적 특성이 사용될 수 있다. 다른 예시적인 예로서, 보안 표지(110)를 형성하는 2D 바코드를 특징적인 감쇠 시간 상수와 광 여기 파장 윈도우 및 발광 방출 파장 윈도우를 갖는 발광 안료를 포함하는 보안 잉크로 원본 물품에 인쇄할 수 있다. 결과는 잉크의 물질 "지문" 역할을 하는 특정 기준 감쇠 시간 값 τ를 갖는 잉크이다. 보안 표지를 인증하기 위해서는 안료 여기 파장 윈도우를 커버하는 조명 파장 윈도우에서 여기광으로 보안 표지(110)를 조명하고, 발광 방출 파장 윈도우 내에서 광 강도를 감지할 수 있는 센서로 보안 표지에서 생성된 발광 광을 수집하는 것으로 충분하다. 예를 들어, 사용자의 영상장치에는 보안 표지에 여기 광을 전달할 수 있는 플래시, 보안 표지로부터 대응하는 발광 광 강도 프로파일 I(t)(검출 시간 간격 동안)을 수집할 수 있는 포토 다이오드가 장착될 수 있으며, 영상장치의 처리 유닛은 수집된 강도 프로파일 I(t)로부터 감쇠 시간 값을 계산하도록 프로그래밍된다. 예를 들어, 여기 파장 윈도우는 UV(자외선) 대역 내에 있을 수 있고 방출 파장 윈도우는 IR(적외선) 대역 내에 있을 수 있다. 물품을 검증하는 동안, 사용자의 영상장치에 의해 수집된 발광 광 강도가 시간이 지남에 따라 후보 감쇠 시간 τ_c에 대응하는 특성 감쇠를 나타내면, $\tau_c \approx \tau$(주어진 공차 범위 내)일 때, 잉크 및 결과적으로 보안 표지가 정품으로 간주된다. 이 경우, 표시된 물품 A_i의 디지털 데

이터 CDD_i는 적어도 기준 감쇠 시간 값 τ(및 가능하게는 여기 파장 윈도우 및 방출 파장 윈도우와 관련된 데이터)를 포함한다. 위의 예에서 명백한 바와 같이, 보안 표지의 검증 정보에 기준 특성 디지털 데이터를 포함하는 것은 물품의 디지털 데이터와 바로 그 물품의 (실질적) 인증 데이터 사이에 위조 방지 링크를 제공하는 기술적 효과가 있다.

[0210] 본 발명의 다른 예시적인 실시예는 도 2a에 나타난 바와 같이, 생체인식 식별 문서, 예를 들어, 생체인식 여권의 배치에 관한 것이다.

[0211] 이 예에서 여권 데이터에 서명하기 위한 단방향 함수로 여전히 해시 함수를 사용하며, 잘 알려진 강건성을 고려하여 SHA-256 해시 함수를 사용하는 것이 바람직하다. 실제로 주어진 배치 크기를 고려할 때 여권 데이터에 서명할 목적으로 선택된 해시 함수(알려진 버킷 목록이 있음)는 각 개별 여권이 그 고유한 서명을 가지며, 이에 따라 서명을 고유하게 하는 단방향 암호화 기능의 예이다. 해시 함수의 도메인(즉, 가능한 키 세트)이 그 범위(즉, 상이한 테이블 인덱스의 수)보다 크면, 동일한 인덱스에 상이한 키를 매핑하여 충돌을 일으킬 수 있다. 배치의 크기를 알 때 해시 함수의 해시 테이블과 연관된 버킷 목록을 고려하고 충돌이 없는 함수만을 유지하거나 해시 테이블 충돌 해결 체계를 독립적으로 선택하여(예를 들어, 통합 해싱, 뻐꾸기 해싱 또는 홉스카치 해싱) 이러한 충돌을 피할 수 있다.

[0212] 도 2a는 기계 판독 가능 보안 표지(210)(여기에서는 QR 코드)로 보호된 생체인식 여권(A_1)의 예를 나타내고, 이는 종래의 여권 데이터, 즉 문서의 제목(230a)("여권"), 여권 소유자의 인명 데이터 세트(230b): 성("Doe"), 이름 ("John"), 성별("M"), 출생일자("1975년 3월 20일"), 국적("미국"), 출신지("Des Moines"), 출생지("오클랜드"), 여권 발급일자(230c)("2018년 2월 24일") 및 유효기간(230d)("2020년 2월 23일")과 같은 가시적인 인쇄 데이터를 포함하는 여권 데이터 표지(230)를 포함한다. 이러한 여권 데이터는 여권을 전달하는 기관에 의해 할당된 일부 (고유한) 일련번호(들) (여기에서는 "12345") (235)를 더 포함할 수 있다. 여권 데이터는 여권과 연관된 개인의 고유한 물리적 특성에 대응하는 데이터로서 여권 소유자의 생체 측정 데이터를 더 포함한다. 상기 생체 측정 데이터에 대응하는 상기 고유한 물리적 특성(도시되지 않음)을 특성화하는 데이터의 기계 판독 가능 표현(230e)(예를 들어, 영숫자 표현)은 여권 데이터(230)와 연관된다. 디지털 데이터의 표현은 용어의 넓은 의미로 이해되어야 한다. 이 데이터 표현은 원본 디지털 데이터를 검색할 수 있도록 하기만 하면 된다. 고유한 물리적 특성의 기계 판독 가능 데이터 표현(230e), 즉 생체 측정 데이터는 예를 들어 여권 소유자의 지문 식별 데이터 또는 홍채 식별 데이터에 대응할 수 있다. 예를 들어, 사람의 지문에 대응하는 생체 측정 데이터(230e)는 능선 끝, 분기 및 짧은 능선과 같은 지문 능선의 특정 사소한 특징의 집합에 대한 분석의 결과일 수 있다(기존의 Henry 시스템 분류에 따름).

[0213] 따라서, μ개의 전달된 생체인식 여권의 배치의 일정한 여권 A_j에 대하여(여기에서 μ = 1024), 연관된 여권 디지털 데이터 D_j는 상기 언급된 데이터(230a-230e)에 대응하는 디지털 데이터를 포함한다.

[0214] 실시예의 변형에서, 연관된 여권 디지털 데이터 D_j는 모든 전달된 여권에 대해 공통인 필드 값만을 포함할 수 있으며, 공통 필드, 즉 "여권", "성", "성별", "출생일자", "국적", "출신지", "출생지", "여권 발급일자" 및 "유효 기간" 필드가 위에서 설명한 별도의 필드 데이터 블록(FDB)에 포함되고, 예를 들어, D_1는 필드 값의 표현 "Doe", "John", "M", "1975년 3월 20일", "미국", "Des Moines", "오클랜드", "2018년 2월 24일" 및 "2020년 2월 23일"만을 포함한다.

[0215] 바람직하게는, 추가적인 여권 디지털 데이터가 위에서 언급한 여권 데이터(230)와 연관된다. 예를 들어, 여권 소유자의 지문 패턴의 디지털 이미지 또는 디지털 신원 사진 등. 실시예의 변형에서, 이러한 추가적인 여권 디지털 데이터는 일부 여권 데이터(예를 들어, 소유자의 이름 또는 생체 측정 데이터 또는 보안 표지의 데이터 또는 고유 일련번호(235))를 포함하는 정보 요청을 통해 검색할 수 있는 검색 가능한 정보 데이터베이스(250)에 저장되어 대응하는 지문 패턴 데이터를 검색하고 다시 수신한다. 바람직하게는, 정보 데이터베이스(250)에 대한 링크가 여권에 적용된 정보 접근 표지(240)에 포함된다. 여기에서 이것은 정보 데이터베이스(250)에서 대응하는 추가적인 데이터를 검색하기 위한 참조 색인을 포함하는 QR 코드이다. 그러나, 원격 정보 데이터베이스에 대한 접근을 포함하는 여권 제어 작업의 변형에서(온라인 작업), QR 코드는 예를 들어 웹을 통해 접근할 수 있는 정보 데이터베이스의 URL을 포함할 수 있다.

