

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 004 667**

51 Int. Cl.:

G07D 7/00 (2006.01)

G07D 7/12 (2006.01)

G07D 7/20 (2006.01)

G07D 7/0043 (2006.01)

G07D 7/0047 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **28.05.2020** **PCT/EP2020/064812**

87 Fecha y número de publicación internacional: **10.12.2020** **WO20245024**

96 Fecha de presentación y número de la solicitud europea: **28.05.2020** **E 20727673 (4)**

97 Fecha y número de publicación de la concesión europea: **30.10.2024** **EP 3977422**

54 Título: **Documento de texto certificado**

30 Prioridad:

03.06.2019 EP 19177919

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2025

73 Titular/es:

SICPA HOLDING SA (100.00%)

Avenue de Florissant 41

1008 Prilly, CH

72 Inventor/es:

DECOUX, ERIC

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 3 004 667 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Documento de texto certificado

5 CAMPO TÉCNICO

La presente invención se refiere al campo técnico de los métodos y sistemas antifraude y de seguridad. En particular, la invención se refiere a la protección de datos frente a falsificación o manipulación indebida, como, por ejemplo, datos de texto de un documento de valor (digitalizado o impreso).

10

ANTECEDENTES DE LA INVENCION

Los problemas de falsificación y manipulación indebida de archivos digitales o documentos impresos son bien conocidos, son graves y van en aumento. El ejemplo de falsificación de datos marcados en un documento original (digital o material) tal como un documento de identidad o a diploma es bien conocido, y la preocupación es incluso mayor si se considera una copia digital del documento digital/material 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.

20

Hay muchas técnicas conocidas para proteger un contenido de un documento físico o digital frente a falsificación. Por ejemplo, al tomar un troceo de datos digitales de un documento digital original, o de una versión digitalizada de un documento físico original (por ejemplo, al explorar el documento y extraer datos de texto por medio de un software de escáner de OCR), y almacenar el valor de troceo en un libro mayor (por ejemplo, una mera base de datos o una cadena de bloques). Entonces, al explorar un contenido de datos de un documento bajo escrutinio como se representa visualmente en un soporte físico (por ejemplo, el soporte puede ser una hoja de papel en la que se imprimen datos) y calcular un valor de troceo de dicho contenido de datos, y comparar entonces el valor de troceo calculado con el valor de troceo almacenado en el libro mayor correspondiendo a un documento original, se puede detectar un cambio en el contenido de datos. Sin embargo, un inconveniente de este método es que, debido a una cierta alteración de la representación visual en el soporte del contenido del documento, incluso si este documento es genuino, el valor de troceo calculado puede diferir del valor de troceo almacenado. Esta diferencia se puede deber, asimismo, a la forma en la que se realiza la operación de exploración, o incluso depender del tipo de escáner usado (dos escáneres diferentes pueden dar dos conclusiones opuestas). Esto también es cierto para un documento digital como se visualiza en un soporte como una pantalla (de un ordenador, por ejemplo): incluso si el contenido del documento es genuino, cualquier alteración en el contenido visualizado generará, cuando se explora el contenido visualizado para su verificación, un valor de troceo que difiere del valor de troceo almacenado. Por lo tanto, en la práctica, explorar un documento y calcular un valor de troceo de la imagen de captura no funciona debido a que, cada vez que se explora un documento, en general, se obtiene como resultado un troceo diferente. El uso de un escáner de OCR ("Reconocimiento Óptico de Caracteres") antes de computar un valor de troceo no soluciona la cuestión anterior, debido a que no hay sistema de OCR alguno que presente un desempeño del 100 %: por ejemplo, si solo un punto se vuelve una coma, o una letra "l" (es decir, L) se vuelve un "1" (es decir, uno), el troceo computado será diferente.

25

30

35

40

45

50

55

Algunas técnicas existentes para proteger documentos de papel (por ejemplo, certificados, diplomas, contratos...) con solo una poca información extraída del documento implican crear un código de barras en 2D (por ejemplo, un código QR), poner la información extraída dentro del código de barras en 2D e imprimir el mismo en el documento. Cada vez que se lee el código de barras en 2D se obtiene el mismo resultado, pero con el inconveniente de que la información incluida en el código de barras se ha de comparar con la información impresa en el documento. Además, en el caso en el que se desea proteger, por ejemplo, una página de texto completa, es necesario colocar el texto completo en el código de barras y, por lo tanto, el código de barras se vuelve de un tamaño enorme y requiere mucho espacio en la página, lo que es percibido como molesto por un lector (de tal modo que, en la práctica, el texto completo que se puede codificar tiene un tamaño limitado), y se vuelve necesario (y tedioso) comparar varios miles de caracteres entre el texto impreso y el texto descodificado a partir del código de barras.

Se sabe que los documentos US 6047093 A, EP 2048867 y US 2004/145661 describen la determinación de errores en el texto impreso en el documento y la formación de información en el mismo.

60 SUMARIO DE LA INVENCION

La invención tiene por objeto resolver los inconvenientes anteriormente mencionados de la técnica anterior con respecto a la falsificación y manipulación indebida de archivos digitales o documentos impresos, al permitir una detección automática de cualquier modificación en una disposición de símbolos gráficos (por ejemplo, un texto) marcados (respectivamente, visualizados) con respecto a una disposición original y, en particular, eliminar la redundancia entre los datos dentro de un código y un texto impreso (respectivamente,

65

visualizado), evitando la carga de comparar visualmente un texto dentro de un código con un texto impreso (respectivamente, visualizado), al tiempo que se resuelve el problema del tamaño demasiado grande del código cuando el tamaño de los datos para el texto impreso (respectivamente, visualizado) es grande. El alcance de la invención está definido por las reivindicaciones adjuntas.

5

Por lo tanto, la presente invención tiene por objeto proporcionar un método fiable y robusto para producir en un soporte material, como un visualizador (por ejemplo, una pantalla de un ordenador) o un sustrato (por ejemplo, una hoja de papel, una etiqueta, un envasado), símbolos gráficos visibles (por ejemplo, caracteres de texto o glifos) cuya conformidad con símbolos gráficos de referencia auténticos puede ser comprobada fácilmente por un usuario que lee dichos símbolos gráficos visibles y que evita los inconvenientes de la técnica anterior. Los símbolos gráficos son legibles por seres humanos y se toman de un conjunto finito dado de símbolos gráficos (por ejemplo, como caracteres de texto de un alfabeto). Los símbolos gráficos legibles por seres humanos, como se visualizan o se marcan en el sustrato de acuerdo con la invención, son, por lo tanto, verificables por el usuario y se puede detectar cualquier intento de modificar cualquier parte de los símbolos gráficos.

10

15

Por lo tanto, la invención se refiere a un "método de marcado", es decir, un método de generación, en un soporte, de datos gráficos verificables de acuerdo con la reivindicación 1 mediante el uso de un conjunto finito dado de símbolos gráficos, siendo el soporte un visualizador o un sustrato, que comprende las etapas de:

20

- almacenar, en una memoria de una unidad de procesamiento, un bloque de datos gráficos que contiene una representación digital de símbolos gráficos;
- procesar, con la unidad de procesamiento, la representación digital de símbolos gráficos del bloque de datos gráficos almacenado con un código de corrección de errores programado en la unidad de procesamiento para generar datos de corrección de errores en un bloque de datos de corrección de errores correspondiente;
- formatear el bloque de datos gráficos y el bloque de datos de corrección de errores con la unidad de procesamiento para proporcionar respectivamente, en un bloque de datos gráficos legibles por seres humanos, una representación legible por seres humanos de los símbolos gráficos del bloque de datos gráficos y, en un bloque de datos de corrección de errores legibles por máquina, una representación legible por máquina de los datos de corrección de errores del bloque de datos de corrección de errores separada de la representación legible por seres humanos de los símbolos gráficos del bloque de datos gráficos, para obtener un bloque de datos gráficos verificables correspondiente que comprende dicho bloque de datos gráficos legibles por seres humanos y dicho bloque de datos de corrección de errores legibles por máquina; y

25

30

- (i) visualizar símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores del bloque de datos gráficos verificables obtenido en el visualizador conectado a la unidad de procesamiento, o
- (ii) marcar en el sustrato, por medio de un dispositivo de marcado conectado a la unidad de procesamiento y equipado con una unidad de control accionable para controlar la operación de marcar basándose en datos recibidos de la unidad de procesamiento, símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores del bloque de datos gráficos verificables recibido de la unidad de procesamiento,

35

40

proporcionando de este modo, en el soporte, unos símbolos gráficos legibles por seres humanos junto con unos datos de corrección de errores legibles por máquina correspondientes que son verificables por un usuario.

45

La representación legible por máquina de los datos de corrección de errores puede ser una cualquiera de una representación alfanumérica o una representación de código de barras (código de barras en 1D o código de barras en 2D como, por ejemplo, un código de Matriz de Datos o un código QR). Preferiblemente, el código de barras puede ser un código de barras lineal PDF417 convencional, que puede ser leído por un escáner lineal simple arrastrado por encima del código de barras. Preferiblemente, los símbolos gráficos pueden ser caracteres de texto y el conjunto finito de símbolos gráficos puede ser un alfabeto. Preferiblemente, el dispositivo de marcado puede ser una impresora (por ejemplo, una impresora de inyección de tinta) y el sustrato puede ser una hoja de papel o una etiqueta. Asimismo, preferiblemente, el código de corrección de errores puede ser un código de corrección de errores de Reed-Solomon.

