(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 989 818**

(51) Int. Cl.:

H04L 9/32 (2006.01)
H04L 9/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.07.2019 PCT/EP2019/068986**

(87) Fecha y número de publicación internacional: **13.02.2020 WO20030382**

(96) Fecha de presentación y número de la solicitud europea: **15.07.2019 E 19737560 (3)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2024 EP 3834362**

(54) Título: **Protección antfalsificación de archivos digitales**

(30) Prioridad:

06.08.2018 EP 18187473

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2024

(73) Titular/es:

SICPA HOLDING SA (100.0%)
Avenue de Florissant 41
1008 Prilly, CH

(72) Inventor/es:

DECOUX, ERIC;
GILLET, PHILIPPE;
THEVOZ, PHILIPPE y
WALLACE, ELISABETH

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Protección antfalsificación de archivos digitales

CAMPO TÉCNICO

La presente invención se refiere al campo técnico de la protección de datos digitales contra falsificación o manipulación, y la trazabilidad de archivos digitales.

ANTECEDENTES DE LA TÉCNICA

La solicitud de patente EP 3 031 169 A1 divulga al menos un nodo en una infraestructura de verificación de documentos de árbol hash distribuido que se aumenta con un identificador de una entidad en una ruta de registro. Una firma de datos, que incluye parámetros para el recálculo de un valor de verificación, y que está asociada a un registro de entrada digital, incluirá por tanto también datos que identifiquen al menos a una entidad en la ruta del árbol hash utilizada para su registro inicial en la infraestructura.

La solicitud de patente EP 3 820 712 A1 divulga una solución para asegurar un artículo contra la falsificación y el falseamiento de sus datos asociados, y en particular de los datos relativos a su pertenencia a un lote específico de artículos, permitiendo al mismo tiempo la comprobación fuera de línea o en línea de la autenticidad de un artículo asegurado y la conformidad de sus datos asociados con respecto a los de un artículo auténtico.

La solicitud de patente WO 2010/0112101 A1 divulga un documento digital que se protege mediante: la recepción del documento digital; la recepción de datos asociados que comprenden al menos parcialmente datos del documento digital; la creación de un troceo de los datos asociados; el cifrado asimétrico del troceo con una clave privada para generar una firma digital; la codificación en un código legible por máquina de la firma digital y los datos asociados; y la grabación del código legible por máquina en una copia impresa resultante. La autenticidad de una copia impresa en papel del documento digital puede verificarse mediante la comparación de los datos extraídos de la copia impresa en papel con los datos asociados decodificados y verificados a partir del código legible por máquina.

Los problemas de falsificación y manipulación de archivos digitales se conocen bien, son graves y van en aumento. Se conoce bien el ejemplo de falsificación de datos marcados en un documento digital original, tal como un documento de identidad digital o una versión digital de un diploma, y el problema es incluso peor si se considera una copia digital del documento digital original (posiblemente genuino). Simplemente realizar un seguimiento de identificadores tales como números de serie, o incluso incluir algunas marcas de agua digitales es, en general, una respuesta débil, debido asimismo a que los falsificadores pueden copiar fácilmente tales números o marcas de agua digitales.

Otro inconveniente de la mayoría de métodos convencionales para asegurar la autenticidad de archivos digitales, o asegurar sus datos digitales, es que tienden a ver los archivos de manera aislada, incluso si son miembros de un grupo bien definido, tal como un lote de documentos digitales, por ejemplo. Esto ignora información de autenticación valiosa.

Por lo tanto es un objeto de la invención asegurar un archivo digital imprimible contra falsificación y falsificación de sus datos asociados, y particularmente de datos relacionados con su pertenencia a un lote específico de archivos digitales. También es un objeto de la invención permitir la comprobación fuera de línea de la autenticidad de un archivo digital imprimible asegurado de acuerdo con la invención y conformidad de su contenido de datos asociados con respecto a los de un archivo digital genuino. La invención también tiene por objetivo asegurar archivos digitales imprimibles de modo que es fácil comprobar la autenticidad del contenido de datos tanto de los archivos digitales imprimibles como sus versiones impresas. Particularmente, un objetivo de la invención es asegurar archivos digitales listos para imprimir, siendo un archivo digital listo para imprimir conocido como un archivo de impresión que cumple los siguientes criterios: todas las imágenes RGB posibles se convierten a color CMYK, el archivo está en un formato correcto como PSD, EPS, AL, JPG de alta resolución, PDF o TIF, y la imagen final tiene una resolución suficiente (es decir, 300 ppp o mayor).

SUMARIO DE LA INVENCIÓN

De acuerdo con un aspecto la invención se refiere a un método de aseguramiento de un archivo digital original que pertenece a un lote de una pluralidad de archivos digitales originales contra falsificación o manipulación, incluyendo cada archivo digital original sus propios datos digitales, caracterizado por que comprende las etapas de:

- para cada archivo digital original del lote, calcular por medio de una función unidireccional una firma de archivo digital asociada de sus datos digitales;

- formar un árbol basándose en la pluralidad de firmas de archivo digital calculadas para los archivos digitales originales del lote y que comprende nodos dispuestos de acuerdo con un orden de nodos dado en el árbol, comprendiendo dicho árbol niveles de nodo a partir de los nodos hoja, que corresponden a la pluralidad de firmas de archivo digital respectivamente asociadas a la pluralidad de archivos digitales originales en el lote, al nodo raíz del árbol, correspondiendo cada nodo no hoja del árbol a una firma digital por medio de la función unidireccional de una concatenación de las respectivas firmas digitales de sus nodos hijo de acuerdo con un orden de concatenación de árbol, correspondiendo el nodo raíz a una firma digital raíz de referencia, es decir, una firma digital por medio de la función unidireccional de una concatenación de las firmas digitales de los nodos de un penúltimo nivel de nodos en el árbol de acuerdo con dicho orden de concatenación de árbol;

- asociar con el archivo digital original dado una correspondiente clave de verificación digital que es una secuencia de las respectivas firmas digitales, desde el nivel de nodos hoja hasta el penúltimo nivel de nodos, de cada otro nodo hoja que tiene el mismo nodo padre en el árbol que el nodo hoja que corresponde a la firma de archivo digital del archivo digital original dado, y sucesivamente en cada siguiente nivel en el árbol, de cada nodo no hoja que tiene el mismo nodo padre en el árbol que el mismo nodo padre anterior considerado en el nivel anterior;
- poner a disposición de un usuario la firma digital raíz de referencia del árbol; e
- incluir en el archivo digital original una correspondiente marca de seguridad digital que comprende una representación legible por máquina de sus datos digitales y su correspondiente clave de verificación digital,

obteniendo de este modo un archivo digital original marcado cuyos datos digitales se aseguran contra falsificación o manipulación.

Por lo tanto, si la marca de seguridad digital incluida en el archivo digital es imprimible como un código de barras, también se asegura el documento impreso (incluyendo el código de barras impreso) obtenido imprimiendo el archivo digital asegurado (por medio de una impresora convencional), es decir, sus datos impresos se aseguran contra falsificación o manipulación.

La firma digital raíz de referencia del nodo raíz del árbol puede o bien publicarse en un medio accesible por el usuario, o bien almacenarse en una base de datos raíz consultable accesible por el usuario, o en una cadena de bloques, o en una base de datos asegurada por una cadena de bloques, accesible por el usuario. Por lo tanto, la firma digital raíz de referencia se hace inmutable.

Por lo tanto, de acuerdo con la invención, el conflicto de las firmas digitales de todos los archivos digitales originales de un lote, debido a la estructura de árbol y uso de funciones unidireccionales robustas para calcular los valores de nodo del árbol, junto con la firma digital raíz del árbol que se hace inmutable y la inclusión de los datos digitales y su clave de verificación digital asociada en una marca de seguridad digital incluida en el correspondiente archivo digital original, permite el rastreo y trazabilidad de los archivos marcados y sus copias, así como sus versiones impresas, con un nivel alto de fiabilidad mientras se evita la falsificación de datos y falsificación de los archivos marcados.

El archivo digital original marcado puede comprender adicionalmente datos de acceso de nodo raíz incluidos en el mismo y que contienen información suficiente para permitir que el usuario acceda a la firma digital raíz de referencia del nodo raíz del árbol que corresponde al lote de archivos digitales originales, siendo dicha información un enlace a una interfaz de acceso operable para recibir desde el usuario una petición raíz que contiene datos digitales, o firma de archivo digital, obtenidos a partir de una marca de seguridad digital de un archivo digital original marcado, y enviar de vuelta una firma digital raíz de referencia del árbol correspondiente, permitiendo la interfaz de acceso acceso a, respectivamente, uno de los siguientes:

- el medio en el que se publica la firma digital raíz de referencia;
- la base de datos raíz consultable en la que se almacena la firma digital raíz de referencia; y
- la cadena de bloques, o respectivamente la base de datos asegurada por una cadena de bloques, en la que se almacena la firma digital raíz de referencia con indicaciones de tiempo.

De acuerdo con la invención, también es posible que:

- un archivo digital virtual se cuenta como que pertenece al lote de archivos digitales originales, incluyendo dicho archivo digital virtual sus propios datos digitales virtuales, y una firma de archivo digital virtual asociada obtenida por medio de la función unidireccional de los datos digitales virtuales, no siendo dicho archivo digital virtual real sino usado únicamente para generar la firma de archivo digital virtual asociada a partir de sus datos digitales virtuales; y
- siendo la firma digital raíz de referencia asociada con dicho lote de archivos digitales originales calculada a partir de un árbol que tiene todas las firmas de archivos digitales de los archivos digitales originales del lote, incluyendo la firma de archivo digital virtual, como nodos hoja.

Para tener firmas más cortas la función unidireccional puede ser una función de troceo y una firma digital de

un archivo digital original puede ser una secuencia de una pluralidad dada de bits de pesos menores seleccionados a partir de los bits de un valor de troceo de los correspondientes datos digitales.

En el método anterior, datos digitales adicionales que corresponden a los datos digitales asociados con el archivo digital original marcado pueden almacenarse en una base de datos de información consultable accesible por el usuario a través de una interfaz de base de datos de información operable para recibir desde el usuario una petición de información que contiene datos digitales, o una firma de archivo digital, obtenidos a partir de una marca de seguridad digital de un archivo digital original marcado, y enviar de vuelta correspondientes datos digitales adicionales.

Los datos digitales del archivo digital original marcado pueden incluir adicionalmente datos digitales de característica de referencia de una correspondiente característica física única de un objeto o individuo asociado. Además, la característica física única del objeto o individuo asociado puede ser, respectivamente, la de una marca de seguridad basada en material aplicada en el objeto asociado o identificación de una característica biométrica del individuo asociado.

En el método anterior, la secuencia de firmas digitales en la clave de verificación digital incluida en la marca de seguridad digital puede disponerse de acuerdo con un orden de secuencia de los nodos que es distinto del orden de correspondientes nodos definidos por el orden de concatenación de árbol, y la marca de seguridad digital puede incluir adicionalmente un código de orden asociado con dicho orden de secuencia. Estas características aumentan el nivel de seguridad con respecto a ataques de descifrado de código.

De acuerdo con la invención, en el caso en el que los datos digitales de los respectivos archivos digitales originales del lote se distribuyen entre campos dados comunes a todos los archivos digitales del lote, datos digitales específicos relacionados con estos campos pueden no incluirse en los datos digitales, sino que pueden agruparse en un bloque de datos de campos separados asociado con el lote, en el que:

i) la firma de archivo digital de un archivo digital original se calcula con la función unidireccional de una concatenación de los correspondientes datos digitales y el bloque de datos de campos; y
ii) la firma digital raíz de referencia se pone a disposición del usuario junto con el bloque de datos de campos asociado.

Otro aspecto de la invención se refiere a un método de verificación de la autenticidad de un archivo digital asegurado de acuerdo con el método de aseguramiento anterior, o la conformidad de una copia de tal archivo digital asegurado con respecto al original, que comprende las etapas de, tras procesar un archivo de prueba que es dicho archivo digital o dicha copia del archivo digital por medio de una unidad de procesamiento conectada a una memoria:

- haber almacenado en la memoria el archivo de prueba;
- leer una representación de datos digitales y de una clave de verificación digital en una marca de seguridad digital del archivo de prueba almacenado, y extraer respectivamente correspondientes datos digitales de prueba y clave de verificación digital de prueba de dicha representación leída;
- haber almacenado en la memoria una firma digital raíz de referencia de un nodo raíz de un árbol del lote de archivos digitales originales, y haber programado en la unidad de procesamiento la función unidireccional para calcular una firma digital de datos digitales y de una concatenación de firmas digitales de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol;
- verificar si los datos digitales de prueba extraídos y la clave de verificación digital de prueba asociada corresponden, de hecho, a la firma digital raíz de referencia almacenada realizando las etapas de:

- calcular con la función unidireccional una firma digital de prueba de los datos digitales de prueba extraídos, correspondiendo dicha firma digital de prueba a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital del archivo de prueba;
- extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo hoja del árbol de prueba que tiene el mismo nodo padre que el del nodo hoja de prueba y calcular una firma digital de una concatenación de la firma digital de prueba y la firma digital extraída de dicho cada otro nodo hoja, obteniendo por lo tanto una firma digital de dicho mismo nodo padre del nodo hoja de prueba;
- sucesivamente en cada siguiente nivel en el árbol de prueba y hasta el penúltimo nivel de nodos, extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo no hoja del árbol de prueba que tiene el mismo nodo padre que el del mismo nodo padre anterior considerado en la etapa anterior y calcular una firma digital de una concatenación de la firma digital de dicho cada respectivo otro nodo no hoja y la firma digital obtenida de dicho mismo nodo padre anterior, obteniendo por lo tanto una firma digital de dicho mismo nodo padre de dicho mismo nodo padre anterior;
- calcular una firma digital de una concatenación de las firmas digitales obtenidas de los nodos no hoja que corresponden al penúltimo nivel de nodos del árbol de prueba, obteniendo por lo tanto una firma digital raíz candidata del nodo raíz del árbol de prueba; y

- comprobar si la firma digital raíz candidata obtenida coincide con la firma digital raíz de referencia almacenada,

con lo que, en el caso en el que dichas firmas digitales raíz coinciden, los datos digitales del archivo de prueba son los de un archivo digital genuino.

Si el archivo digital original marcado se asegura mientras tiene el anteriormente mencionado bloque de datos de campos separados, la memoria de la unidad de procesamiento puede almacenar adicionalmente el bloque de datos de campos asociados, y la etapa de calcular una firma digital de prueba que corresponde a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital en el archivo de prueba puede comprender calcular con la función unidireccional una firma digital de una concatenación de los datos digitales de prueba extraídos y el bloque de datos de campos almacenado.

Si el archivo digital se ha asegurado almacenando la firma digital raíz de referencia en una base de datos raíz consultable accesible por el usuario como se ha mencionado anteriormente, y la unidad de procesamiento se conecta adicionalmente a una unidad de comunicación operable para enviar y recibir de vuelta datos a través de un enlace de comunicación, el método de verificación anterior puede comprender las etapas preliminares de:

- enviar con la unidad de comunicación a través del enlace de comunicación una petición a dicha base de datos raíz, y recibir de vuelta la firma digital raíz de referencia; y
- almacenar la firma digital raíz recibida en la memoria de la memoria.

Si el archivo digital asegurado comprende datos de acceso de nodo raíz como se ha explicado anteriormente, y la unidad de procesamiento se conecta adicionalmente a una unidad de comunicación operable para enviar y recibir datos a través de un enlace de comunicación, el método de verificación anterior puede comprender las etapas preliminares de:

- leer los datos de acceso de nodo raíz incluidos en el archivo de prueba;
- enviar con la unidad de comunicación a través del enlace de comunicación una petición raíz a dicha interfaz de acceso que contiene datos digitales, o una firma digital de dichos datos digitales, obtenidos a partir de la marca de seguridad digital en el archivo de prueba, y recibir de vuelta una correspondiente firma digital raíz de referencia del lote asociado; y
- almacenar la firma digital raíz de referencia recibida en la memoria.

Si el archivo digital marcado tiene datos digital almacenados adicionales asociados en una base de datos de información consultable como se ha mencionado anteriormente, el formador de imágenes puede estar equipado adicionalmente con medios de comunicación operables para enviar a la interfaz de base de datos de información una petición de información que contiene datos digitales, o una firma de archivo digital, obtenidos a partir de la marca de seguridad digital del archivo de prueba, y recibir de vuelta correspondientes datos digitales adicionales.