[0216] 여권 A_j의 여권 데이터(230a-230e)에 대응하는 여권 디지털 데이터 D_j의 단방향 해시 함수를 갖는 디지털 서명은 이제, 예를 들어, 위에서 언급한 강건한 SHA-256 해시 함수를 사용하여 계산되어 대응하는 (고유한) 여권 디지

털 서명 $x_j = H(D_j)$을 얻는다. 같은 방식으로 모든 다른 소유자에 대하여, 배치에 있는 모든 여권의 여권 디지털 서명이 계산된다.

[0217] 배치 내의 여권의 모든 서명으로부터, 위에서 설명한 바와 같이, 연관된 (이진) 트리의 트리 순서 및 트리 연결 순서에 따라 기준 루트 디지털 서명 R이 계산된다. 배치 내에 $\mu = 1024$개의 여권이 있으므로, 대응하는 이진 트리는 제1 수준에 1024 리프 노드 a(1,1),…, a(1024), 제2 수준에 512 비-리프 노드 a(2,1),…,a(2,512), 제3 수준에 256 비-리프 노드 a(3,1),…,a(3,256), …, 비-리프 노드 a(10,1) 및 a(10,2)를 갖는 끝에서 두 번째 노드 수준(여기에서는, 수준 10)까지 및 루트 노드 R(트리의 수준 11)에 대응하는 최상위 노드를 갖는다. 리프 노드 값은 $a(1,j) = x_j = H(D_j)$, $j=1,\cdots,1024$이고, 제2 수준 노드 값은 $a(2,1) = H(a(1,1)+a(1,2)),\cdots$, $a(2,512) = H(a(1,1023)+a(1,1024))$이며, …, 및 기준 루트 디지털 서명 R은 $R = H(a(10,1)+a(10,2))$이다. 따라서 각 검증 키 k_j는 10 노드 값의 시퀀스이다. 여권 A_j에 적용된 보안 표지(210)는 여권 디지털 데이터 D_j 및 대응하는 검증 키 k_j(즉, 검증 정보 $V_j = (D_j,k_j)$)를 포함한다.

[0218] 생체인식 여권 A_j의 보안 표지(210) 내의 여권 디지털 데이터 D_j와 검증 키 k_j가 실제로 배치 값 R를 갖는 μ개의 생체인식 여권 배치에 속하는 정품 생체인식 여권의 여권 데이터와 대응하는지 확인하는 연산은 여권 디지털 서명 계산 $x_j = H(D_j)$ 및 x_j 와 검증 키 k_j가 (이진 트리의 노드 순서 및 기존 연결 방식을 사용하는 트리 연결 순서에 따라) 노드 값 a(1, j)와 k_j 내의 노드 값들을 연결하는 해시 함수의 10번(여기에서, 트리는 루트 수준 아래로 10개의 수준을 가짐)의 합성을 통해 사용 가능한 대응하는 기준 루트 디지털 서명 R를 검색할 수 있는지 검증하는 것만을 필요로 한다. 결과적으로, 발명에 따라 보호되는 생체인식 여권은 보유자의 "개인 데이터"와 "생체 측정 데이터" 사이의 위조 방지 링크와 보유자의 실제 사람과 보유자의 신원 사이의 고유하고 위조 방지인 링크를 모두 제공한다.

[0219] 도 2b는 도 2a의 보안 생체인식 여권 A_1의 제어 프로세스를 도시하며, 여권 데이터 표지(230)는 특정 John Doe에 대응하고, 그 생체 측정 데이터(230e)는 John Doe의 지문에 대응하며, 추가적인 여권 디지털 데이터는 정보 접근 표지(240)에 포함된 정보 데이터베이스(250)에 대한 링크를 통해 접근할 수 있는 John Doe의 디지털 신원 사진(255)에 대응한다. 여권 데이터는 여권을 전달한 기관에 의해 할당된 고유 일련번호(235)를 더 포함한다. 여권 A_1에 적용된 보안 표지(210)는 검증 정보 (D_1, k_1), 인쇄된 여권 데이터(230a-230d), 생체 측정 데이터(230e) 및 고유 일련번호(235)에 대응하는 여권 디지털 데이터 D1, 및 ($a(1,1) = x_1 = H(D_1)$를 사용하여) 여권 A_1의 노드 값 a(1,1)로부터 루트 값 R을 검색하기 위하여 필요한 10개의 노드 값 {a(1,2),a(2,2),…,a(10,2)}의 시퀀스에 대응하는 검증 키 k_1을 포함한다. 기준 루트 디지털 서명 R는 타임스탬프가 찍혀 블록체인(260)에 저장될 수 있다. 이 예에서, 배치의 생체인식 여권의 각 소유자의 생체 측정 데이터(230e)는 각각 대응하는 고유 일련번호와 연관되어 (이들 데이터를 불변으로 만들기 위하여) 블록체인(260)에 저장된다. John Doe의 저장된 생체 측정 데이터는 자신의 여권에 언급된 고유 일련번호(235)를 나타내는 요청을 블록체인(260)에 전송하여 검색할 수 있다. 사람들의 신원을 제어하는 권한을 가진 기관(예를 들어, 경찰, 세관 등)은 통신 링크를 통해 블록체인(260)에 접근할 수 있으며, 이 예시적인 실시예에서 전달된 모든 생체인식 여권 배치의 (게시된) 루트 디지털 서명을 저장하기 위한 로컬 저장 기능도 가지고 있다. 도 2b에 도시된 예에서, 정보 데이터베이스(250)는 로컬이다(즉, 공공 통신 네트워크를 사용하지 않고 기관이 직접 접근 가능). 또한, 이들 기관은 개인의 지문을 캡처하고 캡처된 지문을 특성화하는 데이터, 즉 생체 측정 데이터(230e)의 대응하는 기계 판독 가능 표현을 계산하기 위해 지문 스캐너(270)를 갖추고 있다.

[0220] 경찰이나 세관 관리에 의한 John Doe의 신원 관리 중에 관리는 John Doe의 보안 생체인식 여권 A_1을 가져 와서 여권의 보안 표지(210)에 저장된 검증 정보(D_1, k_1)를 컴퓨터(290)(영상장치를 형성)에 연결된 적절한 휴대용 판독기(280)를 사용하여 판독 및 해독하며, 컴퓨터는 로컬 저장 기능(250)에 연결되어 있다. 여권 디지털 데이터 D_1 및 검증 키 k_1을 판독한 다음 이를 컴퓨터(290)로 전송하며, 컴퓨터(290)에서 실행되는 전용 애플리케이션(프로그래밍된 해시 함수 H 및 노드 값의 연결 포함)은 여권 디지털 서명 x_1을 ($x_1 = H(D_1)$로) 및 후보 배치 값 R^c를:

[0221] H(H(H(H(H(H(H(H(a(1,1)+a(1,2))+a(2,2))+..)+..)+..)+..)+..)+..)+a(9,2))+a(10,2)),

[0222] 즉, 노드 값 a(1, 1) 및 k_1= {a(1,2),a(2,2),…,a(10,2)} 내의 노드 값들을 연결하는 해시 함수의 10번의 합성으로 계산한다. 그런 다음, 컴퓨터는, 예를 들어, 로컬 정보 데이터베이스(250)에서 후보 R^c 값과 일치하는 기준 루트 디지털 서명 R를 검색할 수 있다. 일치하는 항목이 없는 경우 여권은 위조된 여권이고 "John Doe"(즉, 그의 이름이 John Doe라고 주장하는 심사되는 개인)는 체포될 수 있다. R^c가 기준 루트 디지털 서명과 일치하는 경우 여권은 정품으로 간주되며 관리는 추가 보안 검사를 수행할 수 있다.