50

55

El método comprende las etapas adicionales de:

- calcular, con una función de troceo programada en la unidad de procesamiento, un valor de troceo de cualquier porción de un bloque de datos que resulta de una concatenación del bloque de datos gráficos y el bloque de datos de corrección de errores; y
- almacenar el valor de troceo calculado como un valor de troceo de referencia en un libro mayor.

60

La función de troceo es un ejemplo bien conocido de una función unidireccional, es decir, una función fácil de computar pero difícil de invertir (véase, por ejemplo, S. Goldwasser y M. Bellare "*Lecture Notes on*

65

Cryptography", MIT, julio de 2008, <http://www-cse.ucsd.edu/users/mihir>). Preferiblemente, la función de troceo criptográfico puede ser de la familia de SHA-2, como el SHA-256, por ejemplo, dando unos valores de troceo de un tamaño de 256 bits: esta función es prácticamente irreversible y resistente a colisiones, es decir, la probabilidad de que dos entradas diferentes conduzcan a la misma salida es despreciable. Asimismo, preferiblemente, el libro mayor puede ser una cadena de bloques, que proporciona de forma ventajosa un registro inmutable de datos. Opcionalmente, puede haber una etapa adicional de firmar el valor de troceo de referencia calculado con una clave privada de firma, por medio de la unidad de procesamiento, para obtener un valor de troceo de referencia firmado correspondiente, y almacenar, o proporcionar adicionalmente en el soporte, el valor de troceo de referencia firmado. Con esta opción, un usuario que tiene una clave pública correspondiendo a la clave privada puede comprobar que un valor de troceo de referencia firmado leído en el soporte es genuino como que está firmado con la clave privada correcta.

En una segunda variante del método de marcado anterior, el soporte comprende una pluralidad de partes y el bloque de datos gráficos verificables se divide en una misma pluralidad de sub-bloques de datos gráficos verificables, y los símbolos gráficos legibles por seres humanos y la representación legible por máquina de datos de corrección de errores correspondientes se diseminan, en consecuencia, de forma conjunta en partes correspondientes del soporte, mediante las etapas siguientes:

- el bloque de datos gráficos se divide en una pluralidad de sub-bloques de datos gráficos, y cada sub-bloque de datos gráficos se formatea para proporcionar una representación legible por seres humanos de sus símbolos gráficos en un sub-bloque de datos gráficos legibles por seres humanos correspondiente;
 - para cada sub-bloque de datos gráficos, la representación digital de sus símbolos gráficos se extrae y se procesa con el código de corrección de errores para generar datos de corrección de errores correspondientes en un sub-bloque de datos de corrección de errores;
 - cada sub-bloque de datos de corrección de errores se formatea para proporcionar, en un sub-bloque de datos de corrección de errores legibles por máquina correspondiente, una representación legible por máquina de datos de corrección de errores correspondientes separada de la representación legible por seres humanos de símbolos gráficos del sub-bloque de datos gráficos legibles por seres humanos correspondiente, para obtener un sub-bloque de datos gráficos verificables correspondiente que comprende dicho sub-bloque de datos gráficos legibles por seres humanos y dicho sub-bloque de datos de corrección de errores legibles por máquina; y
 - en la etapa (i), visualizar símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores de cada sub-bloque de datos gráficos verificables obtenido en el visualizador, o
 - en la etapa (ii), marcar en el sustrato, por medio del dispositivo de marcado, símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores de cada sub-bloque de datos gráficos verificables recibido por la unidad de control a partir de la unidad de procesamiento,
- proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son verificables por un usuario.

Esta segunda variante del método de marcado de generación de símbolos gráficos verificables en un soporte está particularmente adaptada al caso de un documento de varias páginas de texto (es decir, el soporte tiene una pluralidad de partes): el texto completo se divide en una pluralidad de fragmentos, cada fragmento de texto correspondiendo a una página de texto y por lo tanto, cada página del documento proporcionado en el soporte comprende una representación legible por seres humanos de símbolos gráficos de un sub-bloque de datos gráficos correspondiente junto con una representación legible por máquina separada de datos de corrección de errores de un sub-bloque de datos de corrección de errores correspondiente (por ejemplo, como un código de barras PDF417 mostrado en la figura 1).

Con el fin de permitir que un usuario determine adicionalmente si los símbolos gráficos legibles por seres humanos y un sub-bloque de datos de corrección de errores legibles por máquina correspondiente leído en el soporte (es decir, en la parte del soporte correspondiendo a un sub-bloque de datos gráficos del bloque de datos gráficos) son, o no, auténticos, la segunda variante anterior del método de marcado puede comprender adicionalmente las características de una de las siguientes dos sub-variantes.

De acuerdo con una primera sub-variante de la segunda variante del método de marcado,

- un valor de troceo de sub-bloque se calcula por medio de una función de troceo programada en cualquier porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos y dicho sub-bloque de datos de corrección de errores;
- para cada valor de troceo de sub-bloque, se calcula una representación legible por máquina correspondiente de dicho valor de troceo de sub-bloque;
- asociada con cada sub-bloque de datos gráficos verificables, la representación legible por máquina

correspondiente del valor de troceo de sub-bloque se proporciona adicionalmente en la parte correspondiente del soporte;

- un valor de troceo agregado de referencia de la totalidad de los valores de troceo de sub-bloque se determina como una concatenación de la totalidad de los valores de troceo de sub-bloque calculados; y

- 5 - el valor de troceo agregado de referencia se almacena en un libro mayor, proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son autenticables por un usuario.

- 10 De acuerdo con una segunda sub-variante de la segunda variante del método de marcado,

- un valor de troceo de sub-bloque se calcula por medio de una función de troceo programada en la unidad de procesamiento para cualquier porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos y dicho sub-bloque de datos de corrección de errores;

- 15 - un valor de troceo agregado de referencia de la totalidad de los valores de troceo de sub-bloque se determina como un valor de nodo raíz de un árbol que tiene los valores de troceo de sub-bloque calculados como valores de nodo hoja, comprendiendo el árbol unos nodos dispuestos de acuerdo con un ordenamiento de nodos dado en el árbol, comprendiendo dicho árbol unos niveles de nodo desde los nodos hoja al nodo raíz, correspondiendo cada valor de nodo no hoja del árbol a un valor de troceo de una concatenación de los valores de nodo respectivos de sus nodos secundarios de acuerdo con un ordenamiento de concatenación de árbol, correspondiendo el valor de nodo raíz a un valor de troceo de una concatenación de los valores de nodo de los nodos de un penúltimo nivel de nodos en el árbol de acuerdo con dicho ordenamiento de concatenación de árbol;

- para cada valor de troceo de sub-bloque, se determina una clave de trayectoria de verificación de sub-bloque asociada como una serie de valores de troceo de nodos no hoja seleccionados del árbol necesarios para recuperar el valor de nodo raíz a partir de dicho valor de troceo de sub-bloque;

- se incluye una representación legible por máquina de cada clave de trayectoria de verificación de sub-bloque, asociada con el sub-bloque de datos gráficos y el sub-bloque de datos de corrección de errores respectivamente correspondientes, en el sub-bloque de datos gráficos verificables, formateándose adicionalmente el sub-bloque de datos gráficos verificables para proporcionar una representación legible por máquina de dicha clave de trayectoria de verificación de sub-bloque separada de la representación legible por seres humanos del sub-bloque de datos gráficos asociado y la representación legible por máquina del sub-bloque de datos de corrección de errores asociado; y

- 35 (iii) el valor de troceo agregado de referencia se almacena en un libro mayor, o

(iv) poner el valor de troceo agregado de referencia a disposición de un usuario según un ejemplo que no cae dentro del ámbito de la invención, proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son autenticables por un usuario.

40

La invención también se refiere a un "método de verificación" de acuerdo con la reivindicación 5 correspondiendo al "método de marcado" anteriormente mencionado, es decir, un método de verificación de símbolos gráficos legibles por seres humanos proporcionados junto con una representación legible por máquina de datos de corrección de errores en un soporte, que se han generado de acuerdo con el método anteriormente mencionado de generación de símbolos gráficos verificables en dicho soporte, que comprende las etapas de:

45

- explorar con un escáner, equipado con una unidad de formación de imágenes, teniendo una unidad de procesamiento de escáner una memoria de escáner y conectada a un visualizador de escáner, símbolos gráficos legibles por seres humanos en el soporte para obtener, por medio de un procesamiento de imagen de los símbolos gráficos legibles por seres humanos explorados, un bloque de datos gráficos explorado que es una representación digital de dichos símbolos gráficos legibles por seres humanos explorados;

50

- explorar, con el escáner, una representación legible por máquina de datos de corrección de errores en el soporte para obtener, por medio de un descodificador legible por máquina programado en la unidad de procesamiento de escáner, datos de corrección de errores explorados correspondientes en un bloque de datos de corrección de errores explorado, siendo el bloque de datos de corrección de errores explorado una representación digital de dichos datos de corrección de errores explorados;

55

- corregir el bloque de datos gráficos explorado con un código de corrección de errores programado en la unidad de procesamiento de escáner, usando los datos de corrección de errores explorados del bloque de datos de corrección de errores explorado, para obtener un bloque de datos gráficos explorado corregido correspondiente; y

60

(a) visualizar una representación visual del bloque de datos gráficos explorado corregido como símbolos gráficos legibles por seres humanos corregidos correspondientes en el visualizador de escáner, o

65

(b) indicar, por medio del escáner, si el bloque de datos gráficos explorado contiene un error, o

(c) almacenar datos de resultado de exploración que especifican si el bloque de datos gráficos explorado contiene un error en la memoria de escáner.