En el caso en el que el archivo digital asegurado incluye datos digitales de característica de referencia como se ha mencionado anteriormente, y el formador de imágenes está equipado adicionalmente con un sensor operable para detectar una característica física única de respectivamente un objeto o individuo asociado, y la unidad de procesamiento se programa para extraer correspondientes datos digitales de característica de una señal de detección recibida desde el sensor, habiendo almacenado el formador de imágenes en la memoria datos digitales de característica de referencia CDD que corresponden a dicha característica física única de respectivamente el objeto o individuo asociado, el método de verificación puede comprender las etapas adicionales de, tras visualizar un sujeto que es dicho objeto o individuo asociado:

- detectar con el sensor una característica física única del sujeto y extraer correspondientes datos digitales de característica candidatos CDD^c;
- comparar los datos digitales de característica candidatos CDD^c obtenidos con los datos digitales de característica de referencia CDD almacenados; y
- en el caso en el que los datos digitales de característica candidatos CDD^c son similares a los datos digitales de característica de referencia CDD almacenados, dentro de un criterio de tolerancia dado, el sujeto se considera que corresponde respectivamente a un objeto o individuo genuino asociado de forma válida con un archivo digital genuino.

Otro aspecto de la invención se refiere a un archivo digital que pertenece a un lote de una pluralidad de archivos digitales originales y asegurado de acuerdo con el método de aseguramiento anteriormente mencionado, teniendo cada archivo digital original del lote sus propios datos digitales y correspondiente clave de verificación digital, teniendo dicho lote una correspondiente firma digital raíz de referencia, comprendiendo el archivo digital una marca de seguridad legible por máquina que incluye una representación de sus datos digitales y su clave de verificación. Los datos digitales del archivo digital pueden incluir adicionalmente datos

digitales de característica de referencia CDD de una correspondiente característica física única de un objeto o individuo asociado. Además, la característica física única del objeto asociado puede ser la de una marca de seguridad basada en material aplicada en el objeto asociado.

Otro aspecto de la invención se refiere a un sistema de verificación de la autenticidad de un archivo digital, o la conformidad de una copia de tal archivo digital, con respecto a un archivo digital original marcado que pertenece a un lote de archivos digitales originales asegurados de acuerdo con el método de aseguramiento anteriormente mencionado, que comprende un formador de imágenes que tiene una unidad de formación de imágenes, una unidad de procesamiento con una memoria, y una unidad de procesamiento de imágenes, almacenando la memoria una firma digital raíz de referencia de un árbol que corresponde al lote de archivos digitales originales, y programándose en la unidad de procesamiento la función unidireccional para calcular una firma digital de datos digitales y de una concatenación de firmas digitales de acuerdo con el orden de nodos del árbol y el orden de concatenación de árbol, siendo dicho sistema operable para:

- tener almacenado en la memoria un archivo de prueba que es dicho archivo digital o dicha copia del archivo digital;
- leer una representación de datos digitales y de una clave de verificación digital en una marca de seguridad digital del archivo de prueba almacenado, y extraer respectivamente correspondientes datos digitales de prueba y clave de verificación digital de prueba de dicha representación leída;
- verificar si los datos digitales de prueba extraídos y la clave de verificación digital de prueba corresponden, de hecho, a la firma digital raíz de referencia almacenada realizando en la unidad de procesamiento las operaciones programadas de:

- calcular con la función unidireccional una firma digital de prueba de los datos digitales de prueba extraídos, correspondiendo dicha firma digital de prueba a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital del archivo de prueba;
- extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo hoja del árbol de prueba que tiene el mismo nodo padre que el del nodo hoja de prueba y calcular una firma digital de una concatenación de la firma digital de prueba y la firma digital extraída de dicho cada otro nodo hoja, obteniendo por lo tanto una firma digital de dicho mismo nodo padre del nodo hoja de prueba;
- sucesivamente en cada siguiente nivel en el árbol de prueba y hasta el penúltimo nivel de nodos, extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo no hoja del árbol de prueba que tiene el mismo nodo padre que el del mismo nodo padre anterior considerado en la etapa anterior y calcular una firma digital de una concatenación de la firma digital de dicho cada respectivo otro nodo no hoja y la firma digital obtenida de dicho mismo nodo padre anterior, obteniendo por lo tanto una firma digital de dicho mismo nodo padre de dicho mismo nodo padre anterior;
- calcular una firma digital de una concatenación de las firmas digitales obtenidas de los nodos no hoja que corresponden al penúltimo nivel de nodos del árbol de prueba, obteniendo por lo tanto una firma digital raíz candidata del nodo raíz del árbol de prueba; y
- comprobar si la firma digital raíz candidata obtenida coincide con la firma digital raíz de referencia almacenada,

con lo que, en el caso en el que dichas firmas digitales raíz coinciden, el sistema está configurado para entregar una indicación de que los datos digitales del archivo de prueba son los de un archivo digital genuino.

En el sistema anterior, si el archivo digital original marcado tiene un bloque de datos de campos asociados como se ha mencionado anteriormente, almacenando adicionalmente la memoria de la unidad de procesamiento el bloque de datos de campos asociado, las operaciones programadas de calcular una firma digital de prueba que corresponde a un nodo hoja de prueba que corresponden a la marca de seguridad digital del archivo de prueba comprende entonces calcular con la función unidireccional una firma digital de una concatenación de los datos digitales de prueba extraídos y el bloque de datos de campos almacenado.

En el caso en el que el archivo digital original marcado pertenece a un lote de archivos digitales originales asegurados incluyendo datos digitales de característica de referencia de una correspondiente característica física única de un objeto o individuo asociado como se ha mencionado anteriormente, estando el sistema anterior equipado adicionalmente con un sensor conectado a la unidad de procesamiento y operable para detectar una característica física única de un objeto o individuo asociado, y programándose la unidad de procesamiento para extraer correspondientes datos digitales de característica de una señal de detección recibida desde el sensor, habiendo almacenado el sistema en la memoria datos digitales de característica de referencia CDD que corresponden a dicha característica física única del objeto o individuo asociado, el sistema puede ser adicionalmente operable para:

- detectar con el sensor una característica física única de un sujeto que es dicho objeto o individuo asociado, y extraer correspondientes datos digitales de característica candidatos CDD^c;
- comparar los datos digitales de característica candidatos CDD^c obtenidos con los datos digitales de

característica de referencia CDD almacenados; y
- en el caso en el que los datos digitales de característica candidatos CDD^c son similares a los datos digitales de característica de referencia CDD almacenados, dentro de un criterio de tolerancia dado, entregar una indicación de que el sujeto se considera genuino.

La presente invención se describirá más completamente en lo sucesivo con referencia a los dibujos adjuntos en los que números similares representan elementos similares a lo largo de las diferentes figuras, y en los que se ilustran aspectos y características destacados de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es una vista esquemática de un concepto general de aseguramiento de un lote de archivos digitales originales de acuerdo con la invención.
La Figura 2A ilustra un pasaporte biométrico digital asegurado como un ejemplo de documento de identidad biométrica digital asegurado de acuerdo con la invención.
La Figura 2B ilustra un control de un individuo que tiene el pasaporte biométrico digital asegurado de la Figura2A por un agente autorizado.
La Figura 3 ilustra un lote de documentos digitales relacionados con componentes de una aeronave asegurada de acuerdo con la invención.

DESCRIPCIÓN DETALLADA

La presente divulgación se describe en este punto en detalle con referencia a realizaciones no limitantes ilustradas en los dibujos.

La Figura 1 ilustra un concepto general de la invención relacionada con el aseguramiento de un lote de archivos digitales y un método de cálculo de una codificación de información de verificación que puede asociarse con cada archivo digital. La Figura 1 ilustra un grupo o "lote" de archivos digitales $A_1,\ldots,A_8$, que contienen una representación digital de una marca de seguridad legible por máquina 110 (ilustrada en este punto por un código de barras de 2D). En lo que sigue, la expresión "marca de seguridad digital 110" de hecho significa "representación digital de una marca de seguridad legible por máquina 110". La Figura 1 ilustra un grupo o "lote" de archivos digitales y su árbol asociado en el que, por simplicidad, únicamente se muestran ocho archivos digitales originales: $A_1,\ldots,A_8$. También por simplicidad, el árbol asociado con el lote de archivos $A_1,\ldots,A_8$ es en este punto un simple árbol binario. Un archivo digital puede referirse a un artículo fabricado o su embalaje, un documento o imagen físicos, un paquete que contiene varios artículos (tal como un blíster de fármacos), o un contenedor que contiene palés de envases de bienes etc. No únicamente un objeto, sino incluso una persona puede "asociarse" con un archivo digital en el sentido de las realizaciones de la invención; por ejemplo, asistentes autorizados a un evento o miembros de un grupo, o miembros de una manada o rebaño, podrían llevar alguna forma de credencial de ID o ser marcados físicamente con alguna marca que contiene datos registrados en un correspondiente archivo digital.

Un lote de archivos digitales podría referirse, por ejemplo, a un ciclo de fabricación común, artículos entregados por un suministrador particular, artículos fabricados o enviados durante un periodo de tiempo, un conjunto de imágenes relacionadas, un grupo de personas, una manada o rebaño, o cualquier otro agrupamiento definido por un usuario de cualquier objeto para el que puede definirse un archivo digital A_i (que tiene el contenido digital D_i).

Cualquiera de los artículos mostrados en la Figura 1 podría ser un "artículo virtual" A_v, que es una construcción de software opcional que puede incluirse para habilitar la codificación de datos seleccionados. Esto se explica adicionalmente a continuación. Por ejemplo, uno de los ocho artículos, por ejemplo, el artículo A_8, puede ser, de hecho, un artículo virtual A_v que se cuenta como perteneciente al lote de ocho artículos, y se trata como cualquiera de los otros siete artículos reales ya que puede procesarse sustancialmente de la misma forma (aunque no corresponde a un objeto real). Por supuesto, pueden usarse una pluralidad de artículos virtuales $A_{v1},A_{v2},\ldots,A_{vk}$ para codificar datos digitales y producir firmas digitales de artículo más robustas (véase a continuación).

Para cada artículo $A_1,A_2,\ldots,A_7,A_8$ del lote (posiblemente con $A_8 \equiv A_v$) respectivos datos digitales de artículo $D_1,D_2,\ldots,D_7,D_8$ (posiblemente con $D_8 \equiv D_v$) se asocian o extraen (o, en el caso del artículo virtual A_v, creado) usando cualquier método apropiado. Estos datos podrían ser alguna medida de características físicas, datos textuales tales como formulario completado o información de producto, un número de serie u otro identificador, indicaciones de contenido, una representación digital de una imagen, o cualquier otra información que el diseñador de sistema elige para asociar con un artículo. Los datos digitales de artículo D_i pueden extraerse de datos legibles humanos (por ejemplo, datos alfanuméricos) marcados en un artículo asociado (por ejemplo, impresos en el artículo o en una etiqueta fijada en el artículo) por medio de un lector con capacidad de producir correspondientes datos digitales de un archivo digital A_i. Datos digitales adicionales (por ejemplo, instrucciones de uso del artículo asociado o instrucciones de seguridad, etc.)

pueden asociarse con los datos extraídos para constituir los datos digitales de artículo D_i.

Para el artículo virtual A_v, los datos asociados digitales pueden incluir, por ejemplo, un número de identificación de lote, el número de artículos en el lote, un número (pseudo) aleatorio en aras de seguridad creciente aumentando la entropía de datos, información de fecha y/o hora, etc. Otra forma de datos asociados podría ser indicaciones de reglas de operaciones permisibles o no permisibles, fechas de expiración, etc. En breve, los datos digitales D_v pueden ser cualquier cosa que puede representarse en forma digital.

Para cada artículo del lote, sus respectivos datos de artículo digitales $D_1,D_2,\ldots,D_7,D_8$ se transforman preferentemente matemáticamente de tal manera que están esencialmente ocultos, aunque esto no es un requisito absoluto para cualquier realización. Esta transformación aplicada a los datos digitales de artículo D_i de un artículo A_i sirve para crear una correspondiente firma digital x_i. Esta firma digital se produce por medio de una función unidireccional, es decir, una función fácil del calcular pero difícil de invertir (véase S. Goldwasser y M. Bellare "Lecture Notes on Cryptography", MIT, julio 2008, http://www-cse.ucsd.edu/users/mihir).

Una transformación ventajosa tal es, por ejemplo, aplicar una función de troceo H( ) = troceo( ) a los datos digitales, que generalmente tienen la propiedad que devuelve una salida de una longitud de bit conocida independientemente del tamaño de la entrada: este efecto técnico es particularmente útil para crear una firma digital de datos digitales de un archivo digital (por ejemplo, asociado a un artículo) independientemente del tamaño de los datos digitales y el del lote de correspondientes archivos digitales. La función de troceo es un ejemplo bien conocido de una función unidireccional. Si se usa una función de troceo criptográfica, tal como la clase SHA (Algoritmo de Función de Troceo Seguro) de funciones, por ejemplo, SHA-256, entonces existen los beneficios adicionales de que la función es prácticamente irreversible y resistente a colisión, es decir, la probabilidad de que dos diferentes entradas conducirán al mismo resultado es insignificante. Como se entenderá a partir de la descripción a continuación, esto tampoco es un requisito de la invención, aunque es ventajoso por las mismas razones que en otras aplicaciones. Como se muestra en la Figura 1, los valores $x_1,x_2,x_3,\ldots,x_8$ son los valores de troceo, es decir, las firmas digitales de artículo asociadas, de los respectivos conjuntos de datos de artículo, es decir, $x_j = H(D_j)$, para j=1,...,8 (en el caso en el que $A_8 \equiv A_v$, entonces $D_8 \equiv D_v$ y $x_8 \equiv x_v = H(D_v)$).

Para acortar la firma, la firma digital de artículo x_j de artículo A_j puede ser incluso solo una secuencia de una pluralidad dada de bits de pesos menores seleccionados de los bits del valor de troceo $H(D_j)$: por ejemplo, con la función de troceo SHA-256 de la familia SHA-2, es suficiente retener únicamente los 128 bits de menor peso de los 256 bits de la firma para tener aún una firma robusta con respecto a un ataque de descifrado de código.

La Figura 1 muestra un lote de ocho artículos originales marcados $A_1,\ldots,A_8$, teniendo cada uno una correspondiente marca de seguridad 110 aplicada en el mismo, e ilustra el método de aseguramiento de los artículos y sus respectivos datos digitales de artículo asociados $D_1,\ldots D_8$ (representados simbólicamente en los archivos A_i en la Figura 1 mediante una secuencia de bits "0" y "1") por medio de un árbol de firmas digitales de los datos digitales. Los árboles asociados con firmas digitales se conocen bien (árboles de troceo binarios, árboles de troceo n-ario o árboles de Merkle), generalmente tienen nodos base, o nodos hoja, que se usan para construir siguientes nodos de nivel (intermedio) firmando digitalmente una concatenación de las firmas digitales asociadas con los nodos hoja de acuerdo con un cierto agrupamiento de los nodos hoja. En caso de un árbol binario, las firmas digitales asociadas con los primeros nodos de nivel intermedio se calculan respectivamente firmando digitalmente (por ejemplo, con una función de troceo unidireccional H, o una función de curva elíptica unidireccional...) una concatenación de las firmas digitales asociadas con dos nodos hoja consecutivos. En caso de un árbol n-ario, los valores de los primeros nodos de nivel intermedio se obtienen mediante la concatenación de los valores de n nodos hoja consecutivos. Un árbol también puede tener una estructura más compleja (árboles mixtos) ya que la concatenación de los nodos hoja puede realizarse por pares de nodos consecutivos para ciertos nodos hoja, mediante triplete de nodos para otros nodos hoja consecutivos etc. Por razones de simplicidad, en la Figura 1 se muestra un simple árbol binario con ocho nodos hoja: los respectivos valores de los ocho nodos hoja a(1,1),...,a(1,8) del árbol, respectivamente corresponden a las firmas digitales de artículo $x_1 = H(D_1),\ldots, x_8 = H(D_8)$. El valor del primer índice, es decir, "1", para todos los nodos hoja indica el primer nivel (o nivel base) del árbol, y el segundo índice que va desde 1 a ocho indica el orden de nodos (hoja) del árbol. Los valores de los nodos (no hoja) de siguiente nivel, es decir, los cuatro nodos de nivel dos a(2,1), a(2,2), a(2,3) y a(2,4), se obtienen firmando digitalmente una concatenación (representada simbólicamente por un operador "+"), en este punto por medio de una función de troceo, de los valores de pares de nodos hoja, es decir, pares de sus nodos hijo en el árbol. Esta agrupación de nodos hijo para obtener los valores de los nodos del siguiente nivel define el orden de concatenación de árbol. Para simplificar las notaciones, usamos el símbolo de nodo a(i,j) para representar también su valor asociado (es decir, su firma digital asociada). En este punto, el árbol tiene únicamente dos niveles intermedios por encima del nivel de nodos hoja, y el nodo raíz en el nivel superior. El nivel de nodo raíz es, de hecho, el último nivel de nodo no hoja del árbol. Por lo tanto, los valores de los cuatro nodos no

hoja del siguiente nivel intermedio son: a(2,1) = H(a(1,1)+a(1,2)), es decir, a(2,1) = H(H(D_1)+ H(H(D_2)), (ya que a(1,1) y a(1,2) son los nodos hijo del nodo a(2,1))

a(2,2) = H(a(1,3)+a(1,4))

a(2,3) = H(a(1,5)+a(1,6))

a(2,4) = H(a(1,7)+a(1,8))

y, para el siguiente, penúltimo, nivel de nodo (en este punto, nivel tres) existen dos valores de nodo:

a(3,1) = H(a(2,1)+a(2,2))

a(3,2) = H(a(2,3)+a(2,4)).