[0223] - 관리는 A_1에 인쇄된 일련번호(235)가 포함된 컴퓨터(290)를 통해 요청을 전송함으로써 정보 데이터베이스(250)에 저장된 디지털 신원 사진(255)을 검색하고, 이를 다시 수신하여 수신된 신원 사진(255)을 컴퓨터(290)의 화면에 표시한다. 그러면 관리는 표시된 얼굴(즉, 특정 John Doe의 얼굴)을 확인 중인 개인의 얼굴과 시각적으로 비교하고 두 얼굴이 유사한지 여부를 평가할 수 있다.

[0224] - 관리는 컴퓨터(290)에 연결된 휴대용 판독기(280)로 보안 표지(210) 상의 데이터를 판독함으로써 여권 A_1 상의 생체 측정 데이터(230e)를 검색하고, 컴퓨터(290)에 연결된 지문 스캐너(270)를 통해 개인의 지문을 스캔하고 대응하는 개인의 생체 측정 데이터를 획득한다. 관리는 검색된 생체 측정 데이터(230e)가 획득된 개인의 생체 측정 데이터와 유사한지(주어진 오차 범위 내에서) 컴퓨터(290)에서 실행되는 프로그램을 통해 확인한다.

[0225] 두 얼굴과 생체 측정 데이터가 유사하다고 판단되면, 모든 것이 정상이며, 확인된 사람은 정품 생체인식 여권 A_1의 소유자인 실제 John Doe이다.

[0226] 위의 추가적인 보안 검사 중 하나가 실패하는 경우, 관리 앞에 있는 개인은 정품 생체인식 여권 A_1의 진실한 소지자가 아니며, 특정 John Doe의 여권을 훔쳤을 가능성이 있다. 따라서, 본 발명에 따른 보안 생체인식 여권을 사용하면 단순한 오프라인 확인으로 모든 사기를 빠르게 탐지할 수 있다.

[0227] 실제로, 검증 정보 V = (D, k)를 포함하는 인쇄된 2D 바코드(위의 QR 코드의 예와 같음)만으로 생체인식 여권 문서를 단순한 종이 조각으로 줄일 수도 있으며, V는 소지자의 인명 데이터 및 소지자의 지문과 같은 (고유한) 생체 측정 데이터(여권 디지털 데이터 D 내) 및 검증 키 k를 포함한다. 실제로, 본 발명에 따르면, 이 “축소된” 보안 여권조차도 “개인 인명 데이터”와 여권 소지자의 “생체 측정 데이터” 사이에 생성된 위에 언급된 위조 방지 링크 및 보유자의 실제 사람과 보유자의 신원 사이의 고유하고 위조 방지된 링크의 전체 이점을 누릴 수 있다.

[0228] 본 발명의 다른 예시적인 실시예는 도 3에 도시된 바와 같이 항공기의 구성품에 관한 것이다. 랜딩 기어 또는 리액터의 부품(예를 들어, 터빈 블레이드, 펌프…) 또는 배터리 등과 같이 고장이 항공기의 보안에 영향을 미칠 수 있는 특정 중요 구성품의 가격이 매우 높기 때문에, 위조자들은 이러한 구성품의 복제품을 제조하지만, 일반적으로 품질이 낮기 때문에 필요한 안전 기술 요구 사항을 준수하지 않는다. 항공기 구성품에는 일반적으로 식별을 위해 대응하는 고유 일련번호가 표시되어 있지만, 이러한 표지는 쉽게 위조될 수 있다. 이들 위조 비행기 부품은 일반적으로 결함이 있으며 심각한 손상이나 비행기 추락을 일으킬 수 있다. 이것은 오늘날 증가하는 보안 문제이다. 또한 구성품이 정품이더라도, 동일한 유형의 항공기의 어떤 버전에는 편리하지 않을 수 있으며, 예를 들어 특정 항공기를 수리하는 데 부적절한 구성품이 부주의하게 사용되는 심각한 위험이 있다. 따라서 특정 항공기에 허용되는 적어도 중요한 정품 구성품을 확보하는 것이 중요하다.

[0229] 일반적으로 각 구성품은, 예를 들어, 구성품 기술명, 구성품 고유 일련번호, 구성품 제조업체명, 구성품의 제조일자 및 보증 정보를 나타내는 대응하는 기술 데이터 시트가 있다. 또한, 특정 항공기에 대하여, 대응하는 기록에는 각 구성품의 모든 기술 데이터 시트가 포함되어 있다. 그러나, 위조된 구성품에는 대응하는 위조 기술 데이터 시트가 있을 수 있으므로, (예를 들어, 기술 테스트를 수행하지 않는 한) 사기를 감지하는 것이 용이하지 않다. 예를 들어, 기술 데이터 시트가 특정 항공기에 장착된 구성품과 잘 일치하는지 확인하는 방법은 무엇인가(역도 마찬가지)?

[0230] 본 발명의 예시적인 실시예에 따르면, 특정 항공기의 제조 또는 수리에 사용되거나 항공기에 장착된 허용된 부품은 바로 그 항공기에 대한 "물품"의 배치에 속하는 것으로 간주된다.

[0231] 도 3에 도시된 특정 예시적인 실시예에서, 항공기 배치의 각 물품, 즉 특정 항공기에 장착 또는 수리를 위해 허용된 각 항공기 구성품은 기존 기술 데이터 시트에서와 동일한 구성품 데이터(예를 들어, 항공기 ID 코드, 항공기 제조업체명, 구성품 기술명, 구성품 고유 일련번호, 구성품 제조업체명 및 구성품 제조일자)와 함께, 항공기 ID 코드, 항공기 제조업체명, 항공기 구성품의 조립일자, 적합성 검사를 수행한 기술자명 및 적합성 검사일자,

및 검사자의 대응하는 (고유한) 디지털 서명에 대응하는 추가 디지털 데이터를 포함하는 항공기 구성품 식별 문서 AC-ID를 갖는다. 또한 각 항공기 구성품 식별 문서 AC-ID는 (바람직하게는 변조 방지) 기계 판독 가능 보안 표지가 적용되어 보호된다. 바람직하게는, 구성품 또는 구성품 세트가 항공기에서 교체될 때마다, 대응하는 보안 AC-ID 문서가 생성되고 대응하는 항공기 배치의 업데이트된 버전이 위에서 언급한 (새로운 장착 작업과 관련된) 대응하는 추가 디지털 데이터와 함께 또한 생성된다.