5 Por lo tanto, de acuerdo con la invención, un usuario puede visualizar directamente, en el visualizador de escáner (opción (a)), los símbolos gráficos originales (por ejemplo, el texto original de un documento), debido a la corrección del texto explorado, y comparar fácilmente entonces los símbolos gráficos visualizados (es decir, símbolos gráficos legibles por seres humanos corregidos) con los símbolos gráficos en el soporte y detectar cualquier alteración o fraude.

10 El escáner puede ser un dispositivo específicamente dedicado o puede ser un mero teléfono inteligente equipado con una cámara y que tiene una aplicación programada accionable para ejecutarse en un procesador de dicho teléfono inteligente y ejecutar las etapas del método anterior de verificación de símbolos gráficos y datos de corrección de errores legibles por máquina correspondientes proporcionados en un soporte. Algunas de las etapas del método de verificación se pueden ejecutar asimismo en un servidor distante en comunicación con el escáner: por ejemplo, el escáner puede enviar el bloque de datos gráficos explorado y unos datos de corrección de errores legibles por máquina al servidor, unos medios de procesamiento programados de forma conveniente del servidor pueden ejecutar entonces las etapas de obtener datos de corrección de errores explorados correspondientes, corregir el bloque de datos gráficos explorado (con un código de corrección de errores programado en el servidor), usando los datos de corrección de errores explorados, para obtener un bloque de datos gráficos explorado corregido correspondiente, y enviar los datos gráficos explorados corregidos al escáner (posiblemente, con una indicación de si el bloque de datos gráficos explorado contiene un error, o almacenar datos de resultado de exploración que especifican si el bloque de datos gráficos explorado contiene un error en el servidor).

25 El método de verificación anterior, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con la primera variante del método de marcado, estando programada la función de troceo en la unidad de procesamiento de escáner, y estando conectado el escáner a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, comprende las etapas adicionales de:

30 - calcular, de acuerdo con la primera variante del método de marcado con la función de troceo programada en la unidad de procesamiento de escáner, un valor de troceo de exploración de la misma porción de un bloque de datos que resulta de una concatenación del bloque de datos gráficos explorado corregido y el bloque de datos de corrección de errores explorado;

35 - obtener el valor de troceo de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo de referencia obtenido concuerda con el valor de troceo de exploración; y

(e) indicar un resultado de la operación de comprobación, o
(f) almacenar un resultado de la operación de comprobación en la memoria de escáner.

40 Por lo tanto, incluso si se ha modificado un único bit de datos en los datos originalmente proporcionados en el soporte, el valor de troceo de exploración diferirá en gran medida del valor de troceo de referencia y se detectará la modificación.

45 En una segunda variante del método de verificación anterior, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con la segunda variante del método de marcado,

50 - la operación de explorar los símbolos gráficos legibles por seres humanos en el soporte comprende la exploración de los símbolos gráficos de sub-bloque del sub-bloque de datos gráficos correspondiente para obtener, por medio de un procesamiento de imagen, un sub-bloque de datos gráficos explorado correspondiente como una representación digital de los símbolos gráficos de sub-bloque explorados;

55 - la operación de explorar los datos de corrección de errores legibles por máquina en el soporte comprende la exploración de los datos de corrección de errores del sub-bloque de datos de corrección de errores correspondiente para obtener un sub-bloque de datos de corrección de errores explorado correspondiente;

- la operación de corregir el bloque de datos gráficos explorado comprende corregir los datos gráficos del sub-bloque de datos gráficos explorado, usando el sub-bloque de datos de corrección de errores explorado correspondiente, para obtener un sub-bloque de datos gráficos explorado corregido correspondiente; y

60 - la operación (a) de visualizar una representación visual del bloque de datos explorado corregido comprende visualizar una representación visual del sub-bloque de datos gráficos explorado corregido;

- la operación (b) de indicar si el bloque de datos gráficos explorado contiene un error comprende indicar si el sub-bloque de datos gráficos explorado contiene un error;

- la operación (c) de almacenar datos de resultado de exploración comprende almacenar si el sub-bloque de datos gráficos explorado contiene un error.

65 Una primera sub-variante de la segunda variante del método de verificación, en donde los símbolos gráficos

legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con la primera sub-variante de la segunda variante del método de marcado, la función de troceo y el código de corrección de errores se programan en la unidad de procesamiento de escáner, y el escáner es adicionalmente accionable para leer y descodificar una representación legible por máquina de un valor de troceo de sub-bloque en el soporte por medio de la unidad de procesamiento de escáner, el escáner se conecta a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, comprende las etapas adicionales de:

- calcular para cada parte del soporte, con la función de troceo programada en la unidad de procesamiento de escáner y de acuerdo con las operaciones llevadas a cabo para calcular un valor de troceo de sub-bloque, un valor de troceo de sub-bloque de exploración de la misma porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos explorado corregido y dicho sub-bloque de datos de corrección de errores explorado;
- en el caso en el que no es posible calcular un valor de troceo de sub-bloque de exploración para una parte del soporte, explorar y descodificar una representación legible por máquina de un valor de troceo de sub-bloque en dicha parte del soporte para obtener un valor de troceo de sub-bloque descodificado correspondiente, y usar este valor de troceo de sub-bloque descodificado como valor de troceo de sub-bloque de exploración para esta parte del soporte;
- calcular un valor de troceo de exploración agregado como una concatenación de la totalidad de los valores de troceo de sub-bloque de exploración;
- obtener el valor de troceo agregado de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo agregado de referencia obtenido concuerda con el valor de troceo de exploración agregado; e
- indicar un resultado de la operación de comprobación por medio del escáner.

Esta primera sub-variante de la segunda variante del método de marcado permite comprobar la autenticidad de símbolos gráficos de la totalidad de las partes legibles de un soporte, incluso si alguna parte o partes no son legibles (por ejemplo, debido a una alteración grave de los símbolos gráficos y/o los datos de corrección de errores proporcionados en dicha parte o partes), al recuperar el valor de troceo agregado correcto. De hecho, si un valor de troceo de sub-bloque de exploración no se puede calcular para una determinada parte del soporte, este se puede seguir obteniendo al leer y descodificar la representación legible por máquina de un valor de troceo de sub-bloque en dicha parte del soporte, y usar el valor de troceo descodificado en la concatenación de la totalidad de los valores de troceo para determinar un valor de troceo agregado candidato a comparar con el valor de troceo agregado de referencia.

Una segunda sub-variante de la segunda variante del método de verificación, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con la segunda sub-variante de la segunda variante del método de marcado, el valor de troceo agregado de referencia se almacena en el libro mayor, el escáner se conecta a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, y el escáner es adicionalmente accionable para leer y descodificar una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque en una parte correspondiente del soporte y calcular un valor de troceo agregado a partir de un par de valor de troceo de sub-bloque y clave de trayectoria de verificación de sub-bloque correspondientes, comprende las etapas adicionales de:

- calcular, con la función de troceo programada en la unidad de procesamiento de escáner y de acuerdo con las operaciones llevadas a cabo para calcular un valor de troceo de sub-bloque, un valor de troceo de sub-bloque de exploración de la misma porción de un sub-bloque de datos que resulta de una concatenación del sub-bloque de datos gráficos explorado corregido y el sub-bloque de datos de corrección de errores explorado;
- explorar, con el escáner, una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque, correspondiendo al sub-bloque de datos gráficos explorado corregido seleccionado, en una parte correspondiente del soporte, y extraer una clave de trayectoria de verificación de sub-bloque explorada correspondiente;
- calcular un valor de troceo agregado de exploración con el valor de troceo de sub-bloque de exploración calculado y la clave de trayectoria de verificación de sub-bloque explorada;
- obtener el valor de troceo agregado de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo agregado de referencia obtenido concuerda con el valor de troceo agregado de exploración; e
- indicar un resultado de la operación de comprobación por medio del escáner. Esta segunda sub-variante de la segunda variante del método de verificación permite comprobar la autenticidad de cada página de un documento, independientemente, debido a que un valor de troceo de nodo raíz candidato se puede calcular a partir de los datos leídos en cada página y compararse con el valor de troceo agregado de referencia.

Una tercera sub-variante de la segunda variante del método de verificación, que no cae dentro del alcance de la invención, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores

legibles por máquina en el soporte se han generado de acuerdo con la segunda sub-variante de la segunda variante del método de marcado, el valor de troceo agregado de referencia disponible para el usuario se almacena en la memoria de escáner, y el escáner es adicionalmente accionable para leer y descodificar una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque en una parte correspondiente del soporte y calcular un valor de troceo agregado a partir de un par de valor de troceo de sub-bloque y clave de trayectoria de verificación de sub-bloque correspondientes, comprende las etapas adicionales de:

- calcular, con la función de troceo programada en la unidad de procesamiento de escáner y de acuerdo con las operaciones llevadas a cabo para calcular un valor de troceo de sub-bloque, un valor de troceo de sub-bloque de exploración de la misma porción de un sub-bloque de datos que resulta de una concatenación del sub-bloque de datos gráficos explorado corregido y el sub-bloque de datos de corrección de errores explorado;
- explorar, con el escáner, una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque, correspondiendo al sub-bloque de datos gráficos explorado corregido seleccionado, en una parte correspondiente del soporte, y extraer una clave de trayectoria de verificación de sub-bloque explorada correspondiente;
- explorar, en el soporte, un valor de troceo agregado de referencia para obtener un valor de troceo agregado de referencia explorado;
- calcular un valor de troceo de exploración agregado con el valor de troceo de sub-bloque de exploración calculado y la clave de trayectoria de verificación de sub-bloque explorada;
- comprobar si el valor de troceo agregado de referencia almacenado en la memoria de escáner concuerda con el valor de troceo de exploración agregado; e
- indicar un resultado de la operación de comprobación por medio del escáner.