Observamos que es posible elegir un orden de concatenación de árbol diferente para cada nodo no hoja: por ejemplo, en lugar de tener a(2,4) = H(a(1,7)+a(1,8)) podríamos definir a(2,4) = H(a(1,8)+a(1,7)), que proporciona un valor de nodo diferente.

Finalmente, el valor del nodo raíz R del árbol, o firma digital raíz de referencia, se obtiene como: R = H(a(3,1)+a(3,2)).

Debido a la cascada de concatenaciones implicadas en un árbol, es prácticamente imposible recuperar un valor raíz si se cambia cualquier bit de datos digitales en un nodo (particularmente, en un nodo hoja). Además, si se incluyen algunos artículos virtuales en el lote (cuyos datos digitales de artículo virtual se conocen únicamente por el sistema que ha producido las firmas digitales de los nodos hoja del árbol), un falsificador no será capaz de recuperar la firma digital raíz incluso si conoce los datos digitales de todos los artículos producidos (y marcados) del lote.

De acuerdo con la invención, la firma digital raíz de referencia R del lote de archivos digitales originales se hace inmutable y, por lo tanto, a prueba de falsificación, publicándose en un medio (público) accesible por un usuario que tiene que comprobar la autenticidad de un artículo (o sus datos asociados), o almacenándose en una base de datos raíz consultable accesible por el usuario, o, en un modo preferido, almacenándose en una cadena de bloques (o en una base de datos asegurada por una cadena de bloques) accesible por el usuario. El usuario puede almacenar, a continuación, el valor de referencia R adquirido desde estas fuentes disponibles.

Para cada archivo digital original A_i del lote, se calcula, a continuación, una correspondiente clave de verificación digital k_i (o trayectoria de verificación) del árbol asociado como una secuencia de las respectivas firmas digitales, desde el nivel de nodos hoja hasta el penúltimo nivel de nodos, de cada otro nodo hoja que tiene el mismo nodo padre en el árbol que el nodo hoja que corresponde a la firma digital del archivo digital original A_i, y sucesivamente en cada siguiente nivel en el árbol, de cada nodo no hoja que tiene el mismo nodo padre en el árbol que el mismo nodo padre anterior considerado en el nivel anterior. En el ejemplo de la Figura 1, existen ocho claves de verificación $k_1,\ldots,k_8$ que corresponden respectivamente a los ocho artículos $A_1,\ldots,A_8$ del lote y sus correspondientes ocho nodos hoja a(1,1),…,a(1,8):

1) para el nodo hoja a(1,1) = x_1 = H(D_1) que corresponde al artículo A_1, la clave de verificación es k_1 = {a(1,2),a(2,2),a(3,2)}, a partir de la cual puede recuperarse el valor de firma digital raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir del nodo hoja a(1,1) = x_1 y nodo hoja a(1,2) = x_2 en k_1 (a(1,2) es el otro nodo hoja que tiene el mismo nodo padre, es decir, nodo a(2,1), que el nodo hoja que corresponde a la firma digital de artículo x_1, es decir, nodo a(1,1)), el valor de nodo padre a(2,1) se obtiene mediante a(2,1) = H(a(1,1)+a(1,2)) (es decir, a(2,1) = H(x_1 + x_2)),
ii) a partir del a(2,1) obtenido y el siguiente valor de nodo en k_1, es decir, a(2,2) de siguiente nivel de nodos no hoja, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, nodo a(3,1), que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(2,1), el valor de nodo padre a(3,1) se obtiene mediante a(3,1) = H(a(2,1)+a(2,2)),
iii) a partir del a(3,1) obtenido y el siguiente valor de nodo en k_1, es decir, a(3,2) del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, el nodo raíz, que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(3,1), el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Observación: en este ejemplo tenemos tres etapas i), ii) y iii), porque el árbol tiene tres niveles por debajo del nivel de nodo raíz y, por lo tanto, la clave de verificación contiene tres valores de nodo.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2)).

2) para el nodo hoja $a(1,2) = x_2 = H(D_2)$ que corresponde al artículo A_2, la clave de verificación es k_2 = {a(1,1),a(2,2),a(3,2)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de $a(1,2) = x_2$ y $a(1,1) = x_1$ en k_1 (a(1,1) es el otro nodo hoja que tiene el mismo nodo padre, es decir, nodo a(2,1), que el nodo hoja que corresponde a la firma digital de artículo x_2, es decir, nodo a(1,2)), el valor de nodo padre a(2,1) se obtiene mediante a(2,1) = H(a(1,1)+a(1,2)),
ii) a partir del a(2,1) obtenido y el siguiente valor de nodo en k_2, es decir, a(2,2) de siguiente nivel de nodos no hoja, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, nodo a(3,1), que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(2,1), el valor de nodo padre a(3,1) se obtiene mediante a(3,1) = H(a(2,1)+a(2,2)),
iii) a partir del a(3,1) obtenido y el siguiente valor de nodo en k_2, es decir, a(3,2) del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, el nodo raíz, que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(3,1), el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2)).

3) para el nodo hoja $a(1,3) = x_3 = H(D_3)$ que corresponde al artículo A_3, la clave de verificación es k_3 = {a(1,4),a(2,1),a(3,2)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de $a(1,3) = x_3$ y $a(1,4) = x_4$ en k_3 (a(1,4) es el otro nodo hoja que tiene el mismo nodo padre, es decir, nodo a(2,2), que el nodo hoja que corresponde a la firma digital de artículo x_3, es decir, nodo a(1,3)), el valor de nodo padre a(2,2) se obtiene mediante a(2,2) = H(a(1,3)+a(1,4)),
ii) a partir del a(2,2) obtenido y el siguiente valor de nodo en k_3, es decir, a(2,1) de siguiente nivel de nodos no hoja, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, nodo a(3,1), que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(2,2), el valor de nodo padre a(3,1) se obtiene mediante a(3,1) = H(a(2,1)+a(2,2)),
iii) a partir del a(3,1) obtenido y el siguiente valor de nodo en k_3, es decir, a(3,2) del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo padre en el árbol, es decir, el nodo raíz, que el mismo nodo padre anterior considerado en el nivel anterior, es decir, nodo a(3,1), el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2)).

4) para el nodo hoja $a(1,4) = x_4 = H(D_4)$ que corresponde al artículo A_4, la clave de verificación es k_4 = {a(1,3),a(2,1),a(3,2)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de $a(1,4) = x_4$ y $a(1,3) = x_3$ en k_4, el valor de nodo padre a(2,2) se obtiene mediante a(2,2) = H(a(1,3)+a(1,4)),
ii) a partir del a(2,2) obtenido y el siguiente valor de nodo en k_4, es decir, a(2,1) de siguiente nivel de nodos no hoja, el valor de nodo padre a(3,1) se obtiene mediante a(3,1) = H(a(2,1)+a(2,2)),
iii) a partir del a(3,1) obtenido y el siguiente valor de nodo en k_4, es decir, a(3,2) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2)).

5) para el nodo $a(1,5) = x_5 = H(D_5)$ que corresponde al artículo A_5, la clave de verificación es k_5 = {a(1,6),a(2,4),a(3,1)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de $a(1,5) = x_5$ y $a(1,6) = x_6$ en k_5, el valor de nodo padre a(2,3) se obtiene mediante a(2,3) = H(a(1,5)+a(1,6)),
ii) a partir del a(2,3) obtenido y el siguiente valor de nodo en k_5, es decir, a(2,4) de siguiente nivel de nodos no hoja, el valor de nodo padre a(3,2) se obtiene mediante a(3,2) = H(a(2,3)+a(2,4)),
iii) a partir del a(3,2) obtenido y el siguiente valor de nodo en k_5, es decir, a(3,1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

6) para el nodo a(1,6) = x_6 = H(D_6) que corresponde al artículo A_6, la clave de verificación es k_6 = {a(1,5),a(2,4),a(3,1)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de a(1,6) = x_6 y a(1,5) = x_5 en k_6, el valor de nodo padre a(2,3) se obtiene mediante a(2,3) = H(a(1,5)+a(1,6)),
ii) a partir del a(2,3) obtenido y el siguiente valor de nodo en k_6, es decir, a(2,4) de siguiente nivel de nodos no hoja, el valor de nodo padre a(3,2) se obtiene mediante a(3,2) = H(a(2,3)+a(2,4)),
iii) a partir del a(3,2) obtenido y el siguiente valor de nodo en k_6, es decir, a(3,1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

7) para el nodo a(1,7) = x_7 = H(D_7) que corresponde al artículo A_7, la clave de verificación es k_7 = {a(1,8),a(2,3),a(3,1)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de a(1,7) = x_7 y a(1,8) = x_8 en k_7, el valor de nodo padre a(2,4) se obtiene mediante a(2,4) = H(a(1,7)+a(1,8)),
ii) a partir del a(2,4) obtenido y el siguiente valor de nodo en k_7, es decir, a(2,3) de siguiente nivel de nodos no hoja, el valor de nodo padre a(3,2) se obtiene mediante a(3,2) = H(a(2,3)+a(2,4)),
iii) a partir del a(3,2) obtenido y el siguiente valor de nodo en k_7, es decir, a(3,1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

8) para el nodo a(1,8) = x_8 = H(D_8) que corresponde al artículo A_8, la clave de verificación es k_8 = {a(1,7),a(2,3),a(3,1)}, a partir de la cual puede recuperarse el valor raíz R a través de las siguientes etapas (ejecutadas de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol):

i) a partir de a(1,8) = x_8 y a(1,7) = x_7 en k_8, el valor de nodo padre a(2,4) se obtiene mediante a(2,4) = H(a(1,7)+a(1,8)),
ii) a partir del a(2,4) obtenido y el siguiente valor de nodo en k_8, es decir, a(2,3) de siguiente nivel de nodos no hoja, el valor de nodo padre a(3,2) se obtiene mediante a(3,2) = H(a(2,3)+a(2,4)),
iii) a partir del a(3,2) obtenido y el siguiente valor de nodo en k_8, es decir, a(3,1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante R = H(a(3,1)+a(3,2)).

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como: R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

En general, para recuperar un valor de nodo raíz (candidato) comenzando desde un valor de nodo hoja dado y los valores de nodo especificados en la clave de verificación asociada con dicho nodo hoja dado, se realizan las siguientes etapas:

- extraer de la secuencia de valores de nodo en la clave de verificación, un valor de nodo (es decir, un valor de firma digital) de cada otro nodo hoja del árbol que tiene el mismo nodo padre que el del nodo hoja dado y calcular una firma digital de una concatenación del valor de nodo dado y, respectivamente de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol, el valor de nodo extraído de dicho cada otro nodo hoja, obteniendo por lo tanto una firma digital de dicho mismo nodo padre del nodo hoja dado;
- sucesivamente en cada siguiente nivel en el árbol y hasta el penúltimo nivel de nodos:

.extraer de la secuencia de valores de nodo en la clave de verificación, un valor de nodo de cada otro nodo no hoja del árbol que tiene el mismo nodo padre que el del mismo nodo padre anterior considerado en la etapa anterior, y
.calcular una firma digital de una concatenación del valor de nodo de dicho cada respectivo otro nodo no hoja y la firma digital obtenida de dicho mismo nodo padre anterior, de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol, obteniendo por lo tanto un valor de nodo de dicho mismo nodo padre de dicho mismo nodo padre anterior; y

- calcular una firma digital de una concatenación de los valores de nodo obtenidos de los nodos no hoja que

corresponden al penúltimo nivel de nodos del árbol de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol, obteniendo por lo tanto una firma digital raíz del nodo raíz del árbol.

Como es obvio a partir del ejemplo anterior, el valor de nodo raíz R puede recuperarse finalmente a partir de cualquier valor de nodo hoja dado por una firma digital de una concatenación de este valor de nodo hoja con únicamente los valores de nodo especificados en la correspondiente clave de verificación. Por lo tanto, el volumen de datos en la información de verificación que es necesario para recuperar el valor de nodo raíz es claramente mucho menor que el volumen de datos necesario para calcular el valor de nodo raíz de referencia (es decir, basándose únicamente en los valores de nodo hoja, calculando todos los valores de nodo no hoja de los niveles intermedios del árbol): esto es una ventaja de la invención en vista de la restricción de tamaño limitado disponible en una marca de seguridad (como un código de barras bidimensional).

De acuerdo con la invención, la marca de seguridad digital 110 de un archivo digital A_i de un lote de artículos incluye la información de verificación V_i que permite operaciones de comprobación tanto en línea como fuera de línea de autenticidad del archivo marcado, de conformidad de sus datos asociados con respecto a los del archivo marcado genuino, proporcionando un enlace único, inmutable y a prueba de falsificación entre los datos digitales D_i de A_i y el hecho de que el archivo digital original marcado A_i pertenece a un lote dado de artículos genuinos, mientras mantiene un tamaño de bit de una representación digital de esta información de verificación V_i en un nivel compatible con un contenido de datos de un código de barras legible por máquina bidimensional que puede leerse fácilmente por un lector convencional: esta información de verificación comprende los datos digitales de artículo D_i y la correspondiente clave de verificación k_i, $V_i = (D_i,k_i)$. Las operaciones de comprobación incluyen recuperar el valor de lote, o firma digital raíz de referencia R del árbol asociado con el lote, leyendo primero los datos digitales D_i y la correspondiente clave de verificación digital k_i en la marca de seguridad legible por máquina 110 de archivo digital A_i, a continuación calcular una firma digital candidata X_i por medio de una función unidireccional de los datos digitales leídos D_i como $X_i = H(D_i)$, y calcular una firma digital raíz candidata R^c como se ha explicado anteriormente a partir de una firma digital de una concatenación de X_i y valores de nodo del árbol de acuerdo con la secuencia de valores de nodo indicados en la clave de verificación digital k_i. Este esquema de aseguramiento, que tiene la ventaja de no necesitar encriptación de datos y, por lo tanto, gestión de claves de encriptación/desencriptación (particularmente, no se incluye ninguna clave criptográfica en la marca de seguridad digital), es mucho más robusto con respecto a un ataque de descifrado de código en comparación con la encriptación convencional de datos por medio de clave de encriptación pública-clave de desencriptación privada (como el sistema RSA "Rivest-Shamir-Adleman", por ejemplo). Como resultado, el tamaño de datos digitales a representarse en la marca de seguridad digital de acuerdo con la invención es compacto y permite usar una representación convencional de códigos de barra 2D (por ejemplo, un código QR) (particularmente útil para archivos digitales listos para imprimir) y, por lo tanto, lectores de código de barras convencionales (o incluso un simple teléfono inteligente programado que tiene una cámara), mientras proporciona un nivel muy alto de robustez contra ataques de descifrado de código. Además, esta marca de seguridad es compatible con comprobación tanto en línea (a través de un servidor que comunica con un lector de códigos) como fuera de línea (a través de un lector de códigos programado) de la autenticidad de un archivo digital marcado y conformidad de sus datos con respecto a los de un archivo digital (original) genuino. También, de acuerdo con la invención, la representación de datos digitales D_i y la de datos de clave k_i pueden diferir, el esquema de concatenación de datos y/o la función unidireccional puede depender del nivel de nodo en el árbol, que proporcionan niveles adicionales de robustez con respecto a ataques de descifrado de código.

Preferentemente, para reducir adicionalmente el tamaño de datos digitales (es decir, información de verificación V) a incluir en una marca de seguridad digital, si los datos digitales D_i de los respectivos archivos digitales originales A_i del lote se distribuyen entre campos dados que son comunes todos los archivos digitales del lote, datos digitales relacionados con estos campos no se incluyen en cada dato digital Di, sino que se agrupan en un bloque de datos de campos separados FDB asociados con el lote de archivos digitales, y:

- la firma digital x_i de un archivo digital original A_i del lote se calcula entonces con la función unidireccional H de una concatenación de los correspondientes datos digitales D_i y los datos digitales del bloque de datos de campos FDB, es decir $x_i = H(D_i+FDB)$; y
- la firma digital raíz de referencia R se pone a disposición del usuario junto con el bloque de datos de campos asociado FDB (que hace también inmutable el bloque de datos de campos).

En una variante de la invención, el bloque de datos de campos FDB se hace accesible para el usuario independientemente de la firma digital raíz de referencia.