[0232] 따라서 (여기에서는 항공기 ID 참조 HB-SNO를 갖는) 특정 항공기에 장착된 모든 (중요한) 구성품은 대응하는 장착된 구성품 배치(여기에서는 총 μ개의 구성품을 포함)에 속한다. 보안 표지(310)(여기에서는 QR 코드 형식), 예를 들어, AC-ID : A_{125}(항공기 HB-SNO에 장착된, 여기에서는 A_{125}인, 대응하는 항공기 구성품과 연관됨)가 각 항공기 구성품 식별 문서에 인쇄된다. 도 3은 특히 항공기 배치의 구성품 A_{125}가 항공기 HB-SNO에 장착된 리액터 유형에 맞게 조정되고 고유한 제조 일련번호(여기에서는 12781, 일반적으로 제조업체가 각인)가 표시된 터빈 블레이드인 것을 나타낸다. 구성품 A_{125}와 연관된 구성품 디지털 데이터 D_{125}(또는 물품 디지털 데이터)는 AC-ID : A_{125} 상에 인쇄된 데이터 표지(330)에 대응하는 디지털 데이터를 포함하고: 항공기 ID 코드(330a)(여기에서는 HB-SNO), 항공기 제조업체명(330b)(여기에서는 AeroABC), 구성품 기술명(330c)(여기에서는 터빈 블레이드-제1링), 구성품 일련번호(330d)(여기에서는 12781), 구성품 제조업체명(330e)(여기에서는 PCX), 구성품의 제조일자(330f)(여기에서는 2017년 11월 13일), 리액터(330g) 상의 구성품 조립일자(여기에서는 2018년 2월 24일), 적합성 검사를 수행하는 기술자명(330h)(여기에서는 검사자가 마틴 화이트)과 적합성 검사일자(330i)(여기에서는 2018년 3월 20일), 및 검사자의 (고유한) 디지털 서명(330j)(여기에서는 2w9s02u)이다.

[0233] 구성품 A_{125}의 AC-ID: A_{125}의 구성품 디지털 데이터 D_{125}의 구성품 디지털 서명 x_{125}는 $x_{125} = H(D_{125})$와 같이 단방향 해시 함수 H에 의해 계산된다. 마찬가지로, 구성품 A_i의 구성품 디지털 데이터 D_i의 모든 구성품 디지털 서명 x_i는 단방향 해시 함수 H에 의해 $x_i = H(D_i)$(여기에서, $i = 1,\cdots, \mu$)이다. 발명에 따르면, 구성품 배치와 연관된 트리(여기에서는, 이진 트리)는 구성품 $A_1,\cdots,A_\mu$의 구성품 식별 문서 AC-ID:$A_1,\cdots,$AC-ID:A_μ 의 각 구성품 디지털 데이터 $D_1,\cdots,D_\mu$의 μ 구성품 디지털 서명 $x_1,\cdots,x_\mu$에 각각 대응하는 μ 리프 노드 a(1,1),…,a(1,μ)를 갖도록 형성된다. 여기에서, 이진 트리의 노드 순서는 통상적인 것으로서, 즉 노드 a(i,j)는 인덱스 (i,j) 값에 따라 배열되고, 인덱스 i는 리프 노드 수준(i=1)에서 시작하여 루트 노드 아래의 끝에서 두 번째 노드 수준까지 트리 내의 수준을 표시하며, 인덱스 j는 리프 노드 수준(수준 1)에서 1부터 μ까지, 다음 (비-리프) 노드 수준(수준 2)에서 1부터 $\mu/2$까지, …, 및 끝에서 두 번째 노드 수준에서 1부터 2까지 이어진다. 트리는 리프 노드에서 루트 노드까지의 노드 수준을 포함하고, 트리의 모든 비-리프 노드는 트리 연결 순서에 따라 그 자식 노드의 각 디지털 서명의 연결의 단방향 함수 H에 의한 디지털 서명에 대응한다.

[0234] μ 항공기 구성품 $A_1,\cdots A_\mu$의 배치에 대한 기준 루트 디지털 서명 R이 트리의 노드 값의 (통상적인) 연결의 단방향 함수를 사용하여 계산된다(이하에서 설명됨). 기준 루트 디지털 서명 R은 그런 다음 장착된 구성품의 제어 또는 교체를 담당하는 기술자가 접근할 수 있는 검색 가능한 데이터베이스(바람직하게는 블록체인)에 저장된다. 따라서 트리는 리프 노드로부터 트리의 루트 노드까지의 노드 수준을 포함하며, 트리의 모든 비-리프 노드는 (여기에서는 통상적인)트리 연결 순서에 따라 그 (두 개의) 자식 노드의 각 디지털 서명의 연결의 단방향 함수 H에 의한 디지털 서명에 대응하고, 루트 노드는 기준 루트 디지털 서명 R, 즉 (트리 내의 노드 순서 및 트리 연결 순서에 따라) 트리 내의 끝에서 두 번째 노드 수준의 노드의 디지털 서명의 연결의 단방향 함수 H에 의한 디지털 서명에 대응한다.

[0235] 배치의 주어진 구성품 A_i에 대하여, 구성품 디지털 데이터 D_i의 구성품 디지털 서명 x_i(즉 리프 노드 a(1,i))에 대응하는 검증 키 k_i가, 트리의 리프 노드 수준으로부터 끝에서 두 번째 노드 수준까지, 물품 디지털 서명 x_i에 대응하는 리프 노드 a(1,i)와 동일한 부모 노드를 갖는 트리 내의 모든 다른 리프 노드, 및 트리 내의 각 다음 수준에서 연속적으로, 이전 수준에서 고려된 이전 동일한 부모 노드와 동일한 부모 노드를 갖는 트리 내의 모든 비-리프 노드의 각 디지털 서명의 시퀀스로 계산된다. 항공기 HB-SNO에 장착된 각 구성품 A_i에 대하여, 연관된 구성품 디지털 데이터 D_i 및 대응하는 검증 키 k_i가 대응하는 항공기 구성품 식별 문서 AC-ID:A_i에 적용된 보안 표지에 내장된다.

[0236] 예를 들어, HB-SNO 항공기의 구성품을 제어하는 작업의 경우, 기술자는 적절한 판독기를 사용하여 제어할 구성품 A_{125}의 A_{125} AC-ID에서 판독한 구성품 일련번호 12781, 또는 대응하는 AC-ID : A_{125} 문서의 보안 표지(310)에서

판독한 그 검증 키 k_{125}을 포함하는 검색 가능한 데이터베이스로 요청을 보낼 수 있으며 대응하는 배치 값 R를 수신할 것이다. 그러나 완전한 오프라인 검사를 허용하는 바람직한 변형에서, 기술자의 판독기는 제어할 항공기와 관련된 모든 루트 디지털 서명을 저장하는 메모리가 있는 컴퓨터에 연결된다. 후자의 변형에서, 기술자는 보안 표지(310)의 구성품 디지털 데이터 D_{125}를 판독하고, D_{125}에서 추출한 고유 일련번호(330d)(여기에서는 12781)가 장착된 항공기 구성품 A_{125}에 물리적으로 표시된 일련번호와 일치하는지 확인하고, 대응하는 구성품 디지털 서명 x_{125}을 계산하고(예를 들어, 판독된 디지털 데이터 D_{125}에서 서명 $x_{125} = H(D_{125})$를 계산하는 프로그래밍된 애플리케이션을 컴퓨터의 처리 유닛에서 실행하여), 리프 노드 값 $a(1,125)=x_{125}$ 및 대응하는 검증 키 k_{125} 내에 주어진 노드 값의 연결의 해시로 컴퓨터의 처리 유닛에서 프로그래밍된 단방향 함수 H를 통해 후보 배치 값 R^c를 계산하고, 후보 배치 값 R^c이 컴퓨터 메모리에 저장된 기준 루트 디지털 서명 중 하나(즉, 항공기 HB-SNO에 대응하는 R)와 일치하는지 확인하여 구성 요소가 정품인지 확인할 수 있다. 전체 일치(즉, 일련번호 일치 및 R^c = R)의 경우, 구성품 A_{125}는 정품으로 간주되며 HB-SNO 항공기의 허용된 구성품의 (최신) 항공기 배치에 속한다. R^c가 저장된 기준 루트 디지털 서명 R와 일치하지 않거나, 일련번호가 일치하지 않는 경우, 구성품 A_{125}는 위조품일 수 있거나, 항공기 HB-SNO에 허용되지 않는 정품 구성품이며(예를 들어, A_{125}는 이 항공기에 대한 올바른 배치에 속하지 않음), 변경되어야 한다.