Esta tercera sub-variante de la segunda variante del método de verificación permite una comprobación sin conexión de la autenticidad de cada página de un documento, independientemente, debido a que un valor de troceo de nodo raíz candidato se puede calcular a partir de los datos leídos en cada página y compararse con el valor de troceo agregado de referencia almacenado en la memoria de escáner.

La invención también se refiere a un método de verificación alternativo de símbolos gráficos legibles por seres humanos proporcionados junto con datos de corrección de errores legibles por máquina en un visualizador de un ordenador, que se han generado de acuerdo con el método anteriormente mencionado de generación de símbolos gráficos verificables en dicho visualizador, en donde el ordenador tiene una aplicación de exploración programada en un procesador accionable para explorar símbolos gráficos legibles por seres humanos visualizados y datos de corrección de errores legibles por máquina, que comprende las etapas de:

- explorar los símbolos gráficos legibles por seres humanos visualizados, por medio de la aplicación de exploración que se ejecuta en el procesador informático, para obtener un bloque de datos gráficos explorado que es una representación digital de los símbolos gráficos legibles por seres humanos explorados;
- explorar los datos de corrección de errores legibles por máquina visualizados y, por medio de un descodificador legible por máquina de la aplicación de exploración que se ejecuta en el procesador informático, descodificar los datos de corrección de errores legibles por máquina explorados para obtener datos de corrección de errores explorados correspondientes en un bloque de datos de corrección de errores explorado;
- corregir el bloque de datos gráficos explorado con un código de corrección de errores de la aplicación de exploración que se ejecuta en el procesador informático, usando los datos de corrección de errores explorados del bloque de datos de corrección de errores explorado, para obtener un bloque de datos gráficos explorado corregido correspondiente; y

- (a) visualizar una representación visual del bloque de datos gráficos explorado corregido como símbolos gráficos legibles por seres humanos corregidos en el visualizador, o
- (b) visualizar una indicación que especifica si el bloque de datos gráficos explorado contiene un error, o
- (c) almacenar datos de resultado de exploración que especifican si el bloque de datos gráficos explorado contiene un error en una memoria del ordenador.

Este método de verificación alternativo (como un "método de verificación de datos visualizados") está particularmente adaptado para soportar capacidades de software de oficina (por ejemplo, como aplicaciones de procesamiento de texto) para detectar fraudes o errores en documentos de texto (por ejemplo, contratos, informes...) visualizados en una pantalla de ordenador, que se han generado en el ordenador o se han descargado en el ordenador (desde una memoria externa como una llave USB por ejemplo, o por medio de un enlace de comunicación con un servidor externo como, por ejemplo, un servidor de correo electrónico). Una aplicación específica que se ejecuta en el ordenador ejecuta, de hecho, las operaciones realizadas por el escáner en el método de verificación.

La invención se refiere adicionalmente a un soporte marcado con símbolos gráficos legibles por seres humanos y una representación legible por máquina de datos de corrección de errores asociados de acuerdo con el método de marcado anteriormente mencionado, o una cualquiera de su primera y su segunda variantes, o una cualquiera de su primera y su segunda sub-variantes de dicha segunda variante. Estando marcado adicionalmente dicho soporte con:

- una representación legible por máquina de un valor de troceo de sub-bloque de acuerdo con la primera sub-variante de la segunda variante del método de marcado, o
- una representación legible por máquina asociada de una clave de trayectoria de verificación de acuerdo con la segunda sub-variante de la segunda variante del método de marcado.

De acuerdo con otro aspecto, la invención se refiere a un escáner equipado con una unidad de formación de imágenes, una unidad de procesamiento de escáner y un visualizador de escáner, en donde la unidad de procesamiento de escáner se programa para hacer el escáner accionable para leer datos gráficos verificables marcados en un soporte de acuerdo con la invención mediante la implementación de las etapas del método de verificación, o su segunda variante de su segunda variante. El escáner se puede equipar adicionalmente con una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con un libro mayor, en donde la unidad de procesamiento de escáner se programa adicionalmente para hacer el escáner accionable para adquirir un valor de troceo a partir del libro mayor mediante la implementación de las etapas del método de acuerdo con una cualquiera de la primera variante del método de verificación o la primera sub-variante o la segunda sub-variante de la segunda variante del método de verificación.

Por último, la invención también se refiere a un producto de programa informático accionable, cuando se ejecuta en un ordenador equipado con un procesador, una memoria y un visualizador, para implementar las etapas del método de verificación alternativo (es decir, dicho "método de verificación de datos visualizados") para verificar símbolos gráficos legibles por seres humanos proporcionados junto con datos de corrección de errores legibles por máquina en el visualizador, que se han generado de acuerdo con el método de marcado.

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

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La **figura 1** ilustra un ejemplo de un soporte marcado con símbolos gráficos verificables de acuerdo con el método de marcado de la invención.

La **figura 2** es un diagrama de flujo que ilustra el proceso de generación y marcado de símbolos gráficos verificables en un sustrato de acuerdo con el método de marcado de la invención.

La **figura 3** es un diagrama de flujo del proceso de generación y visualización de símbolos gráficos verificables en un visualizador de acuerdo con el método de marcado de la invención.

La **figura 4** es un diagrama de flujo que ilustra el proceso de generación y provisión de símbolos gráficos verificables en un soporte de acuerdo con una segunda variante del método de marcado de la invención.

La **figura 5** muestra un ejemplo de árbol de troceo usado en la segunda sub-variante de la segunda variante del método de marcado de acuerdo con la invención.

La **figura 6** es un diagrama de flujo que ilustra el proceso de verificar símbolos gráficos y datos legibles por máquina proporcionados en un soporte de acuerdo con el método de verificación de la invención.

La **figura 7** es un diagrama de flujo que ilustra una realización de la segunda variante del método de verificación de acuerdo con la invención.

DESCRIPCIÓN DETALLADA

La figura 1 ilustra un ejemplo de un soporte 100 que es un sustrato (en el presente caso, una hoja de papel) marcado con una representación legible por seres humanos de símbolos gráficos 110 (en el presente caso, letras del alfabeto, caracteres de puntuación y números impresos en la hoja de papel 100) que representa un fragmento de texto de un contrato impreso en un área de texto 120 del soporte 100, junto con un código de barras en 2D legible por máquina 130 (en el presente caso, un código de barras PDF417, es decir, código de barras de "Archivo de Datos Portátil"417) impreso por debajo del área de texto 120. El fragmento de texto en el área de texto 120 es una representación legible por seres humanos de un bloque de datos gráficos

correspondiente de símbolos gráficos.

Un código de barras en 2D comprende, en general, las siguientes partes:

- 5 - un patrón de localización (por ejemplo, una forma en "L" y una línea de reloj para una Matriz de Datos, o tres cuadrados grandes para un código QR);
- algunas áreas de información acerca del formato del código;
- una zona de datos para contener datos; y
- 10 - unos datos de corrección de errores legibles por máquina para corregir errores de lectura (por ejemplo, datos de corrección de errores de Reed-Solomon).

Un código de corrección de errores usa, en general, una tabla de correspondencia, es decir, una correlación entre símbolos gráficos de un conjunto finito dado de símbolos gráficos de referencia (por ejemplo, glifos, como caracteres legibles de un alfabeto) y códigos correspondientes uno a uno (por ejemplo, símbolos codificados en un número dado de m bits).

El código de barras PDF417 130 es un código de barras lineal apilado bien conocido (norma ISO 15438) que se puede leer con una exploración lineal simple que es arrastrado por encima del código de barras. En la realización de la figura 1, el código de barras PDF417 130 es una representación legible por máquina de un bloque de datos de corrección de errores que se ha obtenido mediante la aplicación de un código de corrección de errores (en el presente caso, un código de Reed-Solomon convencional) al bloque de datos gráficos de una disposición de símbolos gráficos correspondiendo al fragmento de texto mostrado en el área de texto 120. El código de barras PDF417 130 también contiene (como es habitual) datos en relación con una versión del código (de Reed-Solomon) usado para calcular los datos de corrección de errores, datos en relación con las fuentes, el tamaño de fuente y la separación entre líneas del texto, el número de filas y columnas de texto, la ubicación relativa del área de texto con respecto a los marcadores 140 que delimitan las fronteras del bloque de datos gráficos (en el presente caso, marcas simples que especifican las esquinas del área de texto rectangular 120). Opcionalmente, el código de barras 130 puede contener adicionalmente datos de firma. Estos datos de firma pueden ser, por ejemplo, una firma de una representación digital del fragmento de texto por medio de una clave de cifrado privada (esta firma se puede descifrar por medio de una clave pública correspondiente).