La reducción de tamaño anterior es posible en la mayoría de los casos, ya que la mayoría de datos asociados con los archivos digitales de un lote se clasifican de acuerdo con algunos campos para estructurar los datos: por ejemplo para un producto farmacéutico asociado con un archivo digital asegurado, las indicaciones "número de serie", "datos de expiración" etc., únicamente los datos asociados con estos campos se incluyen en D_i (por ejemplo, 12603, mayo 2020, etc.) mientras los nombres comunes de los campos "número de serie",

"datos de expiración" etc. están en el bloque de datos de campos FDB.

Existen muchos métodos conocidos para codificar información. Cualquier método tal puede usarse en implementaciones de cualquier realización de esta invención. Una forma común de marcado es un código QR bien conocido (como una representación de una imagen en 2D incluida en un archivo digital). Como es bien conocido, para un área dada, cuantos más datos es capaz de codificar un código QR, mayor es la densidad de módulo (aproximadamente, densidad de "cuadrados" negros/blancos) que tiene y mayor es la resolución que se requiere para su impresión y lectura. Además de su densidad (en número de módulos en cuadrados), los códigos QR también se clasifican generalmente dependiendo de qué nivel de corrección de errores incluyen. En la actualidad, los diferentes cuatro "niveles" estándar, L, M, Q y H, representando cada uno el grado de "deterioro", es decir, pérdida de datos, a partir del que la imagen de código QR puede mantenerse o recuperarse. Los niveles L, M, Q y H pueden mantener aproximadamente el 7 %, 15 %, 25 % y 30 % de deterioro, respectivamente.

La siguiente tabla muestra al menos valores aproximados para diferentes versiones de código QR:

Versión	Tamaño (en módulos)	Número de bits codificables	
		Nivel L de ECC	Nivel H de ECC
10	57×57	2192	976
25	117×117	10208	4304
40	177×177	23648	10208

No todos los bits pueden usarse para codificar una "carga" de datos, sin embargo, ya que algunos módulos se usan para escanear objetivos, un patrón de máscara y los módulos de corrección de errores. Existe, por lo tanto, una compensación entre la cantidad de información que un código QR (o cualquiera que sea la marca 110 que se usa) puede codificar, y cuánta información se incluye en una información de verificación V y debe codificarse.

Para un tipo elegido de marca de seguridad digital 110 (tal como un código QR), con una capacidad de codificación limitada, una función unidireccional H adecuada también debería, por lo tanto, elegirse: una función cuya salida es demasiado grande en términos de bits requeridos puede ser imposible de usar en absoluto, y una función cuyo alcance es demasiado pequeño puede no ser lo suficientemente segura. Además, en muchas aplicaciones, la escalabilidad puede ser un problema. Por ejemplo, algunos esquemas de seguridad de datos implican firmas que crecen a medida que el número de miembros de un lote aumenta, y que podría limitar de forma inadmisible el tamaño de un lote desde la perspectiva de cuántos bits puede codificar la marca de seguridad digital 110. Esto es por qué, de acuerdo con un modo preferido de la invención, el tipo de función elegido es una función de troceo unidireccional de la familia SHA-2.

Preferentemente se incluye un módulo de cálculo (no mostrado) dentro de un sistema de aseguramiento para ejecutar el código proporcionado para realizar los cálculos para firmar digitalmente los datos digitales de los archivos digitales originales de un lote, para determinar las claves de verificación digitales para los diferentes archivos digitales y para calcular la firma digital raíz de referencia del correspondiente árbol. El sistema de aseguramiento también puede incluir módulos adecuados para introducir valores (preprogramados) que corresponden a los datos digitales D_v del archivo o archivos digitales virtuales A_v. También sería posible realizar externamente los cálculos de troceo relacionados con el archivo (por ejemplo, en un servidor distante conectado), por ejemplo, donde quiera que se fabriquen los archivos digitales, para tener que evitar transmitir datos digitales Di sin procesar a través de una red desde ese sitio (o sitios) hasta el sistema de aseguramiento, si eso es un problema. Para cada archivo digital A_i, se compila correspondiente información de verificación V_i y se codifica (representa) en alguna forma de marca de seguridad digital 110 legible por máquina que se incluye, a continuación, en el respectivo artículo.

Para cualquier archivo digital "virtual" A_v, su correspondiente información de verificación $V_v = (D_v,k_v)$ puede asociarse internamente con el mismo mediante el sistema de aseguramiento. La información de verificación generalmente al menos incluye, para cualquier archivo digital A_i de un lote de archivos digitales, los correspondientes datos digitales D_i y la correspondiente clave de verificación digital k_i: es decir $V_i = (D_i,k_i)$.

Datos digitales adicionales pueden asociarse adicionalmente con un archivo digital y pueden incluir, por ejemplo, el valor de lote, es decir, firma digital raíz de referencia R, o cualquier otra información que el diseñador de sistema (o administrador de sistema) elija incluir, tal como, por ejemplo, un número de serie de artículo asociado, ID de lote, información de fecha/hora, nombre de producto, un URL que apunta a otra información en línea asociada con o bien el artículo individual (tal como una imagen del artículo, o de su etiquetado o embalaje, etc.), o bien el lote, o el fabricante/suministrador, un número de teléfono al que se puede llamar para su verificación, etc. Los datos digitales adicionales pueden almacenarse en una base de datos de información consultable accesible por un usuario (a través de una interfaz de base de datos de información).

Una vez que se ha calculado la verificación digital k_i de un archivo digital original A_i, e incluido (es decir, a través de a través de codificación o cualquier representación de datos elegida), junto con los correspondientes datos digitales D_i, en la marca de seguridad digital 110 legible por máquina en el archivo digital A_i, el archivo digital original marcado resultante y sus datos digitales asociados se aseguran, de hecho, contra falsificación y manipulación.

Un usuario, receptor de un archivo digital tal como A_1 por ejemplo, puede escanear (o de otra manera leer), a continuación, con un formador de imágenes (lector) la marca de seguridad digital de A_1 y extraer los datos digitales D_1 y la clave de verificación digital k_1, (y cualquier otra información que puede haberse codificado en la marca). En aras de la verificación del archivo digital marcado A_1, el usuario debe recuperar primero la información de verificación $V_1=(D_1,k_1)$ de la marca de seguridad digital 110 de A_1 y, por lo tanto, calcular la firma digital x_1 a partir de los datos digitales D_1 extraídos: para hacer eso el usuario debe conocer la función unidireccional a usar para calcular una firma digital, en este punto la función unidireccional H() (por ejemplo, un troceo SHA-256), y a continuación realizar la operación $x_1=H(D_1)$ para obtener los datos completos (x_1,k_1) necesarios para calcular una correspondiente firma digital raíz candidata R^c. El usuario puede recibir, por ejemplo, la función unidireccional de forma segura (por ejemplo, usando un par de claves pública/privada) o solicitando esta al proveedor de archivo digital o cualquier entidad que haya creado las firmas y claves, o que haya ya programado la misma en la unidad de procesamiento de un usuario de su formador de imágenes.

A continuación, para calcular tal firma digital raíz candidata R^c, el usuario necesitará conocer adicionalmente el tipo de esquema de datos (para concatenar valores de nodo a través de H(a(i,j)+a(i,k)) a usar para eso: el usuario puede recibir esta información de cualquier manera conocida, ya sea de forma segura (por ejemplo, usando un par de claves pública/privada) o simplemente solicitando esta al proveedor de archivo digital o cualquier entidad que creó los datos de verificación, o que haya ya programado la misma en la unidad de procesamiento del usuario. Sin embargo, el esquema de concatenación puede corresponder, de hecho, a una simple "unión extremo a extremo" convencional de los dos bloques de datos digitales que corresponden respectivamente a los dos valores de nodo: en este caso, no debe transmitirse al usuario ningún esquema específico. En algunas variantes, el esquema de concatenación puede insertar adicionalmente un bloque de concatenación, que puede contener datos específicos a la clasificación o nivel de los bloques de datos digitales concatenados en el árbol, con el resultado de hacer incluso más difícil un ataque de descifrado de código.

Conociendo el esquema de concatenación de datos, el usuario puede calcular entonces (por ejemplo, a través del formador de imágenes adecuadamente programado) la firma digital raíz candidata R^c como se ha explicado anteriormente firmando digitalmente etapa a etapa una concatenación de la firma digital x_1 y valores de nodo de acuerdo con la secuencia de nodos especificada en la clave de verificación digital k_1, véase el artículo 1) anterior relacionado con el nodo a(1,1), ejecutada de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol. En este punto, la firma digital raíz candidata se obtiene como (proporcionándose el orden de nodos en el árbol por los respectivos índices (i,j) del nivel y clasificación en el nivel):

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

Esta firma digital raíz candidata R^c calculada debería ser, entonces, igual al valor R de referencia disponible (o publicado): este valor puede haberse adquirido anteriormente por el usuario y/o haberse almacenado ya en una memoria de la unidad de procesamiento del formador de imágenes, podría ser también un valor que solicita el receptor y recibe del administrador de sistema de cualquier manera conocida. Si la R^c candidata y las firmas digitales raíz de referencia R disponibles coinciden, entonces este cálculo verifica la información en la marca segura digital 110 y confirma que el archivo digital A_1 es del lote correcto.

Un enlace para acceder a la firma digital raíz de referencia R para el lote que corresponde al archivo digital A_1 podría incluirse en la marca de seguridad digital 110 (por ejemplo, una dirección web, si R puede recuperarse en un sitio web correspondiente), aunque no es una variante preferida.

Un usuario, receptor de un archivo digital tal como A_1 por ejemplo, puede escanear (o de otra manera leer), a continuación, con un lector la marca de seguridad digital en A_1 y extraer los datos digitales D_1 y la clave de verificación digital k_1, (y cualquier otra información que puede haberse codificado en la marca de seguridad digital). Un ejemplo de lector es un ordenador con un visualizador, o incluso un teléfono inteligente (programable). En aras de la verificación del archivo marcado A_1, el usuario debe recuperar primero la información de verificación $V_1=(D_1,k_1)$ de la marca de seguridad digital en A_1 y, por lo tanto, calcular la firma de archivo digital x_1 a partir de los datos digitales D_1 extraídos: para hacer eso el usuario debe conocer la función unidireccional a usar para calcular una firma digital, en este punto la función de troceo H(), y a continuación realizar la operación $x_1=H(D_1)$ para obtener los datos completos (x_1,k_1) necesarios para calcular una correspondiente firma digital raíz candidata B^c. El usuario puede recibir, por ejemplo, la función unidireccional de forma segura (por ejemplo, usando un par de claves pública/privada) o solicitando esta al

proveedor de archivo digital o cualquier entidad que haya creado las firmas y claves, o que haya ya programado la misma en la unidad de procesamiento de un usuario de su lector.

Preferentemente, la firma digital raíz de referencia (es decir, "valor de lote") R se almacena en una base de datos raíz consultable que puede accederse (a través de un enlace de comunicación) por el usuario por medio de su ordenador equipado con una unidad de comunicación, como es el caso en el ejemplo anterior de un teléfono inteligente. El usuario que tiene que verificar el archivo digital A_1 puede simplemente enviar una petición raíz con su teléfono inteligente a la dirección de la base de datos, a través de una interfaz de acceso de la base de datos, conteniendo la petición los datos digitales D_1 leídos en la marca de seguridad digital 110 de A_1 (o la firma digital calculada $x_1 = H(D_1)$) que permiten recuperar el correspondiente valor de lote de referencia R, y la interfaz de acceso devolverá la firma digital raíz de referencia R al teléfono inteligente. La base de datos puede asegurarse mediante una cadena de bloques para fortalecer la inmutabilidad de las firmas digitales raíz almacenadas. Una ventaja de la invención es hacer prácticamente inmutable el enlace entre un objeto físico, es decir, un archivo digital original almacenado en una memoria, y sus atributos, es decir, los datos digitales asociados y su pertenencia a un lote específico de archivos digitales, a través de la correspondiente firma digital raíz.

El proceso de verificación anteriormente mencionado de un archivo digital A_i también puede servir para autenticar contenido de datos legibles por humanos de A_i en una correspondiente versión impresa del archivo digital A_i. De hecho, un usuario puede leer en un visualizador de un ordenador los correspondientes datos digitales D_i según se decodifican de la marca de seguridad digital en el archivo digital A_i por el ordenador, y comprobar visualmente que la información visualizada es consistente con los datos impresos en la versión impresa del archivo digital.

En una realización preferida, los datos digitales D_i incluyen adicionalmente datos digitales de característica (CDD) de una correspondiente característica física única de un objeto, o un individuo, asociado con el archivo digital original marcado A_i que puede usarse para autenticar (materialmente) el objeto asociado, o el individuo asociado, comparando los datos digitales de característica extraídos de la marca de seguridad digital y correspondientes datos de detección de la característica física única obtenida de un sensor adecuado. Por lo tanto, siendo CDD_i los datos digitales de característica que corresponden a la característica física única en un archivo digital A_i, los correspondientes datos de firma física única UPS_i pueden obtenerse mediante la codificación de CDD_i (preferentemente por medio de una función unidireccional): por ejemplo, tomando un troceo de los datos digitales de característica CDD_i, es decir $UPS_i = H(CDD_i)$. Sin embargo, en su lugar podría usarse cualquier otra codificación conocida: por ejemplo, para tener una forma corta, es posible usar un algoritmo de firma digital de curva elíptica. Como un ejemplo muy simplificado ilustrativo de datos digitales de característica CDD_i que corresponden a una característica física única de un objeto OBJ_i asociado con un archivo digital A_i, consideramos una simple imagen digital obtenida formando una imagen del objeto OBJ_i (o una zona específica en OBJ_i), por ejemplo, por medio de la cámara de un teléfono inteligente, siendo los correspondientes datos de firma física única UPS_i, por ejemplo, un troceo de la imagen digital, $UPS_i = H(CDD_i)$. Los datos digitales de característica CDD_i que han generado la firma UPS_i son los datos digitales de característica de referencia para A_i y la firma obtenida UPS_i son los correspondientes datos de firma física única de referencia para A_i. Preferentemente, UPS_i, es decir, los datos de firma física única de referencia para archivo digital A_i, se almacena en una base de datos consultable o en una cadena de bloques (o en una base de datos asegurada por una cadena de bloques) accesible para los usuarios (por ejemplo, a través de una petición que contiene los datos digitales D_i leídos en la marca de seguridad digital en el archivo digital A_i, o su correspondiente firma de archivo digital x_i). Por lo tanto, la UPS_i almacenada adquiere un carácter inmutable. Una copia de CDD_i puede almacenarse adicionalmente en la memoria del teléfono inteligente (o lector u ordenador) del usuario. En una variante de la realización, una copia de UPS_i también puede almacenarse adicionalmente en la memoria del teléfono inteligente (o lector u ordenador) del usuario para permitir una operación de comprobación fuera de línea.

Puede realizarse una comprobación de autenticidad del archivo digital A_i extrayendo datos digitales de característica candidatos CDD_i^c de los datos digitales D_i leídos (en este punto, con una aplicación de decodificación ejecutándose en el teléfono inteligente) en la marca de seguridad digital incluida en el archivo digital A_i, y comparando los mismos con los datos digitales de característica de referencia CDD_i almacenados en la memoria del teléfono inteligente: en caso de coincidencia $CDD_i^c = CDD_i$, el archivo digital A_i se considera como genuino (su contenido digital corresponde al de un archivo digital original marcado genuino). Si los datos digitales de característica de referencia CDD_i no se almacenan en la memoria del teléfono inteligente, sino que en su lugar los datos de firma física única UPS_i se almacenan en la memoria del teléfono inteligente ((con la ventaja de ocupar mucha menos memoria en comparación con CDD), entonces la autenticidad de A_i puede aún comprobarse verificando que los datos de firma física única candidatos UPS_i^c obtenidos calculando el valor de troceo de los datos digitales de característica candidatos CDD_i^c extraídos de los datos digitales D_i, es decir $UPS_i^c = H(CDD_i^c)$, coincidan con los datos de firma física única de referencia UPS_i almacenados en la memoria.

Un usuario puede comprobar adicionalmente la autenticidad de un archivo digital recibido A_i, aún a través de

un proceso fuera de línea (autoverificación), detectando dicha característica física única en el objeto o individuo asociado con el archivo digital A_i, por medio de un sensor con capacidad de realizar tal medición (en este punto, la cámara del teléfono inteligente), y obteniendo unos datos digitales de característica candidatos CDD_i^c a partir de la característica detectada (en este punto, una imagen digital tomada por el teléfono inteligente). A continuación, el usuario puede comparar (a través de la imagen unidad de procesamiento de su teléfono inteligente, o visualmente en un visualizador del teléfono inteligente) los CDD_i^c obtenidos con una copia de los CDD_i de referencia (almacenados en la memoria del teléfono inteligente): en caso de una coincidencia "razonable" $CDD_i^c \approx CDD_i$ (es decir, los dos datos digitales concuerdan dentro de alguna tolerancia dada o criterio de similitud), el archivo digital A_i se considera como genuino (es decir, su contenido digital corresponde al de un archivo digital original marcado genuino).