[0237] 동일한 방식으로, 본 발명은 저장된 부품에 대한 보안 표지의 진정성을 검증하고 보안 표지로부터의 구성품 일련번호가 대응하는 구성품에 표시된 것과 일치하는지 확인함으로써 창고에 저장된 교체 부품의 보안 AC-ID 배치에서 사기(또는 오류)를 감지할 수 있다. 매우 중요한 구성품의 경우, 변조 방지 물질 기반 보안 표지가 구성품에 추가로 적용될 수 있으며, 이 표지의 대응하는 기준 고유 물리적 특성, 즉 특성 디지털 데이터 CDD와 관련된 디지털 데이터(예를 들어, 물질 기반 보안 표지를 적용할 때 적절한 센서에 의해 캡처됨)는 바람직하게는 이 구성품의 보안 표지에서 구성품 디지털 데이터 D의 일부로 되고, 대응하는 기준 고유 물리적 서명 데이터 UPS가 계산되며(예를 들어, 특징 디지털 데이터 CDD의 해시를 취함으로써 즉, UPS = H(CDD)) 또한 구성품 디지털 데이터의 일부일 수도 있다. 이러한 추가적인 보안 수준은 제조업체가 구성품에 표시한 고유 일련번호로 제공되는 보안을 향상시킨다. 바람직하게는 기준 UPC 및 UPS는 (불변으로 만들기 위하여) 블록체인에 저장되어 기술자가 접근할 수 있다. 또한 이들 기준 값은 매우 중요한 구성품의 물질 기반 보안 표지의 오프라인 인증을 허용하기 위하여 기술자 컴퓨터의 메모리에 추가로 저장될 수 있다.

[0238] 이 물질 기반 보안 표지의 추가 오프라인 인증 작업에는 컴퓨터에 연결된 적절한 센서를 사용하여 구성품의 고유한 물리적 특성을 측정하고 (예를 들어, 컴퓨터의 처리 유닛에 프로그래밍된 특정 애플리케이션을 통해) 측정된 특성으로부터 후보 특성 디지털 데이터 CDD^c를 얻는 것이 포함될 수 있다. 그런 다음 기술자(또는 적절하게 프로그래밍된 경우, 컴퓨터의 처리 유닛)는 획득한 CDD^c를 컴퓨터의 메모리에 저장된 기준 CDD의 사본과 비교한다. "합리적인" 일치 $CDD^c \approx CDD$의 경우(즉, 일부 사전 정의된 오류 공차 기준 이내), 물질 기반 보안 표지 및 따라서 구성품은 정품으로 간주된다.

[0239] 위에서 언급했듯이, 기준 특성 디지털 데이터 CDD의 사본은, 기술자 컴퓨터의 메모리에 저장되는 대신, 구성품에 적용된 보안 표지에 포함된 물품 디지털 데이터 D의 일부이며 (판독기를 사용하여) 보안 표지 상에서 직접 판독하여 얻을 수 있다. 기술자는 보안 표지에서 후보 CDD^c를 판독하고 컴퓨터 메모리에 저장된 서명 UPS가 $UPS^c = H(CDD^c)$를 계산하여 판독한 후보 CDD^c로부터 계산된 후보 서명 UPS^c와 일치하는지 확인할 수 있다. UPS^c = UPS로 일치하면, 물질 기반 보안 표지 및 따라서 구성품은 정품임이 확인된다.

[0240] 실시예의 변형에서, 기술자에 의한 구성품의 진정성 확인은 대안적으로 본 발명의 제1 상세한 실시예에서 이미 설명된 것과 유사한 방식으로 온라인 프로세스를 통해 수행될 수 있으며, 여기에서 반복되지는 않는다.

[0241] 발명에 따르면, 원본 보안 문서에 대해, 예를 들어, 항공기 구성품 식별 문서 AC-ID : A_{125}와 같은 보안 문서의 디지털 이미지의 적합성을 검증하는 것도 가능하다. 실제로, 제어(또는 수리) 작업을 담당하는 기술자가 예를 들어 판독기(예를 들어, 적절하게 프로그래밍된 스마트폰일 수 있음)에서 AC-ID : A_{125} 이미지를 수신함으로써, 보안 문서의 디지털 이미지에만 접근할 수 있는 경우에도, 다음 작업을 수행하여 수신된 문서 이미지에 인쇄된

구성품 데이터가 원본 문서의 것과 대응하는지 확인할 수 있다.

[0242] -문서 AC-ID : A_{125}의 디지털 이미지 상의 보안 표지(310)의 이미지 상의 구성품 디지털 데이터 D_{125} 및 검증 키 k_{125}를 판독;

[0243] -문서 AC-ID : A_{125}에 대응하는 배치의 기준 배치 값 R 획득; 이 기준 값은 판독기 (또는 판독기에 연결된 컴퓨터)의 메모리에 이미 있거나, 판독기에 통신 장치가 장착된 경우 항공기 구성품의 기준 배치 값을 저장하는 데이터베이스에서 통신 링크를 통해, 예를 들어, 보안 표지(310)의 이미지의 판독된 구성품 (고유) 일련번호 또는 단지 키 k_{125}를 포함하는 요청을 전송하고, 대응하는 기준 배치 값 R를 수신함으로써 얻을 수 있다;

[0244] - $x_{125} = H(D_{125})$를 사용하여, 판독된 구성품 디지털 데이터 D_{125}로부터 구성품 디지털 서명 x_{125}를 계산(프로그래밍된 단방향 함수 H 사용);

[0245] - 리프 노드 값 x_{125} 및 검증 키 k_{125} 내에 표시된 노드 값의 연결(트리 내의 노드 순서 및 트리 연결 방식에 따라)의 해시 함수 H의 디지털 서명으로서 후보 배치 값 R^c 계산(프로그래밍된 단방향 해시 함수 H 사용); 및

[0246] -후보 배치 값 R^c가 기준 배치 값 R와 일치하는지 검증.

[0247] 위에서 언급한 적합성 검증 작업은 원본 문서 AC-ID : A_{125}의 단순한 사본으로도 수행할 수 있다. 실제로 복사 방지 기능이 원본 문서의 보안 표시에 있어서 기술자가 단지 사본을 갖고 있음이 밝혀지더라도, 사본의 보안 표지에 있는 데이터를 읽고 원본 데이터에 대해 사본에서 판독한 데이터의 적합성을 검증하는 작업을 수행할 수 있다.