El fragmento de texto impreso en el área de texto 120 y el código de barras PDF417 130 impreso son, respectivamente, ejemplos de símbolos gráficos legibles por seres humanos HrGS y una representación legible por máquina de datos de corrección de errores MrECD correspondientes que se han obtenido mediante el método de marcado ilustrado en la figura 2. De hecho, la figura 2 muestra un diagrama de flujo del proceso de generación de datos gráficos verificables VGD en un sustrato (en el presente caso, una hoja de papel) por medio de una unidad de procesamiento (CPU) que calcula un bloque de datos gráficos verificables VGDB, y marcando un sustrato por medio de un dispositivo de marcado (por ejemplo, una impresora de inyección de tinta) que ha recibido dicho bloque de datos gráficos verificables VGDB. Un bloque de datos gráficos GDB 210 que contiene una representación digital de símbolos gráficos DGS se almacena en una memoria de la CPU, en donde cada símbolo gráfico pertenece a un conjunto finito dado de M ($M \geq 1$) símbolos gráficos $\{GS(1), \dots, GS(M)\}$. Por ejemplo, el conjunto finito de $M = 26$ letras A a Z del alfabeto inglés. Cada símbolo gráfico $GS(i)$, $i \in \{1, \dots, M\}$, tiene su representación digital $DGS(i)$ correspondiente, y la representación digital de símbolos gráficos DGS del bloque de datos gráficos GDB contiene tantas $DGS(i)$ como símbolos gráficos hay en el fragmento de texto (por ejemplo, el fragmento de texto en el área de texto 120). El proceso de generación se inicia 200 al extraer 220 la representación digital de símbolos gráficos DGS del bloque de datos gráficos GDB almacenado, y procesar, con un código de corrección de errores ECC programado, la representación digital extraída de símbolos gráficos DGS para obtener datos de corrección de errores ECD correspondientes. Estos datos de corrección de errores ECD se representan en un bloque de datos de corrección de errores ECDB 230. El bloque de datos de corrección de errores ECDB obtenido se formatea 240 entonces para proporcionar unos datos de corrección de errores legibles por máquina MrECD correspondientes representados en un bloque de datos de corrección de errores legibles por máquina MrECDB. El bloque de datos gráficos GDB también se formatea para obtener 215 una representación legible por seres humanos correspondiente de sus símbolos gráficos HrGS que se incluyen en un bloque de datos de representación gráfica legibles por seres humanos HrGDB. Se obtiene 250 un bloque de datos gráficos verificables VGDB resultante, que está compuesto por los dos bloques de datos respectivos, el bloque de datos de representación gráfica legibles por seres humanos HrGDB y el bloque de datos de corrección de errores legibles por máquina MrECDB. De forma simbólica: $VGDB = HrGDB + MrECDB$. El bloque de datos gráficos verificables VGDB obtenido se envía entonces a un dispositivo de marcado, en el presente caso una impresora, y su contenido se marca 260 (es decir, se imprime) en el sustrato 100 de acuerdo con el formateo como datos gráficos verificables VGD correspondientes. El VGD marcado contiene símbolos gráficos legibles por seres humanos HrGS correspondientes y datos de corrección de errores legibles por máquina MrECD (de forma simbólica: $VGD = HrGS + MrECD$) que se disponen respectivamente en la hoja de papel 100 de acuerdo con el formateo (es decir, como bloques separados de datos), lo que expone el final 270 del proceso de generación de datos gráficos verificables en el sustrato 100 (véase la etapa (ii) del método de marcado

anteriormente mencionado).

En lugar de marcarse sobre un sustrato, el fragmento de texto se puede visualizar, por ejemplo, en un visualizador de una tableta o un ordenador, como se ilustra en el diagrama de flujo de la figura 3. Al igual que en la figura 2 previa, un bloque de datos gráficos GDB 310 que contiene una representación digital de símbolos gráficos DGS se almacena en una memoria de la CPU (perteneciendo cada símbolo gráfico al conjunto finito dado de $M \geq 1$ símbolos gráficos $\{GS(1), \dots, GS(M)\}$). El bloque de datos gráficos GDB contiene tantas representaciones digitales DGS (i) como símbolos gráficos GS (i) hay en el fragmento de texto visualizado. El proceso de generación se inicia 300 al extraer 320 la representación digital de símbolos gráficos DGS del bloque de datos gráficos GDB almacenado, y procesar, con un código de corrección de errores ECC programado, la DGS extraída para obtener datos de corrección de errores ECD correspondientes. Estos datos de corrección de errores ECD se incluyen en un bloque de datos de corrección de errores ECDB 330 que se formatea 340 entonces para proporcionar unos datos de corrección de errores legibles por máquina MrECD correspondientes incluidos en un bloque de datos de corrección de errores legibles por máquina MrECDB. El bloque de datos gráficos GDB también se formatea para obtener 315 una representación legible por seres humanos correspondiente de sus símbolos gráficos HrGS que se incluye en un bloque de datos de representación gráfica legibles por seres humanos HrGDB. Se obtiene 350 un bloque de datos gráficos verificables VGDB resultante, compuesto por los dos bloques de datos HrGDB y MrECDB respectivos (de forma simbólica, $VGDB = HrGDB + MrECDB$). El bloque de datos gráficos verificables VGDB se visualiza 360 entonces en el visualizador de acuerdo con el formateo como una representación legible por seres humanos separada de símbolos gráficos HrGS y una representación legible por máquina de datos de corrección de errores MrECD, lo que expone el final 370 del proceso de generación de símbolos gráficos verificables en un soporte (véase la etapa (i) del método de marcado anteriormente mencionado).

De acuerdo con la invención, varias variantes y sub-variantes del método de marcado aumentan el nivel de confianza en la conformidad entre los símbolos gráficos legibles por seres humanos como son leídos directamente en el soporte por un usuario y la versión legible por seres humanos que se puede extraer de la representación legible por máquina de los datos de corrección de errores (leída por un dispositivo dedicado). Estas variantes corresponden a la primera y la segunda variantes anteriormente mencionadas.

El método de marcado usa la cuasi-no invertibilidad de las funciones unidireccionales, como las funciones de troceo. En este método, después de haber llevado a cabo las etapas del método de marcado anterior, una función de troceo H, programada en la unidad de procesamiento, se usa adicionalmente para obtener un troceo de la representación digital de los símbolos gráficos o los datos de corrección de errores (o algunas partes de estos datos), al calcular un valor de troceo del bloque de cualquier porción de una concatenación (GDB $\oplus$ ECDB) del bloque de datos gráficos GDB y el bloque de datos de corrección de errores ECDB. El valor de troceo (por ejemplo, con una función de troceo SHA-256) se puede calcular en el mero bloque de datos gráficos: H (GDB). Preferiblemente, el valor de troceo se calcula sobre el bloque de concatenación completo: H (GDB $\oplus$ ECDB). En el caso en el que el valor de troceo se calcula en solo una porción de la concatenación del bloque de datos gráficos GDB y el bloque de datos de corrección de errores ECDB, es obvio que una longitud de bits de esa porción ha de ser suficiente para proporcionar un buen nivel de seguridad, póngase por ejemplo que ha de ser al menos igual a 100 bits y tener, preferiblemente, la longitud de bits del resultado entregado por la función de troceo seleccionada: por ejemplo, con un troceo de SHA-256, la longitud de bits de la porción es al menos de 256 bits (entonces, en la práctica, el troceo es no invertible). Por lo tanto, cualquier cambio, incluso de un único bit, en el argumento de la función de troceo (es decir, cualquier cambio en los símbolos gráficos o datos legibles por máquina en el soporte) generará un valor diferente del troceo.

En dicho método de marcado, el valor de troceo se almacena adicionalmente en un libro mayor, preferiblemente una cadena de bloques (siendo entonces el valor almacenado prácticamente inmutable), como un valor de troceo de referencia H_{ref} . Opcionalmente, el valor de troceo de referencia H_{ref} se puede firmar adicionalmente con una clave de cifrado, preferiblemente una clave privada Pr_k (almacenada en una memoria de la unidad de procesamiento), para obtener un valor de troceo de referencia firmado $S(H_{ref})$ correspondiente y el valor de troceo de referencia firmado $S(H_{ref})$ se almacena (por ejemplo, en un libro mayor como una base de datos o una cadena de bloques) o se proporciona en el soporte, siendo compatible esta última opción con un proceso de verificación sin conexión, con la condición de que una clave pública Pu_k correspondiendo a la clave privada Pr_k se use para comprobar la firma (es decir, verificar que el valor de troceo de referencia firmado se ha firmado con la clave privada correcta, o incluso para recuperar H_{ref} mediante el descifrado de $S(H_{ref})$ con la clave de descifrado pública al igual que con el algoritmo de RSA "Rivest-Shamir-Adleman").