Además, el usuario también puede calcular adicionalmente los correspondientes datos de firma física candidata a partir de la copia de los CDD_i de referencia almacenados en la memoria del teléfono inteligente como $UPS_i^c = H(CDD_i)$, y comparar los mismos con los datos de firma física de referencia UPS_i almacenados en la memoria del teléfono inteligente: en caso de coincidencia $UPS_i^c = UPS_i$, el archivo digital A_i se confirma como genuino con un grado de confianza incluso mayor (ya que un solo bit de diferencia es suficiente para provocar una falta de coincidencia). Además, en caso de coincidencia, también se autentican los datos digitales D_i asociados con A_i, que se han verificado como que corresponden a los de un archivo digital genuino, como se ha explicado anteriormente recuperando el correspondiente valor de lote R de la información de verificación (D_i,k_i) leída almacenada en la marca de seguridad digital en A_i.

En una variante de la realización, la comprobación de autenticidad de un archivo digital A_i por un usuario puede realizarse a través de un proceso en línea. En este caso, los datos de referencia, es decir los datos digitales de característica CDDi y/o los datos de firma física única de referencia UPSi, se almacenan en una base de datos consultable accesible por el usuario en la que los datos de referencia relacionados con un archivo digital A_i se almacenan en asociación con, respectivamente, los correspondientes datos digitales D_i (incluidos en la marca de seguridad digital en A_i) o con la correspondiente firma de archivo digital x_i (que puede calcularse por el usuario una vez que los datos D_i se extraen de la marca de seguridad digital a través de la operación $x_i=H(D_i)$): los datos de referencia pueden solicitarse enviando a la base de datos una consulta que contiene, respectivamente, D_i o x_i.

Una forma convencional de aseguramiento de un objeto es aplicar en el mismo una marca de seguridad basada en material (posiblemente a prueba de manipulaciones), es decir, una marca que tiene una propiedad física o química intrínseca detectable que es muy difícil (si no imposible) de reproducir. Si un sensor apropiado detecta esta propiedad intrínseca en una marca, esta marca se considera, entonces, como genuina con un alto grado de confianza y, por lo tanto, también el correspondiente objeto marcado. Existen muchos ejemplos de tales propiedades intrínsecas de autenticación conocidas: la marca puede incluir algunas partículas, posiblemente dispersadas de forma aleatoria, o tiene una estructura en capas específica, teniendo propiedades intrínsecas de reflexión óptica o transmisión o absorción o incluso emisión (luminiscencia, por ejemplo, o polarización o difracción o interferencia...), posiblemente detectable en condiciones de iluminación específicas "luz" de contenido espectral específico. Esta propiedad intrínseca puede resultar de la composición química específica del material de la marca: por ejemplo, pigmentos luminiscentes (posiblemente no disponibles comercialmente) pueden dispersarse en una tinta usada para imprimir algún patrón en el objeto y se usan para emitir una luz específica (por ejemplo, en una ventana espectral dentro del intervalo infrarrojo) tras su iluminación con una luz específica (por ejemplo, con luz en el intervalo espectral de UV). Esto se usa para asegurar billetes de banco, por ejemplo. Pueden usarse otras propiedades intrínsecas: por ejemplo, las partículas luminiscentes en la marca pueden tener un tiempo de extinción de emisión de luminiscencia específico después de su iluminación con un pulso de luz de excitación apropiado. Otros tipos de propiedades intrínsecas son la propiedad magnética de partículas incluidas, o incluso una propiedad de "huella" del propio objeto tal como, por ejemplo, el posicionamiento relativo de fibras dispersadas inherentemente aleatoriamente de un sustrato de papel de un documento, en una zona dada en el documento, que, cuando se observa con una resolución suficiente, puede servir para extraer una firma característica única, o algunos artefactos de impresión aleatorios de datos impresos en el objeto que, visualizados con una magnificación suficiente, también pueden conducir a una firma única, etc. El principal problema con una propiedad de huella intrínseca de un objeto es su robustez con respecto a envejecimiento o desgaste. Sin embargo, una marca de seguridad basada en material no siempre permite también asegurar datos asociados con el objeto marcado: por ejemplo, incluso si un documento está marcado con una marca de seguridad basada en material como un logotipo impreso con una tinta de seguridad en alguna zona del documento, los datos impresos en la parte restante del documento aún pueden falsificarse. Además, las firmas de autenticación demasiado complejas necesitan capacidades de almacenamiento significativas que implican bases de datos externas, y enlaces de comunicación para consultar tales bases de datos, de modo que no es posible una autenticación fuera de línea de un objeto. De acuerdo con la invención, un objeto marcado por medio de una marca de seguridad basada en material y asociado con un archivo digital marcado (digitalmente) se asegura por el conflicto que resulta del hecho de que los datos digitales de característica que corresponden a la característica física única del objeto marcado, o sus correspondientes datos de firma física única, se enlazan de forma inmutable (gracias a la publicación o almacenamiento de la firma digital

agregada en una cadena de bloques) y a prueba de falsificación con los datos digitales en la marca de seguridad digital que con parte del archivo digital asociado. La invención puede usarse, por lo tanto, para asegurar tanto un lote de objetos como un correspondiente lote de archivos digitales asociados.

Por supuesto, puede usarse cualquier otra propiedad física/química intrínseca conocida para obtener los datos digitales de característica CDD_i relacionados con una característica física única de un objeto OBJ_i asociado con un archivo digital A_i, y los correspondientes datos de firma física única UPS_i. Como otro ejemplo ilustrativo, es posible imprimir un código de barras 2D que forma una marca de seguridad basada en material en un objeto con una tinta de seguridad que incluye un pigmento luminiscente que tiene su tiempo de extinción de característica constante así como su ventaja de longitud de onda de excitación de luz y su ventana de longitud de onda de emisión de luminiscencia: el resultado es una tinta que tiene un tiempo de extinción de referencia específico τ que sirve como una "huella dactilar" material de la tinta. Basta con iluminar el código de barras con una luz de excitación en una ventana de longitud de onda de iluminación que cubre la ventana de longitud de onda de excitación de pigmento, y recopilar una luz de luminiscencia resultante del código de barras con un sensor con capacidad de detectar la intensidad de luz dentro de la ventana de longitud de onda de emisión de luminiscencia para autenticar el código de barras y, por lo tanto, el objeto. Por ejemplo, el lector de un usuario puede estar equipado con un flash con capacidad de emitir la luz de excitación al código de barras, un fotodiodo con capacidad de recopilar el correspondiente perfil de intensidad de luz de luminiscencia I(t) (durante un intervalo de tiempo de detección) del código de barras, y estando la CPU del lector programada para calcular un valor de tiempo de extinción a partir del perfil de intensidad I(t) recopilado. Por ejemplo, la ventana de longitud de onda de excitación puede estar dentro de la banda UV (ultravioleta) y la ventana de longitud de onda de emisión dentro de la banda IR (infrarrojos). Si, durante la verificación del objeto, la intensidad de luz de luminiscencia recopilada por el formador de imágenes del usuario muestra una extinción de característica con el paso del tiempo que corresponde a un tiempo de extinción candidato τ_c, entonces la tinta y, en consecuencia el objeto, se considera como genuino si $\tau_c \approx \tau$ (dentro de un intervalo de tolerancia dado). En este caso, los datos digitales de característica CDD_i de un objeto marcado OBJ_i incluye al menos el valor de tiempo de extinción de referencia τ (y posiblemente datos relacionados con la ventana de longitud de onda de excitación y la ventana de longitud de onda de emisión). Como es obvio a partir de los ejemplos anteriores, incluyendo datos digitales (únicos) de referencia de característica en la información de verificación de una marca de seguridad digital de un archivo digital asociado A_i tiene el efecto técnico de proporcionar un enlace a prueba de falsificación entre los datos digitales del archivo digital y los datos de autenticación de su objeto asociado.

Otra realización ilustrativa de la invención se refiere a un lote de documentos de identificación biométrica, por ejemplo, pasaportes digitales biométricos, como se muestra en la Figura 2A. Cada pasaporte digital, como un archivo digital, se asocia con un correspondiente individuo, es decir, el titular de pasaporte. Por razones de claridad, los datos digitales de A_1 se representan en la Figura 2A como información textual y alfanumérica equivalente (es decir, legible por humanos), por ejemplo, como podría visualizare a partir de un archivo pdf ("Formato de Documento Portable") digital, y la marca de seguridad digital se muestra como un patrón bidimensional de código QR convencional equivalente. Esta realización de la invención es particularmente útil para crear archivos digitales imprimibles, como archivos digitales listos para imprimir, para permitir que una impresora emita un documento asegurado impreso directamente a partir de un correspondiente archivo digital imprimible asegurado (por ejemplo, un archivo digital relacionado con un documento de identidad, diploma, contrato, etc.). En este ejemplo usaremos una función de troceo como una función unidireccional para firmar los datos digitales de pasaporte, preferentemente una función de troceo SHA-256 en vista de su bien conocida robustez. De hecho, en vista de un tamaño dado del lote, la función de troceo que se selecciona (que tiene su propio listado de ranuras) para el propósito de firmar los datos digitales de pasaporte es, por lo tanto, un ejemplo de una función de encriptado unidireccional de tal forma que cada pasaporte digital distinto tiene su firma de pasaporte digital distinta, que por lo tanto hace la firma única. El dominio de una función de troceo (es decir, el conjunto de posibles claves) que es mayor que su intervalo (es decir, el número de diferentes índices de tabla), correlacionará diferentes claves con un mismo índice que podría resultar en colisiones: tales colisiones pueden evitarse, cuando se conoce el tamaño del lote, considerando el listado de ranuras asociado con la tabla de función de troceo de una función de troceo y reteniendo únicamente una función que proporciona cero colisiones, o eligiendo independientemente un esquema de resolución de colisiones de tabla de troceo (por ejemplo, tal como función de troceo combinado, función de troceo de cuco, o función de troceo de rayuela).

La Figura 2A muestra un ejemplo de pasaporte biométrico digital A1 asegurado con una marca de seguridad digital legible por máquina 210 (en este punto un código QR) codificada en A_1, y que comprende datos digitales de pasaporte 230 que contienen datos de pasaporte convencionales, por ejemplo, datos digitales que representan un título del documento 230a ("Pasaporte"), un conjunto de datos biográficos del titular del pasaporte 230b: apellido ("Doe"), nombre ("John"), sexo ("M"), fecha de nacimiento ("20 de marzo de 1975"), nacionalidad ("Estados Unidos"), origen ("Des Moines"), lugar de nacimiento ("Oakland"), una fecha de emisión del pasaporte 230c ("24 de febrero de 2018") y un periodo de validez 230d ("23 de febrero de 2020"). Estos datos digitales de pasaporte pueden comprender adicionalmente algún número o números de serie (únicos) 235 asignados por la autoridad que entrega el pasaporte (en este punto "12345"). Los datos digitales

de pasaporte comprenden además datos biométricos del titular del pasaporte como datos digitales de característica (CDD) que corresponden a una característica física única de un individuo asociado con el pasaporte digital. Una representación legible por máquina 230e (por ejemplo, una alfanumérica) de datos que caracteriza dicha característica física única (no mostrada), que corresponde a dichos datos biométricos, se asocia con los datos digitales de pasaporte 230. Una representación de datos digitales se entenderá en un sentido amplio del término: esta representación de datos únicamente necesita habilitar la recuperación de los datos digitales originales. La representación de datos legible por máquina 230e, es decir, los datos biométricos, de la característica física única puede corresponder, por ejemplo, a datos de identificación de huella dactilar o datos de identificación de iris del titular del pasaporte digital. Por ejemplo, los datos biométricos 230e que corresponden a una huella dactilar de una persona pueden resultar de un análisis de un conjunto de características específicas de puntos característicos de huellas dactilares como finalización de crestas, crestas cortas y de bifurcación (de acuerdo con el Sistema de Clasificación de Henry convencional).

Por lo tanto, para un pasaporte digital dado A_j del lote de μ pasaportes biométricos digitales entregados, en este punto con μ = 1024, los datos digitales de pasaporte D_j asociados incluyen los datos digitales 230a-230e anteriormente mencionados. En una variante de la realización, los datos digitales de pasaporte asociados D_j pueden incluir únicamente los valores de los campos que son comunes a todos los pasaportes entregados, mientras los campos en común, es decir, "Pasaporte", "Apellido", "Sexo", "Fecha de nacimiento", "Nacionalidad", "Origen", "Lugar de nacimiento", "Fecha de emisión" y "Validez" se incluyen en un bloque de datos de campos separados FDB como se ha explicado anteriormente: por ejemplo, D_1 contiene únicamente una representación de los valores de campo "Doe", "John", "M", "20 de marzo de 1975", "Estados Unidos", "Des Moines", "Oakland", "24 de febrero de 2018" y "23 de febrero de 2020".

Preferentemente, los datos digitales de pasaporte adicionales se asocian con los datos digitales de pasaporte 230 anteriormente mencionados. Por ejemplo, una imagen digital del patrón de huella dactilar del titular del pasaporte, o una fotografía de identidad digital, etc. En una variante de la realización, estos datos digitales de pasaporte adicionales se almacenan en una base de datos de información consultable 250 que puede consultarse a través de una petición de información que contiene algunos datos de pasaporte (por ejemplo, el nombre del titular o los datos biométricos o datos de la marca de seguridad o el número de serie único 235) para recuperar los datos de patrón de huella dactilar correspondientes y recibir los mismos de vuelta. Preferentemente, se incluye un enlace a la base de datos de información 250, como datos de acceso a información 240, en el pasaporte digital: en este punto estos datos de acceso a información se codifican en una representación digital de un código QR que contiene un índice de referencia para recuperar correspondientes datos adicionales en la base de datos de información 250. Sin embargo, en una variante de operación de control de pasaporte que implica el acceso a una base de datos de información distante (operación en línea), el código QR podría contener, por ejemplo, el URL de la base de datos de información que es accesible a través de la web.

A continuación se calcula una firma de pasaporte digital con una función de troceo unidireccional de los datos digitales de pasaporte D_j que corresponden a los datos digitales de pasaporte 230a-230e del pasaporte digital A_j por medio, por ejemplo, de la función de troceo SHA-256 robusta anteriormente mencionada para obtener la correspondiente firma digital de pasaporte (única) $x_j=H(D_j)$. De una misma forma, se calculan las firmas digitales de pasaporte de todos los pasaportes digitales en el lote, para todos los diferentes titulares.

A partir de todas las firmas de los pasaportes en el lote, se calcula una firma digital raíz de referencia R de acuerdo con un orden de árbol y orden de concatenación de árbol de un árbol (binario) asociado, como se ha explicado anteriormente. Ya que existen μ = 1024 pasaportes en el lote, el árbol binario correspondiente tiene 1024 nodos hoja a(1,1),…,a(1024) para el primer nivel, 512 nodos no hoja a(2,1),…,a(2,512) para el segundo nivel, 256 nodos no hoja a(3,1),…,a(3,256) para el tercer nivel, etc., hasta el penúltimo nivel de nodos (en este punto, nivel 10) con nodos no hoja a(10,1) y a(10,2), y el nodo superior que corresponde al nodo raíz R (nivel 11 del árbol). Los valores de nodo hoja son $a(1,j) = x_j = H(D_j)$, j=1,…,1024, los valores de nodo de segundo nivel son a(2,1) = H(a(1,1)+a(1,2)),…., a(2,512) = H(a(1,1023)+a(1,1024)), etc., y la firma digital raíz de referencia R es R = H(a(10,1)+a(10,2)). Cada clave de verificación digital k_j es, por lo tanto, una secuencia de 10 valores de nodo. La marca de seguridad digital 210 del pasaporte digital A_j incluye los datos digitales de pasaporte D_j y la correspondiente clave de verificación digital k_j (es decir, la información de verificación $V_j = (D_j,k_j)$).

La operación de comprobar que los datos digitales de pasaporte D_j y la clave de verificación digital k_j en la marca de seguridad digital 210 de a pasaporte digital biométrico A_j corresponden, de hecho, a datos de pasaporte de un pasaporte digital biométrico genuino que pertenece al lote de μ pasaportes digitales biométricos que tienen el valor de lote R únicamente necesita calcular la firma digital de pasaporte $x_j = H(D_j)$ y verificar que x_j y la clave de verificación digital k_j permiten recuperar la correspondiente firma digital raíz de referencia R disponible a través de la composición de diez veces (ya que en este punto, el árbol tiene diez niveles por debajo del nivel raíz) una función de troceo de una concatenación del valor de nodo a(1,j) y los valores de nodo en k_j (de acuerdo con el orden de nodos en el árbol binario y el orden de concatenación de árbol con el esquema de concatenación convencional). En consecuencia, un pasaporte digital biométrico

asegurado de acuerdo con la invención proporciona tanto un enlace a prueba de falsificación entre los "datos personales" y los "datos biométricos" de su titular, como un enlace único y a prueba de falsificación entre la persona física del titular y la identidad del titular.