[0248] 본 발명의 다른 예시적인 실시예는 도 4에 도시된 바와 같이 의약품 팩과 같은 의약품의 자체 보안 번호부여 체계(serialization)에 관한 것이다. 이 실시예는 μ 상자(또는 물품) A_1, …, A_μ를 포함하는 특정 유형의 약제의 의약품 팩의 생산 배치에 관한 것이다. 도 4에 도시된 전형적인 상자 A_1의 이 예시적인 예에서, 환자용 정제는 상자 A_1에 포함된 일련의 블리스터 팩(401)(하나만 도시됨)에 포장된다. 각 블리스터 팩(401)에는 고유한 일련번호(435)(여기에서는 "12345", 제조업체에서 적용)가 표시되어 있으며, 상자 A_1에는 의약품명(430a), 로고(430b), 상자 고유 일련번호(상자 ID)(430c), 유효기간(430d)과 같은 기존 정보가 인쇄되어 있다. 이 예에서, 권장 소매 가격(430e), 판매 국가(430f) 및 판매 제한 표시(430g)(예를 들어, 약국에서만 판매)의 추가 기존 데이터가 상자에(또는, 변형의 경우, 상자 A_1에 넣은 패키지 전단지에) 인쇄될 수 있다. 상자 A_1은 인쇄된 2D 바코드(또는 데이터 매트릭스) 형태의 기계 판독 가능 보안 표지(410)에 의해 보호되고, 추가로 상자 A_1에 적용되는 무작위로 분산된 입자를 포함하는 별도의 변조 방지 접착 복사 방지 스탬프(415) 형태의 물질 기반 보안 표지로 보호된다. 실제로 스탬프 상의 입자의 (무작위이며 따라서 고유한) 위치는 상자 A_1에 적용된 스탬프(415)의 고유한 물리적 특성을 구성하는 것으로 알려져 있으며, 따라서 여기에서도 상자 A_1 자체의 고유한 물리적 특성을 구성한다. 스탬프(415) 상에서 분산된 입자의 검출된 위치는 통상적으로 상자 A_1의 대응하는 기준 특성 디지털 데이터 CDD-A_1을 계산하는 데 사용된다. 일반적으로 분산된 입자 및 그 위치의 검출은 스탬프의 디지털 이미지의 이미지 처리를 통해 수행된다. 여기에서, 입자는 예를 들어 스마트폰의 플래시와 같이 단순한 흰색 플래시(예를 들어, 흰색 LED)로 스탬프를 조명할 때 검출할 수 있다. 바람직하게는, 스탬프(415)를 이미지화하고, 분산된 입자의 위치를 검출하고, 이들 위치로부터 대응하는 특성 디지털 데이터 CDD를 계산할 수 있도록 하기 위하여 특정 이미지 처리 애플리케이션을 스마트폰에 다운로드할 수 있다.

[0249] 발명에 따르면, 배치의 상자 A_i($i \in \{1,\cdots, \mu\}$)의 바코드(410)는 상자 A_i의 위에서 언급한 종래 데이터(430a-430g)의 디지털 표현에 대응하는 상자 디지털 데이터 D_i, 상자 Ai에 포함된 블리스터 팩(401)의 각각의 일련번호(435) 및 상자 A_i의 기준 고유 물리적 특성 디지털 데이터 CDD-A_i를 포함한다. 배치의 각 상자 A_i에 대하여, 그 상자 디지털 데이터 Di의 연관된 상자 디지털 서명 x_i는 단방향 해시 함수 H를 통해 $x_i = H(D_i)$, $i = 1,\cdots, \mu$와 같이 계산된다.

[0250] 상자의 배치와 연관된 트리(여기에서는, 이진 트리)가 상자 $A_1,\cdots,A_\mu$의 각 상자 디지털 데이터 $D_1,\cdots,D_\mu$ 의 μ

상자 디지털 서명 $x_1,\cdots,x_\mu$ 에 각각 대응하는 μ 리프 노드 a(1,1),…,a(1,μ)를 갖도록 형성된다. 여기에서, 이진 트리의 노드 순서는 통상적인 것으로서, 즉 노드 a(i,j)는 인덱스 (i,j) 값에 따라 배열되고, 인덱스 i는 리프 노드 수준(i=1)에서 시작하여 루트 노드 아래의 끝에서 두 번째 노드 수준까지 트리 내의 수준을 표시하며, 인덱스 j는 리프 노드 수준(수준 1)에서 1부터 μ까지, 다음 (비-리프) 노드 수준(수준 2)에서 1부터 μ/2까지, …, 및 마지막으로 끝에서 두 번째 노드 수준에서 1부터 2까지 이어진다. 트리는 리프 노드 a(1,1), …,a(1,μ)에서 루트 노드까지의 노드 수준을 포함하고, 트리의 모든 비-리프 노드는 트리 내의 노드 순서 및 트리 연결 순서에 따라 그 자식 노드의 각 디지털 서명의 연결의 단방향 해시 함수 H에 의한 디지털 서명에 대응한다(루트 노드는 기준 루트 디지털 서명에 대응한다).

[0251] 그런 다음 배치의 모든 상자에 대한 기준 루트 디지털 서명 R이 단방향 해시 함수 H를 사용하여 (트리 내의 노드 순서 및 트리 연결 순서에 따라) 트리 내의 끝에서 두 번째 노드 수준의 노드의 디지털 서명의 연결의 디지털 서명으로서 계산된다.

[0252] 획득된 기준 루트 디지털 서명 R는 이제 보안 의약품 팩 A_i의 유효성을 확인하여야 하는 사용자가 접근할 수 있는 미디어에 게시되거나, 또는 사용자가 접근할 수 있는 검색 가능한 루트 데이터베이스에 저장되거나, 또는 사용자가 접근할 수 있는 블록체인(또는 블록체인으로 보호되는 데이터베이스)에 저장된다. 예를 들어, 사용자는 상기 상자 A_i의 보안 표지(410)에서 판독된 일련번호(430c)가 포함된 요청을 검색 가능한 루트 데이터베이스 또는 블록체인으로 전송하고, 대응하는 기준 배치 값 R를 다시 수신할 수 있다. 검색 가능한 루트 데이터베이스에 (예를 들어, 웹을 통해) 또는 블록체인에 접근하기 위한 링크는 상자 A_i에 인쇄된 상자 데이터 표지(440)(도 4에서 QR 코드로 도시됨)에 포함될 수 있다. 바람직하게는, 기준 루트 디지털 서명 R는 사용자가 로컬에서 사용할 수 있게 되어, 사용자가 오프라인 모드(즉, R를 얻기 위해 원격 저장 수단에 접근할 필요가 없음)에서 검사 작업을 수행할 수 있다. 예를 들어, 사용자는 (스마트폰의 처리 유닛에서 실행될 수 있는 프로그래밍된 애플리케이션에 의해) 상자 A_i의 보안 표지(410)에 있는 데이터를 판독하고 디코딩할 수 있는 스마트폰과 같은 판독기를 가지며 그 메모리는 기준 루트 디지털 서명 R를 저장한다.

[0253] μ 의약품 팩의 배치의 각 상자 A_i에 대하여, 상자 디지털 서명 x_i, 즉 리프 노드 a(1,i)와 연관된 검증 키 k_i가 대응되고, 트리의 리프 노드 수준으로부터 끝에서 두 번째 노드 수준까지, 물품 디지털 서명 x_i에 대응하는 리프 노드 a(1,i)와 동일한 부모 노드를 갖는 트리 내의 모든 다른 리프 노드, 및 트리 내의 각 다음 수준에서 연속적으로, 이전 수준에서 고려된 이전 동일한 부모 노드와 동일한 부모 노드를 갖는 트리 내의 모든 비-리프 노드의 각 상자 디지털 서명의 시퀀스로 계산된다.

[0254] 상자 디지털 데이터 D_i 및 그에 대응하는 상자 검증 키 k_i(함께 상자 A_i의 검증 정보 V_i를 구성함)는 상자 A_i에 적용된 보안 표지(410)에 포함된 디지털 데이터의 일부이다.