La segunda variante del método de marcado, ilustrada mediante una realización mostrada en la figura 4, es muy conveniente para proporcionar símbolos gráficos en una pluralidad de partes del soporte, como, por ejemplo,

- imprimir (al igual que con la opción (ii) del método de marcado) un documento de texto que comprende una pluralidad de páginas (por ejemplo, las N páginas de un informe o un contrato, etc.), o
- visualizar (al igual que con la opción (i) del método de marcado) una versión digital de un documento de texto de N páginas en una pantalla en un formato dado (por ejemplo, en formato Microsoft Word o pdf),

en donde cada una de las N ($N \geq 2$) páginas marcadas en el sustrato, o cada una de las N páginas visualizadas, muestra un fragmento específico de símbolos gráficos legibles por seres humanos HrGS (j) ($j \in \{1, \dots, N\}$) y una representación legible por máquina de datos de corrección de errores MrECD (j) correspondientes: siendo ambas unas representaciones obtenidas a partir de un fragmento de datos gráficos verificables VGD (j) de un sub-bloque de datos gráficos verificables VGDSB (j) específico correspondiente. En estos casos, de acuerdo con dicha segunda variante del método de marcado, el método se inicia 400 y el bloque de datos gráficos GDB (completo) este dividido 410 por la unidad de procesamiento en N sub-bloques GDSB (1), ..., GDSB (N) (es decir, un sub-bloque para cada parte del soporte), en donde cada sub-bloque de datos gráficos GDSB (j) se formatea para proporcionar 415 una representación legible por seres humanos HrGS (j) correspondiente de sus símbolos gráficos GS (j) en un sub-bloque de datos gráficos legibles por seres humanos HrGDSB (j) correspondiente. Para cada sub-bloque de datos gráficos GDSB (j) ($j = 1, \dots, N$), la unidad de procesamiento genera datos de corrección de errores de sub-bloque correspondientes al corregir 420 el sub-bloque de datos gráficos GDSB (j) con el código de corrección de errores ECC programado, y entonces forma 430, con los datos corregidos, un sub-bloque de datos de corrección de errores ECDSB (j). La unidad de procesamiento genera 440 una representación legible por máquina de cada sub-bloque de datos de corrección de errores ECDSB (j) como un sub-bloque de datos de corrección de errores legibles por máquina MrECDSB (j) correspondiente. Entonces, la unidad de procesamiento formatea cada uno de los sub-bloques HrGDSB (j) y MrECDSB (j), de tal modo que una representación de esto último en el soporte es distinta de la representación legible por seres humanos HrGS (j) de los símbolos gráficos GS (j) del primero, para proporcionar 450 un sub-bloque de datos gráficos verificables correspondiente, escrito de forma simbólica $VGDSB(j) = HrGDSB(j) + MrECDSB(j)$. Dependiendo de la opción (i) o (ii) seleccionada del método de marcado, los datos de los sub-bloques VGDSB (j), $j = 1, \dots, N$, se visualizan 460 en un visualizador o se marcan 470 en un sustrato (por ejemplo, se imprimen en una hoja de papel al igual que en la figura 1) de acuerdo con el formato como datos gráficos verificables VGD (j) (de forma simbólica: $VGD(j) = HrGS(j) + MrECD(j)$), proporcionándose cada marca M (j) de VGD (j) en una parte j del sustrato (por ejemplo, impresa en la j-ésima página del documento de N páginas), lo que expone el final 480 - 490 del proceso de generación de datos gráficos verificables en el soporte.

Varias sub-variantes de la segunda variante anterior del método de marcado aumentan el nivel de confianza en la autenticidad de los símbolos gráficos legibles por seres humanos o la representación legible por máquina de los datos de corrección de errores proporcionados en el soporte. Estas sub-variantes son, de hecho, la primera y la segunda sub-variantes. Estas sub-variantes también usan la cuasi-no invertibilidad de las funciones unidireccionales (por ejemplo, las funciones de troceo como las funciones de troceo de SHA-256). En estas dos sub-variantes, después de haber llevado a cabo las etapas de la segunda variante anterior del método de marcado, una función de troceo H, programada en la unidad de procesamiento, se usa adicionalmente para obtener un troceo de la representación digital de los símbolos gráficos o los datos de corrección de errores (o algunas partes de estos datos). Debido al hecho de que, en dicha segunda variante del método de marcado, el bloque de datos gráficos GDB y el bloque de datos de corrección de errores ECDB correspondiente se dividen en N sub-bloques (correspondiendo a las N partes del soporte), hay varias posibilidades para definir, para cada sub-bloque j ($j = 1, \dots, N$), un valor de troceo de sub-bloque H (j) correspondiente como se ha explicado anteriormente: se ha de seleccionar una de estas posibilidades, y servirá para calcular los N valores de troceo de sub-bloque en una cualquiera de estas sub-variantes (y también en las variantes del método de verificación).

En una primera sub-variante de la segunda variante del método de marcado, la unidad de procesamiento calcula para cada sub-bloque de datos gráficos GDSB (j) ($j = 1, \dots, N$) un valor de troceo de sub-bloque H (j): por ejemplo, en una realización preferida, la concatenación completa del sub-bloque de datos gráficos GDSB (j) y el sub-bloque de datos de corrección de errores ECDSB (j) se selecciona para el valor de troceo de sub-bloque, es decir, $H(j) = H(GDSB(j) \oplus ECDSB(j))$. En general, los valores de troceo de sub-bloque H (j), $j = 1, \dots, N$, se definen de acuerdo con una de las siguientes posibilidades: se puede tener $H(j) = H(GDSB(j))$, o $H(j) = H(ECDSB(j))$, o al tomar un troceo de cualquier porción de una concatenación $(GDSB(j) \oplus ECDSB(j))$ del sub-bloque de datos gráficos GDSB (j) y el sub-bloque de datos de corrección de errores ECDSB (j), es decir, con $H(j) = H(\text{porción de } (GDSB(j) \oplus ECDSB(j)))$ (con la restricción con respecto a la longitud de bits de la porción ya mencionada).

Entonces, una representación legible por máquina MrH (j) de cada valor de troceo de sub-bloque H (j) es calculada por la unidad de procesamiento y se asocia con el sub-bloque de datos gráficos verificables VGDSB (j) ($j = 1, \dots, N$) correspondiente. Como resultado, además de la representación legible por seres humanos de los símbolos gráficos de j-ésimo sub-bloque HrGS (j) y la representación legible por máquina de

los datos de corrección de errores de j-ésimo sub-bloque MrECD (j) (a partir del sub-bloque de datos gráficos verificables VGDSB (j)), la j-ésima página del documento comprende adicionalmente la representación legible por máquina MrH (j) del valor de troceo de j-ésimo sub-bloque. Esta sub-variante permite asegurar adicionalmente los datos gráficos de sub-bloque y los datos de corrección de errores de sub-bloque correspondientes por medio de la función de troceo unidireccional, debido a que cualquier modificación de dichos datos de j-ésimo sub-bloque impedirá recuperar el contenido de datos de MrH (j). Además, esta ventaja adicional se obtiene con solo unos datos adicionales limitados proporcionados en el soporte en forma de mera representación legible por máquina de un valor de troceo de sub-bloque. En dicha primera sub-variante de la segunda variante del método de marcado, los N valores de troceo de sub-bloque H (j) (j = 1, ..., N) se usan entonces para calcular un valor de troceo agregado de referencia H_{ref}. Como se ha mencionado anteriormente, los N valores de troceo de sub-bloque H (j), j = 1, ..., N, se pueden calcular en los meros sub-bloques de datos gráficos, es decir, H (j) $\equiv$ H (GDSB (j)). Preferiblemente, los valores de troceo

de sub-bloque se calculan en la concatenación completa de sub-bloques: H (j) $\equiv$ H (GDSB (j) $\oplus$ ECDSB (j)). Por lo tanto, cualquier cambio, incluso de un único bit, en el argumento de una cualquiera de las funciones de troceo de sub-bloque H (j) (es decir, cualquier cambio en los datos legibles por máquina de sub-bloque o gráficos de sub-bloque en el soporte) generará un valor diferente del valor de troceo agregado H_{ref}. En esta primera sub-variante, la unidad de procesamiento concatena la totalidad de los N valores de troceo de sub-bloque H (j), j = 1, ..., N, para obtener el valor de troceo agregado de referencia H_{ref} = H (1) $\oplus$ H (2) $\oplus$...

$\oplus$ H (N - 1) $\oplus$ H (N) (indicando el símbolo $\oplus$ una operación de concatenación). Este valor de troceo de referencia H_{ref} se almacena adicionalmente en un libro mayor (es decir, en un servidor o base de datos, preferiblemente en una cadena de bloques).

Opcionalmente, la memoria de la unidad de procesamiento puede almacenar adicionalmente una clave para cifrar datos digitales, preferiblemente una clave privada Pr_k emparejada con una clave pública Pu_k (es decir, para un cifrado de clave asimétrica), la unidad de procesamiento, después de haber concatenado la totalidad de los N valores de troceo de sub-bloque para obtener el valor de troceo agregado de referencia H_{ref} = H (1)

$\oplus$ H (2) $\oplus$... $\oplus$ H (N - 1) $\oplus$ H (N), puede firmar (es decir, cifrar) adicionalmente el valor de troceo agregado de referencia H_{ref} con la clave de cifrado (preferiblemente, la clave privada Pr_k) para obtener una firma de valor de troceo agregado de referencia S (H_{ref}). Entonces, esta firma se puede almacenar (por ejemplo, en la memoria de la unidad de procesamiento, o en una base de datos, o en una cadena de bloques), o proporcionarse adicionalmente en el soporte. Esta última opción permite un proceso de verificación sin conexión, con la condición de que una clave correspondiente, preferiblemente la clave pública Pu_k asociada con la clave privada Pr_k, se use para comprobar que la firma es genuina (es decir, se ha obtenido con la clave privada Pr_k correcta).