La Figura 2B ilustra un proceso de control del pasaporte digital biométrico asegurado A_1 de la Figura 2A, con su marca de datos de pasaporte 230 que corresponden a un cierto John Doe, con sus datos biométricos 230e que corresponden a la huella dactilar de John Doe, y con datos digitales de pasaporte adicionales que corresponden a una fotografía de identidad digital 255 de John Doe que es accesible a través del enlace a la base de datos de información 250 incluida en la marca de acceso a información 240. Los datos de pasaporte comprenden además el número de serie único 235 asignado por la autoridad que ha entregado el pasaporte. La marca de seguridad digital 210 del pasaporte A_1 contiene la información de verificación (D_1,k_1), con datos digitales de pasaporte D_1 que corresponden a los datos de pasaporte impresos 230a-230d, los datos biométricos 230e y el número de serie único 235, y la clave de verificación digital k_1 que corresponde a la secuencia de 10 valores de nodo {a(1,2),a(2,2),…,a(10,2)} que son necesarios para recuperar el valor raíz R del valor de nodo a(1,1) del pasaporte digital A_1 (con $a(1,1) = x_1 = H(D_1)$). La firma digital raíz de referencia R puede tener una indicación de tiempo y almacenarse en una cadena de bloques 260. En este ejemplo, los datos biométricos 230e de los respectivos titulares de los pasaportes biométricos del lote se almacenan también en la cadena de bloques 260 en asociación con, respectivamente, sus correspondientes números de serie únicos (para hacer estos datos inmutables). Los datos biométricos almacenados de John Doe pueden recuperarse enviando una petición a la cadena de bloques 260 indicando el número de serie único 235 mencionado en su pasaporte. Las autoridades a cargo de controlar la identidad de las personas (por ejemplo, la policía, las aduanas, etc.) pueden acceder a la cadena de bloques 260 a través de un enlace de comunicación y, en esta realización ilustrativa, también tienen capacidades de almacenamiento local para almacenar las firmas digitales raíz (publicadas) de todos los lotes entregados de pasaportes digitales biométricos. En el ejemplo mostrado en la Figura 2B, la base de datos de información 250 es local (es decir, directamente accesible por las autoridades, sin tener que usar una red de comunicación pública). Además, estas autoridades están equipadas con escáneres de huellas dactilares 270 para capturar las huellas dactilares de individuos y calcular correspondientes representaciones legibles por máquina de datos que caracterizan las huellas dactilares capturadas, es decir, los datos biométricos 230e.

Durante un control de identidad de John Doe, digamos por un policía o agente de aduanas, el agente recibe el pasaporte digital biométrico asegurado A_1 de John Doe, lee y decodifica la información de verificación D_1,k_1) almacenada en la marca de seguridad digital 210 en el pasaporte digital por medio de un lector apropiado, que puede ser, por ejemplo, un ordenador programado 290 adecuado, estando el ordenador conectado a las capacidades de almacenamiento local 250. Habiendo leído los datos digitales de pasaporte D_1 y la clave de verificación digital k_1 y enviado los mismos al ordenador 290, una aplicación especializada (con función de troceo programada H y concatenación de valores de nodo) que se ejecuta en el ordenador 290 calcula la firma digital de pasaporte x_1 (como $x_1=H(D_1)$) y un valor de lote candidato R^c como:
H(H(H(H(H(H(H(H(a(1,1)+a(1,2))+a(2,2))+..)+..)+..)+..)+..)+..)+a(9,2))+a(10,2)),
es decir la composición de diez veces una función de troceo de una concatenación del valor de nodo a(1,1) y los valores de nodo en k_1= {a(1,2),a(2,2),…,a(10,2)}. A continuación, el ordenador puede buscar, por ejemplo, en la base de datos de información local 250 una firma digital raíz de referencia R que coincide con el valor candidato R^c: en el caso en el que no hay coincidencia, el pasaporte es un pasaporte falsificado y "John Doe" (es decir, el individuo examinado que reclama que su nombre es John Doe) puede ser arrestado. En el caso en el que R^c coincide con alguna firma digital raíz de referencia almacenada, el pasaporte se considera como genuino y el agente puede realizar comprobaciones de seguridad adicionales:

- el agente recupera la fotografía de identidad digital 255 almacenada en la base de datos de información 250, enviando una petición a través del ordenador 290 que contiene el número de serie 235 impreso en A_1, recibe la misma de vuelta y visualiza la fotografía de identidad 255 recibida en una pantalla del ordenador 290: el agente entonces puede comparar visualmente el rostro visualizado (es decir, la de un cierto John Doe) con el del individuo que se está comprobando y estimar si los dos rostros son similares o no; y
- el agente recupera los datos biométricos 230e en el pasaporte A1 leyendo estos datos en la marca de seguridad digital 210 con el ordenador 290, y escanea la huella dactilar del individuo por medio de un escáner de huellas dactilares 270 conectado al ordenador 290 y obtiene los datos biométricos del individuo correspondiente: el agente, a continuación, comprueba por medio de un programa que se ejecuta en el ordenador 290 si los datos biométricos 230e recuperados son similares (dentro de un margen dado de error) a los datos biométricos del individuo obtenidos.

Si los dos rostros y los datos biométricos se evalúan como similares, todo está correcto y el individuo comprobado es, de hecho, el John Doe real, el titular del pasaporte biométrico A_1 genuino.

En el caso en el que cualquiera de las comprobaciones de seguridad adicionales anteriores falla, claramente, el individuo enfrente del agente no es el verdadero titular del pasaporte biométrico A_1 genuino. Por lo tanto, con un pasaporte digital biométrico asegurado de acuerdo con la invención una simple comprobación fuera de línea puede detectar rápidamente cualquier fraude.

De hecho, es incluso posible reducir un documento de pasaporte biométrico digital a un simple archivo digital con solo una representación digital de código de barras 2D (como el ejemplo anterior de un código QR) que incluye la información de verificación V = (D,k): comprendiendo V los datos biográficos del titular y datos biométricos (únicos), como la huella dactilar del titular (dentro de los datos digitales de pasaporte D) y la clave de verificación. De hecho, de acuerdo con la invención, incluso este pasaporte digital asegurado "reducido" se aprovecha totalmente del enlace a prueba de falsificación anteriormente mencionado creado entre los "datos biográficos personales" y los "datos biométricos" del titular de pasaporte, y el enlace único y a prueba de falsificación entre la persona física del titular y la identidad del titular.

Otra realización ilustrativa de la invención se refiere a componentes de una aeronave, como se muestra en la Figura 3. Debido al precio muy alto de ciertos componentes críticos cuyo fallo podría afectar a la seguridad de la aeronave, como algunas partes de los reactores (por ejemplo, palas de turbina, bombas...) o del tren de aterrizaje, o baterías, etc., los falsificadores están interesados en producir copias de estos componentes, pero por supuesto sin cumplir con los requisitos técnicos de seguridad requeridos debido a su generalmente menor calidad. Incluso si un componente de aeronave se marca generalmente con un correspondiente número de serie único para identificar el mismo, esa clase de marca puede falsificarse fácilmente. Estas partes de avión falsificadas generalmente son defectuosas y pueden provocar graves daños o incluso accidentes aéreos. Este es un problema de seguridad creciente en la actualidad. Además, incluso si los componentes son genuinos, pueden no ser convenientes para ciertas versiones de un mismo tipo de aeronave, y existe un grave riesgo de que un componente inapropiado se use involuntariamente para reparar una aeronave dada, por ejemplo. Por lo tanto, es importante asegurar al menos los componentes genuinos críticos que se permiten para una aeronave dada.

En general, cada componente tiene una correspondiente hoja de datos técnicos (posiblemente digital) que indica, por ejemplo, el nombre técnico del componente, el número de serie único del componente, el nombre del fabricante del componente, la fecha de fabricación del componente e información de certificación. Además, para una aeronave dada, un correspondiente registro contiene todas las hojas de datos técnicos (digitales) de sus respectivos componentes. Sin embargo, los componentes falsificados pueden tener su correspondiente hoja de datos técnicos digital falsa y, por lo tanto, no es obvio (a no ser mediante la realización de pruebas técnicas, por ejemplo) detectar el fraude. Por ejemplo, ¿cómo estar seguros de que una hoja de datos técnicos digital corresponde correctamente a un componente montado en una aeronave específica (y viceversa)?

De acuerdo con una realización ilustrativa de la invención, las partes permitidas a usar para fabricación o reparación una aeronave dada, o que se montan en la aeronave, se consideran que pertenece a un lote de "componentes" (u "objetos") para esa misma aeronave.

En la realización ilustrativa específica mostrada en la Figura 3, cada componente de un lote de aeronave, es decir, cada componente de aeronave permitido para montar o reparar en una aeronave dada, tiene un correspondiente documento de identificación digital de componente de aeronave AC-ID que contiene los mismos datos digitales de componente como en una hoja de datos técnicos convencional (por ejemplo, el código de ID de aeronave, el nombre del fabricante de la aeronave, el nombre técnico del componente, el número de serie único del componente, el nombre del fabricante del componente, y la fecha de fabricación del componente) junto con datos digitales adicionales correspondientes, al código ID de aeronave, el nombre del fabricante de la aeronave, la fecha de ensamblaje del componente en la aeronave, el nombre del técnico a cargo de realizar la comprobación de conformidad junto con la fecha de la comprobación de conformidad, y la correspondiente firma digital (única) del verificador. Además, cada documento de identificación digital de componente de aeronave AC-ID se asegura por medio de una marca de seguridad digital legible por máquina añadida al mismo. Por razones de claridad, los datos digitales de AC-ID:A_{125} se representan en la Figura3 como información textual y alfanumérica equivalente (es decir, legible por humanos), y la marca de seguridad digital 310 se muestra como un patrón bidimensional de código QR convencional equivalente.

Preferentemente, cada vez que un componente o un conjunto de componentes se sustituyen en la aeronave, se crean correspondientes documentos digitales seguros AC-ID y también se crea una correspondiente versión actualizada del lote de aeronave, con los correspondientes datos digitales adicionales anteriormente mencionados (relacionados con las nuevas operaciones de montaje).

Por lo tanto, todos los componentes montados (críticos) en una aeronave específica (en este punto, teniendo la referencia de ID de aeronave HB-SNO), pertenecen a un correspondiente lote de componentes montados (en este punto, que tiene un total de µ componentes) y se documentan en un correspondiente lote de µ archivos digitales asociados, es decir, el documento de identificación digital AC-ID. Una marca de seguridad digital 310 (en este punto en forma de un código QR) se incluye en cada documento de identificación digital de componente de aeronave, por ejemplo AC-ID:A_{125}, que se asocia con el correspondiente componente de aeronave, en este punto A_{125}, montado en la aeronave HB-SNO. La Figura 3 particularmente muestra el componente A_{125} del lote de aeronave que es una pala de turbina adaptada para el tipo de reactor montado

en la aeronave HB-SNO y marcado con un número de serie de fabricación único (en este punto, 12781, generalmente grabado por el fabricante). Los datos digitales de componente D_{125} en la marca de seguridad digital 310 del documento de identificación digital de componente de aeronave AC-ID:A_{125} asociados con el componente A_{125} comprenden los datos digitales que corresponden a los de la hoja de datos técnicos: el código de ID de aeronave 330a (en este punto, HB-SNO), el nombre del fabricante de la aeronave 330b (en este punto, AeroABC), el nombre técnico del componente 330c (en este punto, pala de turbina – 1er anillo), el número de serie de componente 330d (en este punto, 12781), el nombre del fabricante del componente 330e (en este punto, PCX), la fecha de fabricación del componente 330f (en este punto, 13 de noviembre de 2017), la fecha de ensamblaje del componente en el reactor 330g (en este punto, 24 de febrero de 2018), el nombre del técnico a cargo de realizar la comprobación de conformidad 330h (en este punto, el verificador es Martin White) junto con la fecha de la comprobación de conformidad 330i (en este punto, 20 de marzo de 2018), y la firma digital (única) del verificador 330j (en este punto, 2w9s02u).

Una firma digital de componente x_{125} de los datos digitales de componente D_{125} del archivo digital AC-ID:A_{125} del componente A_{125} se calcula por medio de una función de troceo unidireccional H como $x_{125} = H(D_{125})$. De la misma forma, todas las firmas digitales de componente x_i de los datos digitales de componente D_i de componente A_i se calculan por medio de la función de troceo unidireccional H como $x_i = H(D_i)$ (en este punto, $i = 1,\ldots,\mu$). De acuerdo con la invención, un árbol asociado con el lote de componentes $A_1,\ldots,A_\mu$ (en este punto, un árbol binario) y, por lo tanto, con el correspondiente lote de archivos digitales AC-ID:$A_1,\ldots$,AC-ID:A_μ, se construye teniendo μ nodos hoja $a(1,1),\ldots,a(1,\mu)$ que corresponden respectivamente a las μ firmas digitales de componente $x_1,\ldots,x_\mu$ de respectivos datos digitales de componente $D_1,\ldots,D_\mu$ de los documentos de identificación digital de componente AC-ID:$A_1,\ldots$,AC-ID:A_μ de componentes $A_1,\ldots,A_\mu$. En este punto, el orden de nodos del árbol binario es el orden convencional, es decir, los nodos a(i,j) se disponen de acuerdo con los valores de los índices (i,j): índice i indica el nivel en el árbol, comenzando desde el nivel de nodos hoja (i=1) hasta el penúltimo nivel de nodos por debajo del nodo raíz, e índice j que va desde 1 a μ para el nivel de nodos hoja (nivel 1), desde 1 a $\mu/2$ para los siguiente nodos nivel (no hoja) (nivel 2), etc. y desde 1 a 2 para el penúltimo nivel de nodos. Comprendiendo el árbol niveles de nodo a partir de los nodos hoja al nodo raíz, correspondiendo cada nodo no hoja del árbol a una firma digital por medio de la función unidireccional H de una concatenación de las respectivas firmas digitales de sus nodos hijo de acuerdo con el orden de concatenación de árbol.

Una firma digital raíz de referencia R para el lote de μ componentes de aeronave $A_1,\ldots A_\mu$ se calcula por medio de una función unidireccional de una concatenación (convencional) de valores de nodo del árbol (como se explica a continuación). La firma digital raíz de referencia R se almacena, a continuación, en una base de datos consultable (preferentemente una cadena de bloques) accesible por técnicos a cargo de controlar o cambiar los componentes montados. El árbol, por lo tanto, comprende niveles de nodo a partir de los nodos hoja al nodo raíz del árbol, correspondiendo cada nodo no hoja del árbol a una firma digital por medio de la función unidireccional H de una concatenación de las respectivas firmas digitales de sus (dos) nodos hijo de acuerdo con el orden de concatenación de árbol (en este punto convencional), correspondiendo el nodo raíz a la firma digital raíz de referencia R, es decir, la firma digital por medio de la función unidireccional H de una concatenación de las firmas digitales de los nodos del penúltimo nivel de nodos en el árbol (de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol).

Para un componente A_i dado del lote, una clave de verificación digital k_i, que corresponde a la firma digital de componente x_i (es decir, nodo hoja a(1,i)) de los datos digitales de componente D_i, se calcula como la secuencia de las respectivas firmas digitales, desde el nivel de nodos hoja hasta el penúltimo nivel de nodos del árbol, de cada otro nodo hoja que tiene el mismo nodo padre en el árbol que el nodo hoja a(1,i) que corresponde a la firma digital x_i, y sucesivamente en cada siguiente nivel en el árbol, de cada nodo no hoja que tiene el mismo nodo padre en el árbol que el mismo nodo padre anterior considerado en el nivel anterior. Para cada componente A_i montado en la aeronave HB-SNO, los datos asociados digitales de componente D_i y la correspondiente clave de verificación digital k_i se embeben en la marca de seguridad digital 310 incluida en el correspondiente documento de identificación digital de componente de aeronave AC-ID:A_i.