[0255] 기준 루트 디지털 서명 R를 갖는 상자 배치에 속하는 도 4의 보안된 상자 A_1의 진정성 검증은 상자 A_1의 보안 표지(410)에 있는 상자 디지털 데이터 D_1을 판독 및 디코딩하고(적절한 판독기를 사용하여, 예를 들어, 단방향 해시 함수 H를 사용하여 서명을 계산하고 검증 정보 $V_1=(D_1,k_1)$로부터 루트 노드 값을 검색하기 위한 추가 프로그래밍된 애플리케이션이 있는 위에서 언급한 스마트폰을 사용하여), 단방향 함수 H를 사용하여 $x_1 = H(D_1)$로 대응하는 상자 디지털 서명 x_1을 계산하고, 기준 루트 디지털 서명(배치 값) R(이 예에서는 기준 배치 값 R가 판독기의 메모리에 저장됨)를 획득하고, (리프 노드 a(1,1)의) 리프 노드 값 및 검증 키 k_1에 의해 표시된 노드 값의, 트리 내의 노드 순서 및 트리 연결 방식에 따른, 연결의 단방향 해시 함수 H에 의한 디지털 서명으로서 획득한 기준 루트 디지털 서명 R가 판독된 검증 정보 (D_1, K_1)에서 획득한 후보 루트 디지털 서명 R^c와 일치하는지 확인하기만 하면 된다. $R^c \neq R$ 이면 상자 A_1은 위조품이다. $R^c = R$ 인 경우, 보안 표지(410)는 정품 상자에 대응한다. 이 경우, 몇 가지 추가 보안 검사를 수행할 수 있다. 예를 들어, 디스플레이가 장착된 판독기(위에서 언급한 스마트폰과 같은)의 경우, 판독된 상자 디지털 데이터 D_1에서 정보(430a-430d) 중 하나를 추출하고, 추출된 정보를 표시하고 상자 A1에 인쇄된 대응하는 정보와 일치하는지 시각적으로 확인할 수 있다. 표시된 정보가 인쇄된 정보와 일치하지 않는 경우 상자는 위조품이다.

[0256] 물질 기반 보안 표지(415)가 정품임을 검증함으로써 상자 A_1의 추가 인증 확인이 가능하다. 스탬프(415)를 영상

화함으로써(예를 들어, 위에서 언급한 영상 처리 성능이 있는 스마트폰으로) 분산된 입자의 위치를 검출하고, 이들 위치로부터 대응하는 후보 특성 디지털 데이터 CDD^{c}-A_1을 계산하고, 그런 다음 이 CDD^{c}-A_1이 상자 디지털 데이터 D_1에서 추출된 기준 고유 물리적 특성 디지털 데이터 CDD-A_1과 실제로 유사한지(주어진 오차 범위 내에서) 확인하는 것으로 충분하다. 이들이 스탬프(415)와 일치하면, 따라서 상자 A_1은 정품이며, 스탬프(415)와 일치하지 않으면, 상자 A_1(스탬프는 변조 방지됨)은 위조품이다.

[0257] 여전히 루트 디지털 서명의 일치가 검증된 경우(즉, R^{c} = R), 정보(430a-430d)가 검증되었거나 및/또는 물질 기반 보안 표지(415)가 정품인 경우에도, 상자 A_1에 포함된 블리스터 팩(401)이 올바른 것인지 확인하는 것이 가능하다. 블리스터 팩에 표시된 고유 일련번호(435)가 보안 표지(410)에서 판독된 상자 디지털 데이터 D_1에 표시된 것과 일치하는지 확인하는 것으로 충분하다. 이들 데이터가 일치하지 않으면, 이는 사기의 증거이다. 정품 상자 A_1의 블리스터 팩이 다른 것으로 교체되었다(가능하게는 위조되었거나, 또는 상이한 의약품에 대응하는 다른 표지의 것이다). 또한 진정한 상자 A_1의 경우(즉 R^{c} = R), 블리스터 팩(401)이 올바른 경우에도 상자 디지털 데이터 D_1에서 추출된 추가 정보 중 임의의 것, 즉 권장 소매가(430e), 판매 국가(430f) 및 판매 제한 표시(430g)가 경험된 판매 조건과 일치하지 않는 경우(예를 들어, 의약품 A_1이 데이터(430f)에 표시된 국가와 다른 국가에서 판매된 경우) 대응하는 사기를 검출할 수 있다. 이는 또한 배치 자체, 또는 적어도 그 일부가 우회되었다는 심각한 경고를 구성한다.

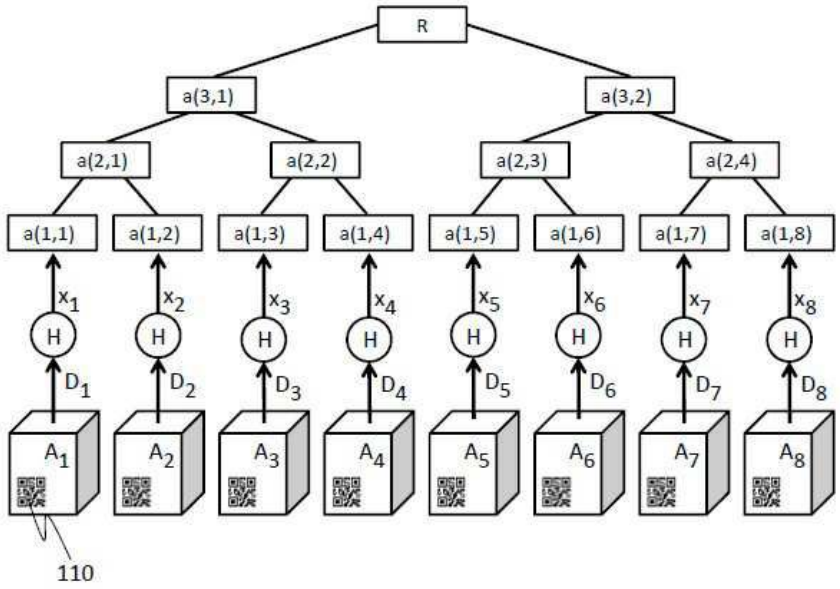
[0258] 따라서, 상자 데이터, 포함된 블리스터 팩의 블리스터 팩 데이터, 상자와 그 블리스터 팩의 고유한 특성화 물리적 특성 및 특정 배치에 대한 상자의 소속 사이의 루트 디지털 서명에 의해 본 발명에 따라 제공되는 위조 방지 링크로 인하여 보안 의약품 팩의 전체 트랙 및 추적 작업과 인증 확인이 모두 가능하다.

[0259] 위의 상세한 설명에 따르면, 본 발명은 보안 물품의 진정성 또는 원본 보안 물품과 연관된 데이터에 대하여 보안 물품의 이미지(또는 사본) 상의 데이터의 적합성을 검증하기 위한 오프라인 및 로컬 검사 작업과 명확하게 호환된다. 그러나, 본 발명은 또한 예를 들어 외부 소스(예를 들어, 서버 또는 블록체인)에서 기준 배치 값을 (통신 링크를 통해) 수신하거나, 외부 컴퓨팅 수단(예를 들어, 서버에서 작동)을 통해 단방향 함수 또는 단방향 누산기를 포함하는 계산 단계의 일부 또는 전체를 수행하거나, 또는 후보 루트 디지털 서명이 기준 루트 디지털 서명과 일치하는지 검증(및 단지 결과만을 수신)을 수행함으로써 온라인 검증 프로세스와 호환된다.