En la segunda sub-variante de la segunda variante del método de marcado, después de haber calculado los N valores de troceo de sub-bloque H (j), j = 1, ..., N (de la misma forma que en la primera sub-variante anterior), el valor de troceo agregado de referencia H_{ref} es calculado por la unidad de procesamiento como el valor de nodo raíz R de un árbol, preferiblemente un árbol binario. Este árbol tiene los N valores de troceo de sub-bloque H (1), H (2), ..., H (N - 1), H (N) como nodos hoja, como se ilustra en la figura 5 (con un ejemplo de un mero árbol binario con N = 8). También en el presente caso, los valores de troceo son representativos de los valores generalmente obtenidos por medio de una función unidireccional (por ejemplo, una función de troceo H () de la familia de SHA-256). Por lo tanto, el árbol se basa, en general, en la pluralidad de valores de troceo de sub-bloque H (j) calculados, j = 1, ..., N, y comprende nodos dispuestos de acuerdo con un ordenamiento de nodos dado en el árbol. El árbol comprende unos niveles de nodo desde los nodos hoja

a (1, j), j = 1, ..., N, respectivamente correspondientes a la pluralidad de valores de troceo de sub-bloque H (1), H (2), ..., H (N - 1), H (N), y nodos no hoja subiendo hasta el nodo raíz R del árbol, correspondiendo cada nodo no hoja (es decir, un nodo comprendido entre un nodo hoja y el nodo raíz) del árbol a un valor de troceo de una concatenación de los valores de troceo respectivos de sus nodos secundarios de acuerdo con un ordenamiento de concatenación de árbol, el nodo raíz R correspondiendo al valor de troceo agregado de referencia H_{ref}, es decir, un valor de troceo de una concatenación de los valores de troceo de los nodos de un penúltimo nivel de nodos en el árbol de acuerdo con dicho ordenamiento de concatenación de árbol. En el ejemplo de la figura 5, con N = 8, se tienen, por lo tanto, ocho nodos hoja (primer nivel del árbol) a (1,

j) = H (j), j = 1, ..., 8, y para los cuatro valores de nodo del segundo nivel: a (2, 1) = H (a (1, 1) $\oplus$ a (1, 2)); a (2, 2) = H (a (1, 3) $\oplus$ a (1, 4)); a (2, 3) = H (a (1, 5) $\oplus$ a (1, 6)); a (2, 4) = H (a (1, 7) $\oplus$ a (1, 8)). Para los dos valores de nodo del tercer (penúltimo) nivel: a (3, 1) = H (a (2, 1) $\oplus$ a (2, 2)) y a (3, 2) = H (a (2, 3) $\oplus$ a (2, 4)). El valor de nodo raíz R es, por lo tanto: R = H (a (3, 1) $\oplus$ a (3, 2)) $\equiv$ H_{ref}. Se hace notar que es posible elegir un ordenamiento de concatenación de árbol diferente para cada nodo no hoja: por ejemplo, en lugar de tener a (2, 4) = H (a (1, 7) $\oplus$ a (1, 8)), se podría definir a (2, 4) = H (a (1, 8) $\oplus$ a (1, 7)), lo que da un valor de nodo diferente. La unidad de procesamiento calcula entonces para cada valor de troceo de sub-bloque H (j) (es decir, para cada nodo hoja del árbol a (1, j)), j = 1, ..., N, una clave de trayectoria de verificación VPK (j) de sub-bloque asociada. La clave de trayectoria de verificación VPK (j) de sub-bloque en

relación con el nodo hoja $a(1, j)$ (y, por lo tanto, con el valor de troceo de sub-bloque $H(j)$) es una serie de valores de troceo de nodos no hoja seleccionados del árbol que son necesarios para recuperar el valor de nodo raíz R empezando desde el nodo hoja $a(1, j)$. De hecho, los nodos no hoja seleccionados corresponden a una determinada trayectoria en el árbol entre el nodo hoja $a(1, j)$ y el nodo raíz R . Una clave de trayectoria de verificación de sub-bloque asociada con un nodo hoja dado del árbol es, de hecho, una secuencia de los valores de nodo respectivos, desde el nivel de nodos hoja al penúltimo nivel de nodos, de uno de cada dos nodos hoja que tiene el mismo nodo primario en el árbol que el nodo hoja dado y, de forma sucesiva, en cada nivel siguiente en el árbol, de cada nodo no hoja que tiene el mismo nodo primario en el árbol que el mismo nodo primario previo considerado en el nivel precedente. En el ejemplo del mero árbol binario con ocho nodos hoja $a(1, 1), \dots, a(1, 8)$ mostrado en la figura 5, las ocho claves de trayectoria de verificación VPK (1), $\dots$, VPK (8) de sub-bloque se determinan como sigue (de acuerdo con la definición anterior):

1) para un nodo hoja dado $a(1, 1) = H(1)$, la clave de trayectoria de verificación de sub-bloque asociada es VPK (1) = $\{a(1, 2), a(2, 2), a(3, 2)\}$, a partir de lo cual se puede recuperar el valor de firma digital de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

i) a partir de un nodo hoja dado $a(1, 1) = H(1)$ y un nodo hoja $a(1, 2) = H(2)$ en la VPK (1) ($a(1, 2)$ es el "otro nodo hoja que tiene el mismo nodo primario", es decir, el nodo $a(2, 1)$, "que el nodo hoja dado", es

decir, el nodo $a(1, 1)$), el valor de nodo primario $a(2, 1)$ se obtiene mediante $a(2, 1) = H(a(1, 1) \oplus a(1, 2))$ (es decir, $a(2, 1) = H(H(1) \oplus H(2))$),

ii) de la $a(2, 1)$ obtenida y el valor de nodo siguiente en la VPK (1), es decir, $a(2, 2)$ del nivel de nodos no hoja siguiente, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo $a(3, 1)$, que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo $a(2, 1)$, el valor de

nodo primario $a(3, 1)$ se obtiene mediante $a(3, 1) = H(a(2, 1) \oplus a(2, 2))$,

iii) de la $a(3, 1)$ obtenida y el valor de nodo siguiente en la VPK (1), es decir, $a(3, 2)$ del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo raíz R , que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo $a(3, 1)$, el valor de nodo

raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Comentario: en este ejemplo, se tienen tres etapas i), ii) y iii), debido a que el árbol tiene tres niveles por debajo del nivel de nodo raíz y por lo tanto, la clave de trayectoria de verificación de sub-bloque contiene tres valores de nodo.

Por lo tanto, basándose en la VPK (1) = $\{a(1, 2), a(2, 2), a(3, 2)\}$ asociada con $a(1, 1)$, el valor del nodo raíz del árbol se puede obtener como: $R = H(H(H(a(1, 1) \oplus a(1, 2)) \oplus a(2, 2)) \oplus a(3, 2))$.

2) para un nodo hoja dado $a(1, 2) = H(2)$, la clave de trayectoria de verificación de sub-bloque asociada es VPK (2) = $\{a(1, 1), a(2, 2), a(3, 2)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

i) a partir de $a(1, 2) = H(2)$ y $a(1, 1) = H(1)$ dados en la VPK (2) ($a(1, 1)$ es el otro nodo hoja que tiene el mismo nodo primario, es decir, el nodo $a(2, 1)$, que el nodo hoja dado, es decir, el nodo $a(1, 2)$), el valor de

nodo primario $a(2, 1)$ se obtiene mediante $a(2, 1) = H(a(1, 1) \oplus a(1, 2))$,

ii) de la $a(2, 1)$ obtenida y el valor de nodo siguiente en la VPK (2), es decir, $a(2, 2)$ del nivel de nodos no hoja siguiente, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo $a(3, 1)$, que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo $a(2, 1)$, el valor de

nodo primario $a(3, 1)$ se obtiene mediante $a(3, 1) = H(a(2, 1) \oplus a(2, 2))$,

iii) de la $a(3, 1)$ obtenida y el valor de nodo siguiente en la VPK (2), es decir, $a(3, 2)$ del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo raíz, que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo $a(3, 1)$, el valor de nodo

raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, basándose en la VPK (2) = $\{a(1, 1), a(2, 2), a(3, 2)\}$ asociada con $a(1, 2)$, el valor del nodo raíz del árbol se puede obtener como: $R = H(H(H(a(1, 1) \oplus a(1, 2)) \oplus a(2, 2)) \oplus a(3, 2))$.

3) para un nodo hoja dado $a(1, 3) = H(3)$, la clave de trayectoria de verificación de sub-bloque es VPK (3) = $\{a(1, 4), a(2, 1), a(3, 2)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

i) de $a(1, 3) = H(3)$ y $a(1, 4) = H(4)$ en la VPK (3) ($a(1, 4)$ es el otro nodo hoja que tiene el mismo nodo primario, es decir, el nodo $a(2, 2)$, que el nodo hoja dado, es decir, el nodo $a(1, 3)$), el valor de nodo primario

a (2, 2) se obtiene mediante $a(2, 2) = H(a(1, 3) \oplus a(1, 4))$,

ii) de la a (2, 2) obtenida y el valor de nodo siguiente en la VPK (3), es decir, a (2, 1) del nivel de nodos no hoja siguiente, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo a (3, 1), que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo a (2, 2), el valor de

5 nodo primario a (3, 1) se obtiene mediante $a(3, 1) = H(a(2, 1) \oplus a(2, 2))$,

iii) de la a (3, 1) obtenida y el valor de nodo siguiente en la VPK (3), es decir, a (3, 2) del penúltimo nivel de nodos, que es un nodo no hoja que tiene el mismo nodo primario en el árbol, es decir, el nodo raíz, que el mismo nodo primario previo considerado en el nivel precedente, es decir, el nodo a (3, 1), el valor de nodo

raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

10

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

$$R = H(H(a(2, 1) \oplus H(a(1, 3) \oplus a(1, 4))) \oplus a(3, 2)).$$

15 4) para un nodo hoja dado $a(1, 4) = H(4)$, la clave de trayectoria de verificación de sub-bloque es $VPK(4) = \{a(1, 3), a(2, 1), a(3, 2)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