Por ejemplo, en caso de una operación de control de un componente en la aeronave HB-SNO, un técnico puede enviar una petición a la base de datos consultable que contiene el número de serie de componente 12781 leído en el archivo digital AC-ID:A_{125} del componente A_{125} a controlar, o su clave de verificación digital k_{125} como se lee en la marca de seguridad digital 310 en el correspondiente documento AC-ID:A_{125} con un lector apropiado, como por ejemplo un ordenador programado para decodificar el contenido de la marca de seguridad digital, y recibirá de vuelta el correspondiente valor de lote R. En una variante preferida que permite una comprobación fuera de línea completa, el ordenador del técnico tiene una memoria que almacena todas las firmas digitales raíz relacionadas con las aeronaves a controlar. En esta última versión, el técnico puede comprobar, a continuación, si el componente es genuino leyendo los datos digitales de componente D_{125} en la marca de seguridad digital 310 de AC-ID:A_{125}, comprobando que el número de serie único 330d (en este punto, 12781) extraído de D_{125} coincide con el número de serie marcado físicamente en el componente de aeronave A_{125} montado, calculando la correspondiente firma digital de componente x_{125} (por ejemplo, ejecutando una aplicación programada en una unidad de procesamiento CPU del ordenador que calcula la

firma $x_{125} = H(D_{125})$, a partir de los datos digitales D_{125} leídos), calculando un valor de lote candidato R^c a través de la función unidireccional H programada en la CPU del ordenador como el troceo de una concatenación del valor de nodo hoja $a(1,125)=x_{125}$ y los valores de nodo dados en la correspondiente clave de verificación digital k_{125}, y comprobando que el valor de lote candidato R^c coincide con una de las firmas digitales raíz de referencia almacenadas en la memoria del ordenador (es decir, el valor de referencia R, que corresponde a la aeronave HB-SNO). En caso de coincidencia completa (es decir, los números de serie coindicen y $R^c = R$), el componente A_{125} se considera como genuino y pertenece al lote de aeronave (actualizado) de componentes permitidos de la aeronave HB-SNO, si R^c no coincide con una firma digital raíz de referencia R almacenada, o si los números de serie no coinciden, el componente A_{125} es posiblemente falso, o es un componente genuino no permitido para la aeronave HB-SNO (por ejemplo, A_{125} no pertenece al lote correcto para esta aeronave), y debe cambiarse.

De una misma forma, la invención permitiría detectar fraude (o errores) de lotes de AC-ID asegurados de partes de sustitución almacenadas en un almacén verificando la autenticidad de las marcas en las partes almacenadas y comprobar que el número de serie de componente de la marca de seguridad digital coincide con el marcado en el correspondiente componente. En caso de un componente altamente crítico, una marca de seguridad basada en material prueba de manipulaciones puede aplicarse adicionalmente en el componente, mientras los datos digitales relacionados con la correspondiente característica física única de referencia, es decir, los datos digitales de característica CDD (por ejemplo, como se capturan por un sensor adecuado cuando se aplica la marca de seguridad basada en material) de esta marca se hace preferentemente parte de los datos digitales de componente D en la marca de seguridad digital del documento de identificación digital de componente de aeronave para este componente, y se calculan unos correspondientes datos de firma digital única UPS de referencia (por ejemplo, tomando un troceo de los datos digitales de característica CDD, es decir, UPS = H(CDD)) y también puede ser parte de los datos digitales de componente D. Este nivel adicional de seguridad mejora la seguridad proporcionada por el número de serie único marcado en el componente por su fabricante. Preferentemente, los UPC y UPS de referencia se almacenan en la cadena de bloques (para hacer los mismos inmutables) y son accesible por el técnico. Además, estos valores de referencia también pueden almacenarse adicionalmente en la memoria del ordenador del técnico para permitir autenticación fuera de línea de la marca de seguridad basada en material en el componente altamente crítico.

La operación de autenticación fuera de línea adicional de esta marca de seguridad basada en material puede comprender medir la característica física única en el componente, por medio de un sensor adecuado conectado al ordenador, y obtener unos datos digitales de característica candidatos CDD^c a partir de la característica medida (por ejemplo, a través de una aplicación específica programada en la CPU del ordenador). A continuación, el técnico (o la CPU de su ordenador, si se programa adecuadamente) compara los CDD^c obtenidos con la copia de los CDD de referencia almacenados en la memoria del ordenador: en el caso de una coincidencia "razonable" $CDD^c \approx CDD$ (es decir, dentro de algún criterio de tolerancia a error predefinido), la marca de seguridad basada en material y, por lo tanto, el componente se consideran como genuinos.

Como se ha mencionado anteriormente, una copia de los datos digitales de característica de referencia CDD, en lugar de almacenarse en la memoria del ordenador del técnico, es parte de los datos digitales D incluidos en la marca de seguridad digital en el documento de identificación digital de componente de aeronave AC-ID:A del componente A y puede obtenerse leyendo directamente en la marca de seguridad digital. El técnico puede leer, a continuación, los CDD^c candidatos en la marca de seguridad digital y comprobar que la firma UPS almacenada en la memoria del ordenador coincide con la firma candidata UPSc calculada a partir de los CDD^c candidatos leídos calculando $UPS^c = H(CDD^c)$: en caso de coincidencia $UPS^c = UPS$, la marca de seguridad basada en material y, por lo tanto, el componente, se confirman como genuinos.

En una variante de la realización, la comprobación de autenticidad de un componente por un técnico puede realizarse como alternativa a través de proceso en línea de una manera similar como ya se ha explicado con la primera realización detallada de la invención, y no se repetirá en este punto.

De acuerdo con la invención, es posible además verificar la autenticidad de una copia de un documento de identificación digital de componente de aeronave, AC-ID:A_{125} por ejemplo, con respecto al archivo digital asegurado original. De hecho, si un técnico a cargo de las operaciones de control (o reparación) tiene acceso al archivo digital AC-ID:A_{125} en su ordenador (que puede ser, por ejemplo, un teléfono inteligente adecuadamente programado), puede comprobar que los datos digitales de componente corresponden a los del documento original realizando las siguientes operaciones de:

- leer los datos digitales de componente D_{125} y la clave de verificación digital k_{125} en la marca de seguridad digital 310 del documento de identificación digital de componente AC-ID:A_{125};
- adquirir un valor de lote de referencia R del lote que corresponde al documento AC-ID:A_{125}; este valor de referencia puede estar ya en la memoria del ordenador o puede adquirirse a través de un enlace de comunicación desde una base de datos que almacena los valores de lote de referencia de documentos de

identificación digital de componente en el caso en el que el ordenador está equipado con una unidad de comunicación, enviando una petición que contiene, por ejemplo, el número de serie (único) de componente o solamente la clave k_{125} leída de la marca de seguridad digital 310, y recibiendo de vuelta el correspondiente valor de lote de referencia R;

- calcular (con la función unidireccional H programada) una firma digital de componente x_{125} a partir de los datos digitales de componente D_{125} leídos, con $x_{125} = H(D_{125})$;
- calcular un valor de lote candidato R^c (por medio de la función de troceo unidireccional programada H y firma digital de una concatenación de firmas digitales) como la firma digital mediante la función de troceo H de una concatenación del valor de nodo hoja x_{125} y los valores de nodo indicados en la clave de verificación digital k_{125} (de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol); y
- verificar que el valor de lote candidato R^c coincide con el valor de lote de referencia R.

De acuerdo con la anterior descripción detallada, la invención es claramente compatible con operaciones de comprobación fuera de línea y locales para verificar la autenticidad de un archivo digital asegurado, o conformidad de datos de una copia de un archivo digital asegurado, con respecto a los datos asociados con el archivo digital asegurado original. Sin embargo, la invención es también compatible con un proceso de verificación en línea, por ejemplo, recibiendo (a través de un enlace de comunicación) un valor de lote de referencia (o firma digital raíz) desde una fuente externa (por ejemplo, servidor o cadena de bloques), o realizando algunas o todas las etapas de cálculo que implican la función unidireccional o la concatenación de firmas digitales a través de medios informáticos externos (por ejemplo, operando en un servidor), o incluso realizando la verificación de que una firma digital raíz candidata coincide con una firma digital raíz de referencia (y solo recibir el resultado).

La materia objeto anteriormente divulgada se ha de considerar ilustrativa, y no restrictiva, y sirve para proporcionar una mejor comprensión de la invención definida por las reivindicaciones dependientes.

REIVINDICACIONES

1. Método de aseguramiento de un archivo digital original ($A_1,\ldots,A_8$) que pertenece a un lote de una pluralidad de archivos digitales originales ($A_1,\ldots,A_8$) contra falsificación o manipulación, incluyendo cada archivo digital original ($A_1,\ldots,A_8$) sus propios datos digitales ($D_1,\ldots,D_8$), que comprende las etapas de:

para cada archivo digital original ($A_1,\ldots,A_8$) del lote, calcular por medio de una función unidireccional (H) una firma de archivo digital asociada ($x_1,\ldots,x_8$) de sus datos digitales ($D_1,\ldots,D_8$);
formar un árbol basándose en la pluralidad de firmas de archivo digital calculadas ($x_1,\ldots,x_8$) para los archivos digitales originales ($A_1,\ldots,A_8$) del lote y que comprende nodos dispuestos de acuerdo con un orden de nodos dado en el árbol, comprendiendo dicho árbol niveles de nodo a partir de los nodos hoja, que corresponden a la pluralidad de firmas de archivo digital ($x_1,\ldots,x_8$) respectivamente asociadas a la pluralidad de archivos digitales originales ($A_1,\ldots,A_8$) en el lote, al nodo raíz del árbol, correspondiendo cada nodo no hoja del árbol a una firma digital por medio de la función unidireccional de una concatenación de las respectivas firmas digitales de sus nodos hijo de acuerdo con un orden de concatenación de árbol, correspondiendo el nodo raíz a una firma digital raíz de referencia (R), es decir, una firma digital por medio de la función unidireccional de una concatenación de las firmas digitales de los nodos de un penúltimo nivel de nodos en el árbol de acuerdo con dicho orden de concatenación de árbol;
asociar con el archivo digital original dado ($A_1,\ldots,A_8$) una correspondiente clave de verificación digital ($k_1,\ldots k_8$) que es una secuencia de las respectivas firmas digitales, desde el nivel de nodos hoja hasta el penúltimo nivel de nodos, de cada otro nodo hoja que tiene el mismo nodo padre en el árbol que el nodo hoja que corresponde a la firma de archivo digital ($x_1,\ldots,x_8$) del archivo digital original dado ($A_1,\ldots,A_8$), y sucesivamente en cada siguiente nivel en el árbol, de cada nodo no hoja que tiene el mismo nodo padre en el árbol que el mismo nodo padre anterior considerado en el nivel anterior;
poner a disposición de un usuario la firma digital raíz de referencia (R) del árbol; e caracterizado por que comprende
incluir en el archivo digital original ($A_1,\ldots,A_8$) una correspondiente marca de seguridad digital legible por máquina (110) que comprende una representación de sus datos digitales ($D_1,\ldots,D_8$) y su correspondiente clave de verificación digital ($k_1,\ldots k_8$),
obteniendo de este modo un archivo digital original marcado ($A_1,\ldots,A_8$) cuyos datos digitales ($D_1,\ldots,D_8$) se aseguran contra falsificación o manipulación.

2. Método de acuerdo con la reivindicación 1, en el que la firma digital raíz de referencia (R) del nodo raíz del árbol o bien se publica en un medio accesible por el usuario o bien se almacena en una base de datos raíz consultable accesible por el usuario, o en una cadena de bloques, o en una base de datos asegurada por una cadena de bloques, accesible por el usuario.

3. Método de acuerdo con la reivindicación 1 o la reivindicación 2, en el que

un archivo digital virtual se cuenta como que pertenece al lote de archivos digitales originales ($A_1,\ldots,A_8$), incluyendo dicho archivo digital virtual sus propios datos digitales virtuales, y una firma de archivo digital virtual asociada obtenida por medio de la función unidireccional (H) de los datos digitales virtuales, no siendo dicho archivo digital virtual real sino usado únicamente para generar la firma de archivo digital virtual asociada a partir de sus datos digitales virtuales; y
siendo la firma digital raíz de referencia (R) asociada con dicho lote de archivos digitales originales ($A_1,\ldots,A_8$) calculada a partir de un árbol que tiene todas las firmas de archivos digitales de los archivos digitales originales ($A_1,\ldots,A_8$) del lote, incluyendo la firma de archivo digital virtual, como nodos hoja.

4. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que
datos digitales adicionales que corresponden a los datos digitales ($D_1,\ldots,D_8$) asociados con el archivo digital original marcado ($A_1,\ldots,A_8$) se almacenan en una base de datos de información consultable accesible por el usuario a través de una interfaz de base de datos de información operable para recibir desde el usuario una petición de información que contiene datos digitales ($D_1,\ldots,D_8$), o una firma de archivo digital ($x_1,\ldots,x_8$), obtenidos a partir de una marca de seguridad digital (110) de un archivo digital original marcado ($A_1,\ldots,A_8$), y enviar de vuelta correspondientes datos digitales adicionales.

5. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que los datos digitales ($D_1,\ldots,D_8$) del archivo digital original marcado ($A_1,\ldots,A_8$) incluyen datos digitales de característica de referencia de una correspondiente característica física única de un objeto o individuo asociado.

6. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que los datos digitales ($D_1,\ldots,D_8$) de los respectivos archivos digitales originales ($A_1,\ldots,A_8$) del lote se distribuyen entre campos dados comunes a todos los archivos digitales del lote, y datos digitales específicos relacionados con estos campos no se incluyen en los datos digitales ($D_1,\ldots,D_8$), sino que se agrupan en un bloque de campos separados asociado con el lote, y en el que:

i) la firma de archivo digital ($x_1,\ldots,x_8$) de un archivo digital original ($A_1,\ldots,A_8$) se calcula con la función unidireccional de una concatenación de los correspondientes datos digitales ($D_1,\ldots,D_8$) y el bloque de datos de campos; y
ii) la firma digital raíz de referencia (R) se pone a disposición del usuario junto con el bloque de datos de campos asociado.

7. Método de verificación de la autenticidad de un archivo digital asegurado de acuerdo con el método de una cualquiera de las reivindicaciones 1 a 5, o la conformidad de una copia de tal archivo digital asegurado con respecto al original, caracterizado por que comprende las etapas de, tras procesar un archivo de prueba que es dicho archivo digital o dicha copia del archivo digital por medio de una unidad de procesamiento conectada a una memoria:

haber almacenado en la memoria el archivo de prueba;
leer una representación de datos digitales ($D_1,\ldots,D_8$) y de una clave de verificación digital ($k_1,\ldots,k_8$) en una marca de seguridad digital (110) del archivo de prueba almacenado, y extraer respectivamente correspondientes datos digitales de prueba y clave de verificación digital de prueba de dicha representación leída;
haber almacenado en la memoria una firma digital raíz de referencia (R) de un nodo raíz de un árbol del lote de archivos digitales originales ($A_1,\ldots,A_8$), y haber programado en la unidad de procesamiento la función unidireccional (H) para calcular una firma digital de datos digitales ($D_1,\ldots,D_8$) y de una concatenación de firmas digitales de acuerdo con el orden de nodos en el árbol y el orden de concatenación de árbol;
verificar si los datos digitales de prueba extraídos y la clave de verificación digital de prueba asociada corresponden, de hecho, a la firma digital raíz de referencia almacenada (R) realizando las etapas de:

calcular con la función unidireccional una firma digital de prueba de los datos digitales de prueba extraídos, correspondiendo dicha firma digital de prueba a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital (110) del archivo de prueba;
extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo hoja del árbol de prueba que tiene el mismo nodo padre que el del nodo hoja de prueba y calcular una firma digital de una concatenación de la firma digital de prueba y la firma digital extraída de dicho cada otro nodo hoja, obteniendo por lo tanto una firma digital de dicho mismo nodo padre del nodo hoja de prueba;
sucesivamente en cada siguiente nivel en el árbol de prueba y hasta el penúltimo nivel de nodos, extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo no hoja del árbol de prueba que tiene el mismo nodo padre que el del mismo nodo padre anterior considerado en la etapa anterior y calcular una firma digital de una concatenación de la firma digital de dicho cada respectivo otro nodo no hoja y la firma digital obtenida de dicho mismo nodo padre anterior, obteniendo por lo tanto una firma digital de dicho mismo nodo padre de dicho mismo nodo padre anterior;
calcular una firma digital de una concatenación de las firmas digitales obtenidas de los nodos no hoja que corresponden al penúltimo nivel de nodos del árbol de prueba, obteniendo por lo tanto una firma digital raíz candidata del nodo raíz del árbol de prueba; y
comprobar si la firma digital raíz candidata obtenida coincide con la firma digital raíz de referencia almacenada (R),
con lo que, en el caso en el que dichas firmas digitales raíz coinciden, los datos digitales ($D_1,\ldots,D_8$) del archivo de prueba son los de un archivo digital genuino.

8. Método de acuerdo con la reivindicación 7, en el que el archivo digital original marcado ($A_1,\ldots,A_8$) se asegura de acuerdo con el método de la reivindicación 6, almacenando adicionalmente la memoria de la unidad de procesamiento el bloque de datos de campos asociado, y en el que:
la etapa de calcular una firma digital de prueba que corresponde a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital (110) en el archivo de prueba comprende calcular con la función unidireccional una firma digital de una concatenación de los datos digitales de prueba extraídos y el bloque de datos de campos almacenado.