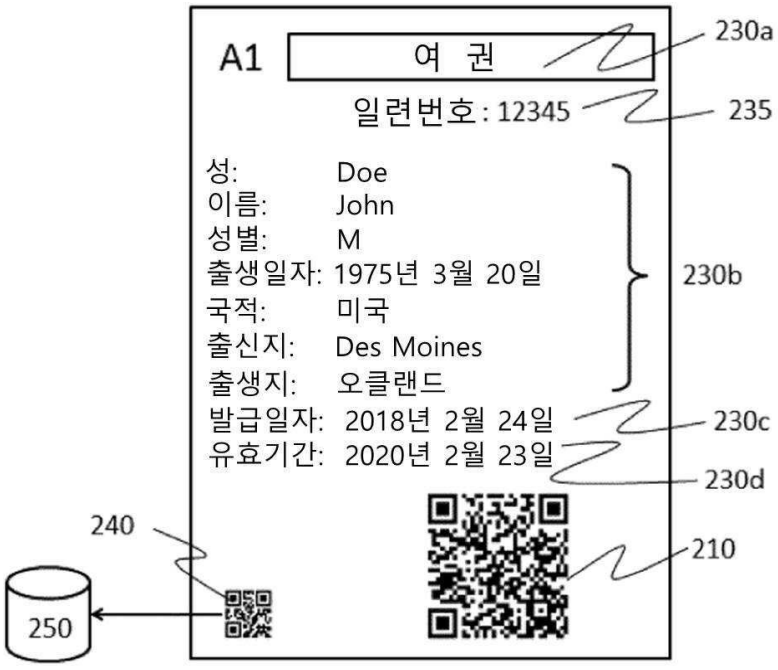
[0260] 상기 개시된 주제는 제한적이지 않고 예시적인 것으로 간주되어야 하며, 독립 청구항에 의해 정의되는 발명의 더 나은 이해를 제공하는 역할을 한다.

도면

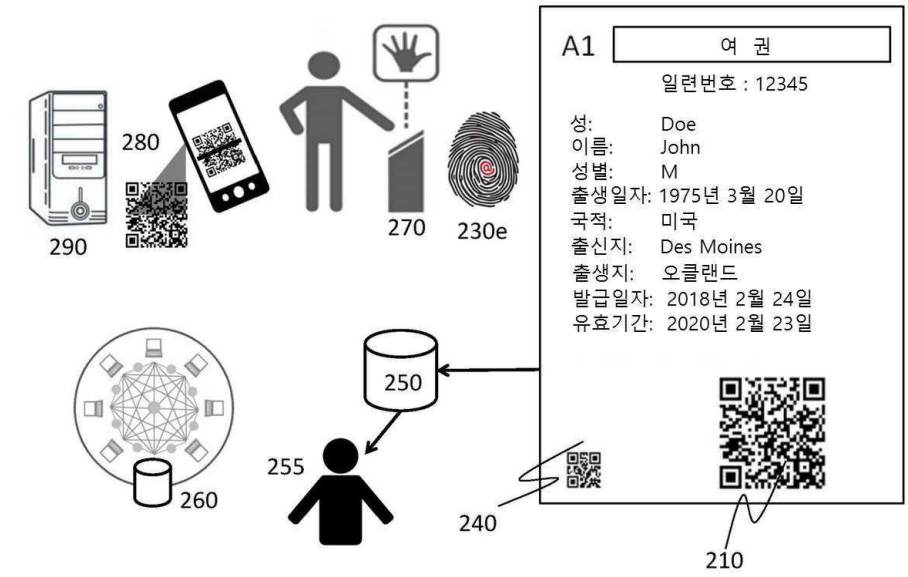
도면1


R
a(3,1)
a(3,2)
a(2,1)
a(2,2)
a(2,3)
a(2,4)
a(1,1)
a(1,2)
a(1,3)
a(1,4)
a(1,5)
a(1,6)
a(1,7)
a(1,8)
x1
x2
x3
x4
x5
x6
x7
x8
H
D1
D2
D3
D4
D5
D6
D7
D8
A1
A2
A3
A4
A5
A6
A7
A8
110

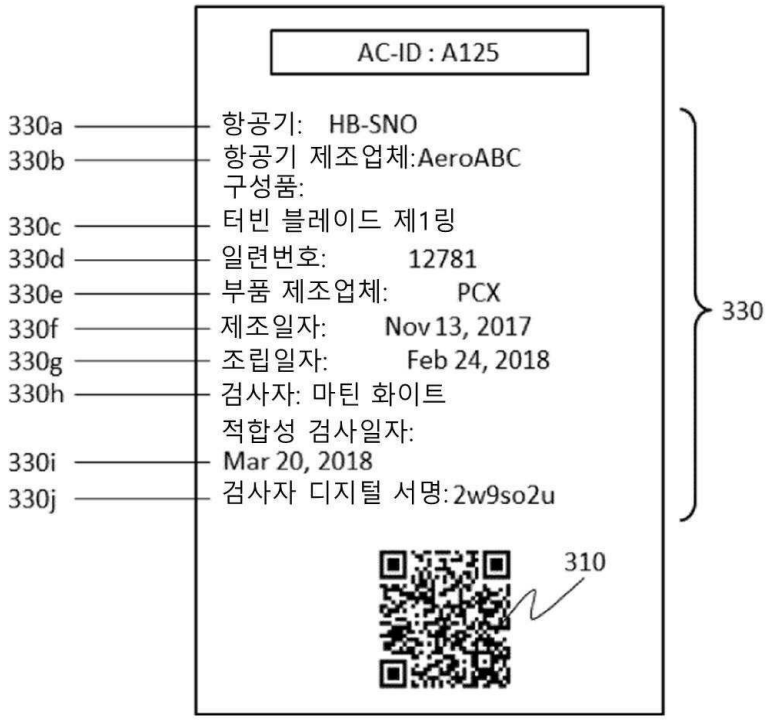
도면2a


A1
여 권
230a
일련번호 : 12345
235
성: Doe
이름: John
성별: M
출생일자: 1975년 3월 20일
국적: 미국
출신지: Des Moines
출생지: 오클랜드
230b
발급일자: 2018년 2월 24일
230c
유효기간: 2020년 2월 23일
230d
240
210
250

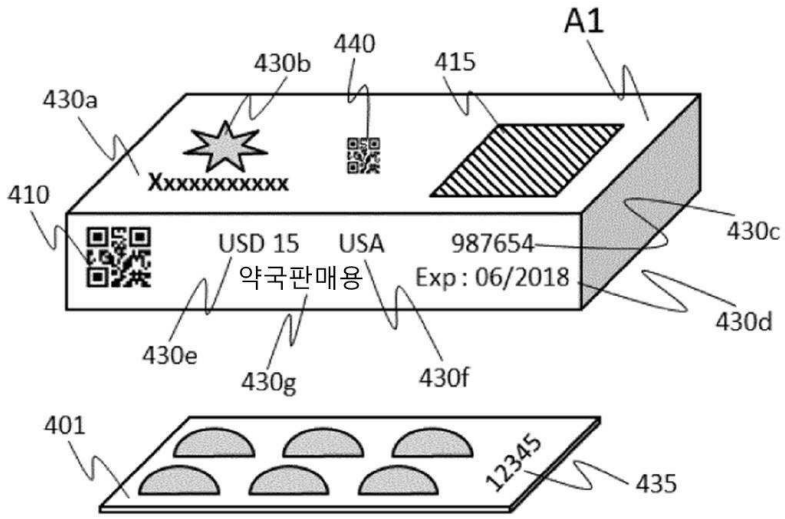
도면2b


A1
여 권
일련번호 : 12345
성: Doe
이름: John
성별: M
출생일자: 1975년 3월 20일
국적: 미국
출신지: Des Moines
출생지: 오클랜드
발급일자: 2018년 2월 24일
유효기간: 2020년 2월 23일
280
290
270
230e
250
255
260
240
210

도면3


AC-ID : A125
330a 항공기: HB-SNO
330b 항공기 제조업체:AeroABC
구성품:
330c 터빈 블레이드 제1링
330d 일련번호: 12781
330e 부품 제조업체: PCX
330f 제조일자: Nov 13, 2017
330g 조립일자: Feb 24, 2018
330h 검사자: 마틴 화이트
적합성 검사일자:
330i Mar 20, 2018
330j 검사자 디지털 서명:2w9so2u
330
310

도면4


A1
440
430b
415
430a
Xxxxxxxxxxx
410
430c
USD 15
USA
987654
약국판매용
Exp : 06/2018
430d
430e
430g
430f
401
12345
435