9. Método de acuerdo con una cualquiera de las reivindicaciones 7 y 8, en el que el archivo digital se asegura almacenando la firma digital raíz de referencia (R) en una base de datos raíz consultable accesible por el usuario de acuerdo con el método de la reivindicación 2, y la unidad de procesamiento se conecta adicionalmente a una unidad de comunicación operable para enviar y recibir de vuelta datos a través de un enlace de comunicación, que comprende las etapas preliminares de:

enviar con la unidad de comunicación a través del enlace de comunicación una petición a dicha base de datos raíz, y recibir de vuelta la firma digital raíz de referencia (R); y
almacenar la firma digital raíz recibida en la memoria de la memoria.

10. Método de acuerdo con una cualquiera de las reivindicaciones 7 a 9, en el que el archivo digital se asegura de acuerdo con el método de la reivindicación 4 y el formador de imágenes está equipado

adicionalmente con medios de comunicación operables para enviar a la interfaz de base de datos de información una petición de información que contiene datos digitales ($D_1,\ldots,D_8$), o una firma de archivo digital ($x_1,\ldots,x_8$), obtenidos a partir de la marca de seguridad digital (110) del archivo de prueba, y recibir de vuelta correspondientes datos digitales adicionales.

11. Método de acuerdo con una cualquiera de las reivindicaciones 7 a 10, en el que el formador de imágenes está equipado adicionalmente con un sensor operable para detectar una característica física única de respectivamente un objeto o individuo asociado, y la unidad de procesamiento se programa para extraer correspondientes datos digitales de característica de una señal de detección recibida desde el sensor, habiendo almacenado el formador de imágenes en la memoria datos digitales de característica de referencia CDD que corresponden a dicha característica física única de respectivamente el objeto o individuo asociado, que comprende las etapas adicionales de, tras visualizar un sujeto que es dicho objeto o individuo asociado:

detectar con el sensor una característica física única del sujeto y extraer correspondientes datos digitales de característica candidatos CDD^c;
comparar los datos digitales de característica candidatos CDD^c obtenidos con los datos digitales de característica de referencia CDD almacenados; y
en el caso en el que los datos digitales de característica candidatos CDD^c son similares a los datos digitales de característica de referencia CDD almacenados, dentro de un criterio de tolerancia dado, el sujeto se considera que corresponde respectivamente a un objeto o individuo genuino asociado de forma válida con un archivo digital genuino.

12. Archivo digital que pertenece a un lote de una pluralidad de archivos digitales originales ($A_1,\ldots,A_8$) y asegurado de acuerdo con el método de una cualquiera de las reivindicaciones 1 a 6, teniendo cada archivo digital original ($A_1,\ldots,A_8$) del lote sus propios datos digitales ($D_1,\ldots,D_8$) y correspondiente clave de verificación digital ($k_1,\ldots,k_8$), teniendo dicho lote una correspondiente firma digital raíz de referencia (R), que comprende:
una marca de seguridad legible por máquina que incluye una representación de sus datos digitales ($D_1,\ldots,D_8$) y su clave de verificación.

13. Sistema de verificación de la autenticidad de un archivo digital, o la conformidad de una copia de tal archivo digital, con respecto a un archivo digital original marcado ($A_1,\ldots,A_8$) que pertenece a un lote de archivos digitales originales ($A_1,\ldots,A_8$) asegurados de acuerdo con el método de una cualquiera de las reivindicaciones 1 a 5, que comprende un formador de imágenes que tiene una unidad de formación de imágenes, una unidad de procesamiento con una memoria y una unidad de procesamiento de imágenes, almacenando la memoria una firma digital raíz de referencia (R) de un árbol que corresponde al lote de archivos digitales originales ($A_1,\ldots,A_8$), y programándose en la unidad de procesamiento la función unidireccional (H) para calcular una firma digital de datos digitales ($D_1,\ldots,D_8$) y de una concatenación de firmas digitales de acuerdo con el orden de nodos del árbol y el orden de concatenación de árbol, siendo dicho sistema operable para:

tener almacenado en la memoria un archivo de prueba que es dicho archivo digital o dicha copia del archivo digital;
leer una representación de datos digitales ($D_1,\ldots,D_8$) y de una clave de verificación digital ($k_1,\ldots,k_8$) en una marca de seguridad digital (110) del archivo de prueba almacenado, y extraer respectivamente correspondientes datos digitales de prueba y clave de verificación digital de prueba de dicha representación leída;
verificar si los datos digitales de prueba extraídos y la clave de verificación digital de prueba corresponden, de hecho, a la firma digital raíz de referencia almacenada (R) realizando en la unidad de procesamiento las operaciones programadas de:

calcular con la función unidireccional una firma digital de prueba de los datos digitales de prueba extraídos, correspondiendo dicha firma digital de prueba a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital (110) del archivo de prueba;
extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo hoja del árbol de prueba que tiene el mismo nodo padre que el del nodo hoja de prueba y calcular una firma digital de una concatenación de la firma digital de prueba y la firma digital extraída de dicho cada otro nodo hoja, obteniendo por lo tanto una firma digital de dicho mismo nodo padre del nodo hoja de prueba;
sucesivamente en cada siguiente nivel en el árbol de prueba y hasta el penúltimo nivel de nodos, extraer de la secuencia de firmas digitales en la clave de verificación digital de prueba, una firma digital de cada otro nodo no hoja del árbol de prueba que tiene el mismo nodo padre que el del mismo nodo padre anterior considerado en la etapa anterior y calcular una firma digital de una concatenación de la firma digital de dicho cada respectivo otro nodo no hoja y la firma digital obtenida de dicho mismo nodo padre anterior, obteniendo por lo tanto una firma digital de dicho mismo nodo padre de dicho mismo nodo padre anterior;
calcular una firma digital de una concatenación de las firmas digitales obtenidas de los nodos no hoja que corresponden al penúltimo nivel de nodos del árbol de prueba, obteniendo por lo tanto una firma digital raíz

candidata del nodo raíz del árbol de prueba; y
comprobar si la firma digital raíz candidata obtenida coincide con la firma digital raíz de referencia almacenada (R),
con lo que, en el caso en el que dichas firmas digitales raíz coinciden, el sistema está configurado para entregar una indicación de que los datos digitales del archivo de prueba son los de un archivo digital genuino.

14. Sistema de acuerdo con la reivindicación 13, en el que el archivo digital original marcado ($A_1,\ldots,A_8$) se asegura de acuerdo con el método de la reivindicación 6, almacenando adicionalmente la memoria de la unidad de procesamiento el bloque de datos de campos asociado, y en el que:
las operaciones programadas de calcular una firma digital de prueba que corresponde a un nodo hoja de prueba en un árbol de prueba que corresponde a la marca de seguridad digital (110) del archivo de prueba comprenden calcular con la función unidireccional una firma digital de una concatenación de los datos digitales de prueba extraídos y el bloque de datos de campos almacenado.

15. Sistema de acuerdo con una cualquiera de las reivindicaciones 13 y 14, en el que el archivo digital original marcado ($A_1,\ldots,A_8$) pertenece a un lote de archivos digitales originales ($A_1,\ldots,A_8$) asegurados de acuerdo con el método de la reivindicacione 5, estando el sistema equipado adicionalmente con un sensor conectado a la unidad de procesamiento y operable para detectar una característica física única de un objeto o individuo asociado, y programándose la unidad de procesamiento para extraer correspondientes datos digitales de característica de una señal de detección recibida desde el sensor, habiendo almacenado el sistema en la memoria datos digitales de característica de referencia CDD que corresponden a dicha característica física única del objeto o individuo asociado, siendo el sistema operable adicionalmente para:

detectar con el sensor una característica física única de un sujeto que es dicho objeto o individuo asociado, y extraer correspondientes datos digitales de característica candidatos CDD^c;
comparar los datos digitales de característica candidatos CDD^c obtenidos con los datos digitales de característica de referencia CDD almacenados; y
en el caso en el que los datos digitales de característica candidatos CDD^c son similares a los datos digitales de característica de referencia CDD almacenados, dentro de un criterio de tolerancia dado, entregar una indicación de que el sujeto se considera como genuino.

DIBUJOS

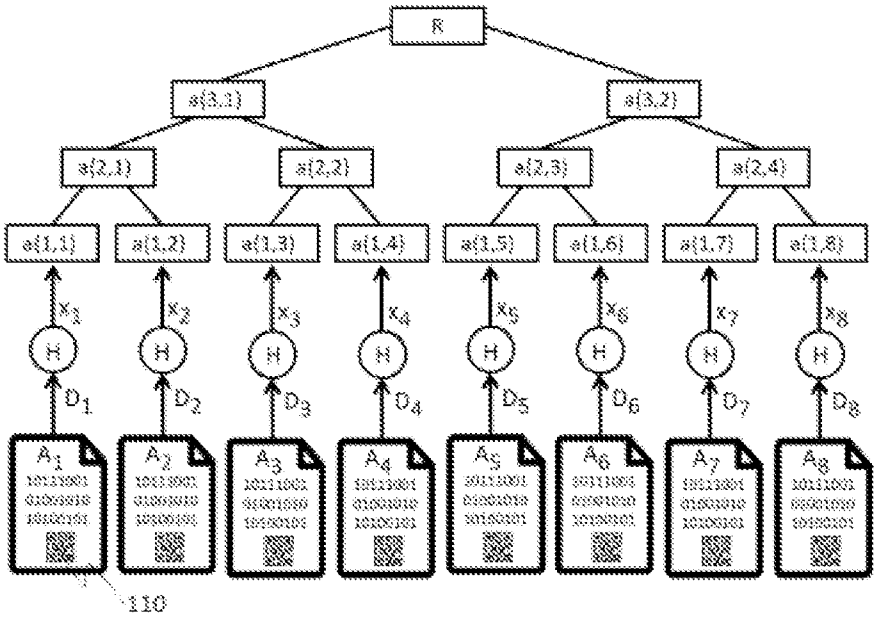

Fig.1

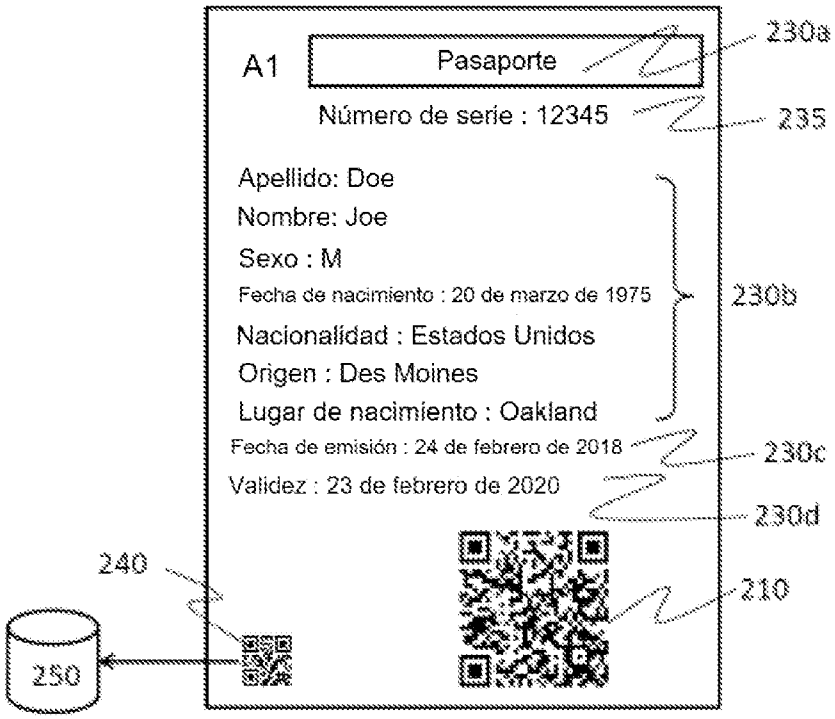
A1
Pasaporte
230a
Número de serie : 12345
235
Apellido: Doe
Nombre: Joe
Sexo : M
Fecha de nacimiento : 20 de marzo de 1975
Nacionalidad : Estados Unidos
Origen : Des Moines
Lugar de nacimiento : Oakland
230b
Fecha de emisión : 24 de febrero de 2018
230c
Validez : 23 de febrero de 2020
230d
240
210
250

Fig.2A

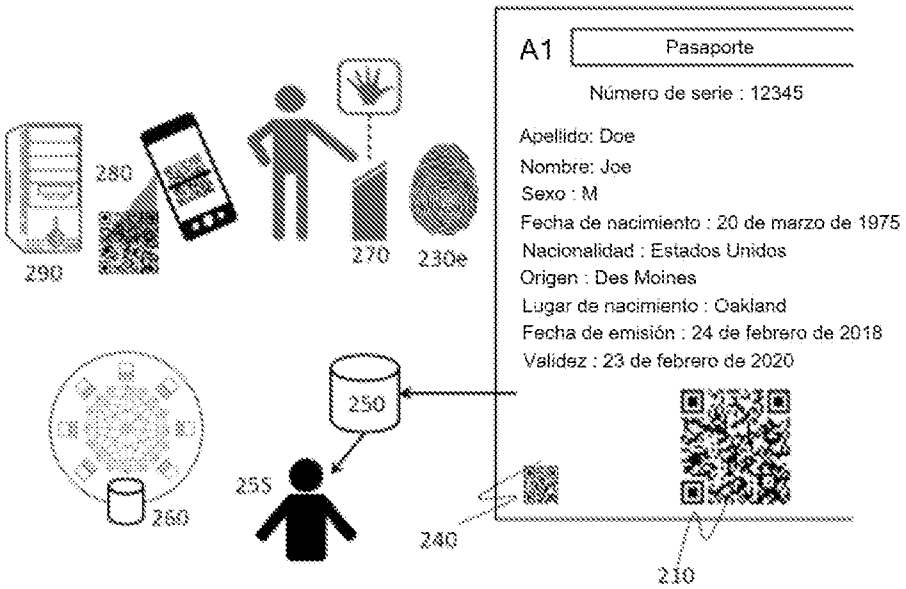
A1
Pasaporte
Número de serie : 12345
Apellido: Doe
Nombre: Joe
Sexo : M
Fecha de nacimiento : 20 de marzo de 1975
Nacionalidad : Estados Unidos
Origen : Des Moines
Lugar de nacimiento : Oakland
Fecha de emisión : 24 de febrero de 2018
Validez : 23 de febrero de 2020
280
290
270
230e
250
255
260
240
210

Fig.2B

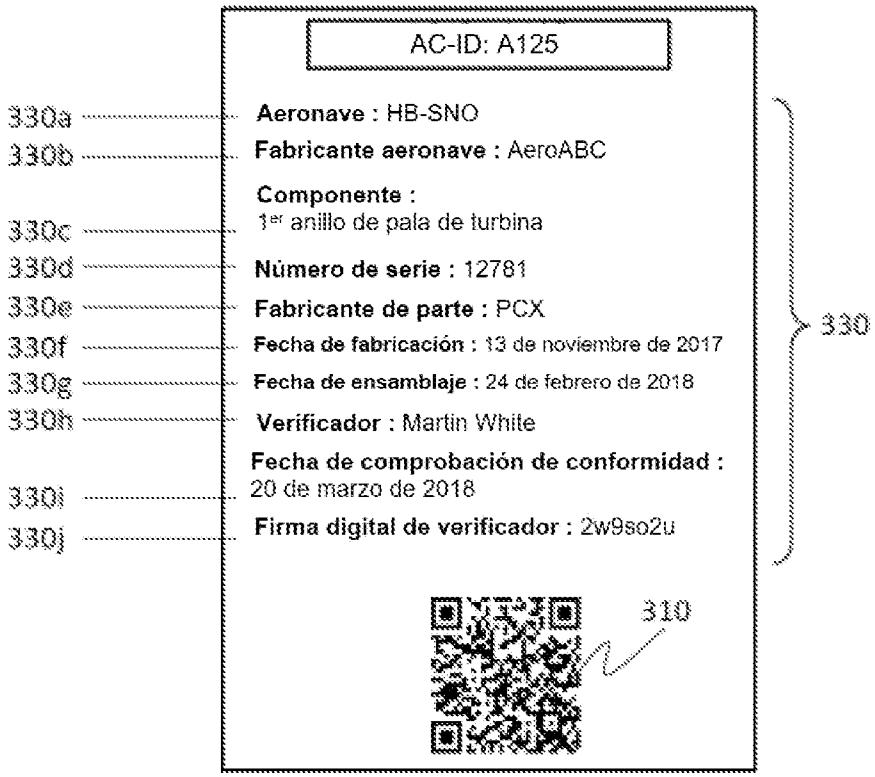
AC-ID: A125
330a
Aeronave : HB-SNO
330b
Fabricante aeronave : AeroABC
Componente :
330c
1er anillo de pala de turbina
330d
Número de serie : 12781
330e
Fabricante de parte : PCX
330f
Fecha de fabricación : 13 de noviembre de 2017
330g
Fecha de ensamblaje : 24 de febrero de 2018
330h
Verificador : Martin White
Fecha de comprobación de conformidad :
330i
20 de marzo de 2018
330j
Firma digital de verificador : 2w9so2u
330
310

Fig.3