20 i) de $a(1, 4) = H(4)$ y $a(1, 3) = H(3)$ en la VPK (4), el valor de nodo primario a (2, 2) se obtiene mediante $a(2, 2) = H(a(1, 3) \oplus a(1, 4))$,

ii) de la a (2, 2) obtenida y el valor de nodo siguiente en la VPK (4), es decir, a (2, 1) del nivel de nodos no hoja siguiente, el valor de nodo primario a (3, 1) se obtiene mediante $a(3, 1) = H(a(2, 1) \oplus a(2, 2))$,

iii) de la a (3, 1) obtenida y el valor de nodo siguiente en la VPK (4), es decir, a (3, 2) del penúltimo nivel de

25 nodos, el valor de nodo raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

$$R = H(H(a(2, 1) \oplus H(a(1, 3) \oplus a(1, 4))) \oplus a(3, 2)).$$

30

5) para un nodo dado $a(1, 5) = H(5)$, la clave de trayectoria de verificación de sub-bloque es $VPK(5) = \{a(1, 6), a(2, 4), a(3, 1)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

35

i) de $a(1, 5) = H(5)$ y $a(1, 6) = H(6)$ en la VPK (5), el valor de nodo primario a (2, 3) se obtiene mediante $a(2, 3) = H(a(1, 5) \oplus a(1, 6))$,

ii) de la a (2, 3) obtenida y el valor de nodo siguiente en la VPK (5), es decir, a (2, 4) del nivel de nodos no hoja siguiente, el valor de nodo primario a (3, 2) se obtiene mediante $a(3, 2) = H(a(2, 3) \oplus a(2, 4))$,

40

iii) de la a (3, 2) obtenida y el valor de nodo siguiente en la VPK (5), es decir, a (3, 1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

45

$$R = H(a(3, 1) \oplus H(H(a(1, 5) \oplus a(1, 6)) \oplus a(2, 4))).$$

6) para un nodo dado $a(1, 6) = H(6)$, la clave de trayectoria de verificación de sub-bloque es $VPK(6) = \{a(1, 5), a(2, 4), a(3, 1)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

50

i) de $a(1, 6) = H(6)$ y $a(1, 5) = H(5)$ en la VPK (6), el valor de nodo primario a (2, 3) se obtiene mediante $a(2, 3) = H(a(1, 5) \oplus a(1, 6))$,

ii) de la a (2, 3) obtenida y el valor de nodo siguiente en la VPK (6), es decir, a (2, 4) del nivel de nodos no hoja siguiente, el valor de nodo primario a (3, 2) se obtiene mediante $a(3, 2) = H(a(2, 3) \oplus a(2, 4))$,

55

iii) de la a (3, 2) obtenida y el valor de nodo siguiente en la VPK (6), es decir, a (3, 1) del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

$$R = H(a(3, 1) \oplus H(H(a(1, 5) \oplus a(1, 6)) \oplus a(2, 4))).$$

5

7) para un nodo dado $a(1, 7) = H(7)$, la clave de trayectoria de verificación de sub-bloque es $VPK(7) = \{a(1, 8), a(2, 3), a(3, 1)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

10

i) de $a(1, 7) = H(7)$ y $a(1, 8) = H(8)$ en la $VPK(7)$, el valor de nodo primario $a(2, 4)$ se obtiene mediante $a(2, 4) = H(a(1, 7) \oplus a(1, 8))$,

ii) de la $a(2, 4)$ obtenida y el valor de nodo siguiente en la $VPK(7)$, es decir, $a(2, 3)$ del nivel de nodos no hoja siguiente, el valor de nodo primario $a(3, 2)$ se obtiene mediante $a(3, 2) = H(a(2, 3) \oplus a(2, 4))$,

15

iii) de la $a(3, 2)$ obtenida y el valor de nodo siguiente en la $VPK(7)$, es decir, $a(3, 1)$ del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

$$R = H(a(3, 1) \oplus H(a(2, 3) \oplus H(a(1, 7) \oplus a(1, 8)))).$$

20

8) para un nodo dado $a(1, 8) = H(8)$, la clave de trayectoria de verificación de sub-bloque es $VPK(8) = \{a(1, 7), a(2, 3), a(3, 1)\}$, a partir de lo cual se puede recuperar el valor de raíz R por medio de las etapas siguientes (ejecutadas de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol):

25

i) de $a(1, 8) = H(8)$ y $a(1, 7) = H(7)$ en la $VPK(8)$, el valor de nodo primario $a(2, 4)$ se obtiene mediante $a(2, 4) = H(a(1, 7) \oplus a(1, 8))$,

ii) de la $a(2, 4)$ obtenida y el valor de nodo siguiente en la $VPK(8)$, es decir, $a(2, 3)$ del nivel de nodos no hoja siguiente, el valor de nodo primario $a(3, 2)$ se obtiene mediante $a(3, 2) = H(a(2, 3) \oplus a(2, 4))$,

30

iii) de la $a(3, 2)$ obtenida y el valor de nodo siguiente en la $VPK(8)$, es decir, $a(3, 1)$ del penúltimo nivel de nodos, el valor de nodo raíz R se obtiene mediante $R = H(a(3, 1) \oplus a(3, 2))$.

Por lo tanto, el valor del nodo raíz del árbol se puede obtener como:

$$R = H(a(3, 1) \oplus H(a(2, 3) \oplus H(a(1, 7) \oplus a(1, 8)))).$$

35

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

40

- extraer de la secuencia de valores de nodo en la clave de trayectoria de verificación de sub-bloque, un valor de nodo de uno de cada dos nodos hoja del árbol que tiene el mismo nodo primario que el del nodo hoja dado y calcular un valor de troceo de una concatenación del valor de nodo dado y, respectivamente de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol, el valor de nodo extraído de dicho uno de cada dos nodos hoja, obteniendo de este modo un valor de troceo de dicho mismo nodo primario del nodo hoja dado;

45

- de forma sucesiva en cada nivel siguiente en el árbol y subiendo hasta el penúltimo nivel de nodos:

- .extraer de la secuencia de valores de nodo en la clave de trayectoria de verificación de sub-bloque, un valor de nodo de uno de cada dos nodos no hoja del árbol que tiene el mismo nodo primario que el del mismo nodo primario previo considerado en la etapa precedente, y

50

- .calcular un valor de troceo de una concatenación del valor de nodo de dicho respectivo uno de cada dos nodos no hoja y el valor de troceo obtenido de dicho mismo nodo primario previo, de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol, obteniendo de este modo un valor de nodo de dicho mismo nodo primario de dicho mismo nodo primario previo; y

55

- calcular un valor de troceo de una concatenación de los valores de nodo obtenidos de los nodos no hoja correspondiendo al penúltimo nivel de nodos del árbol de acuerdo con el ordenamiento de nodos en el árbol y el ordenamiento de concatenación de árbol, obteniendo de este modo un valor de nodo raíz del árbol.

60

En una etapa siguiente de la segunda sub-variante de la segunda variante del método de marcado, la unidad de procesamiento genera una representación legible por máquina MrVPK (j) de cada clave de trayectoria de verificación VPK (j) de sub-bloque ($j = 1, \dots, N$), y la incluye, asociada con el sub-bloque de datos gráficos legibles por seres humanos HrGDSB (j) y el sub-bloque de datos de corrección de errores legibles por máquina MrECDSB (j) respectivamente correspondientes, en el sub-bloque de datos gráficos verificables VGDSB (j). El sub-bloque de datos gráficos verificables VGDSB (j) se formatea adicionalmente entonces para proporcionar una representación legible por máquina de dicha clave de trayectoria de verificación de sub-bloque que está separada de la representación legible por seres humanos del sub-bloque de datos gráficos GDSB (j) asociado y la representación legible por máquina del sub-bloque de datos de corrección de errores ECDSB (j) asociado, y se proporciona entonces en el soporte (como componente de los datos gráficos verificables de sub-bloque correspondientes). Por lo tanto, el sub-bloque de datos gráficos verificables se escribe de forma simbólica a continuación: $VGDSB(j) = HrGDSB(j) + MrECDSB(j) + MrVPK(j)$, $j = 1, \dots, N$. Por último, se realiza adicionalmente una de las etapas siguientes:

(iii) el valor de troceo agregado de referencia $H_{ref} = R$ se almacena en un libro mayor (preferiblemente, en una cadena de bloques),

o

(iv) el valor de troceo agregado de referencia $H_{ref} = R$ se pone a disposición de un usuario.

Opcionalmente, H_{ref} se puede firmar con una clave privada de firma Pr_k (almacenada en una memoria de la unidad de procesamiento), por medio de la unidad de procesamiento, para obtener una firma de valor de troceo agregado de referencia $S(H_{ref})$, y la firma de valor de troceo agregado de referencia $S(H_{ref})$ se almacena (por ejemplo, en el libro mayor) o se proporciona adicionalmente en el soporte o se pone a disposición de un usuario. Entonces, mediante el uso de una clave pública Pu_k correspondiente, es posible comprobar si $S(H_{ref})$ es genuina.

Como resultado, para cada sub-bloque de datos gráficos GDSB (j) ($j = 1, \dots, N$) del bloque de datos gráficos GDB, se proporcionan en el soporte unos símbolos gráficos legibles por seres humanos de sub-bloque correspondientes junto con unos datos de corrección de errores legibles por máquina de sub-bloque correspondientes que son autenticables por un usuario al recuperar el valor de raíz R por medio del valor de troceo de sub-bloque H (j) y su clave de trayectoria de verificación VPK (j) correspondiente que se puede obtener a partir de datos leídos en el soporte, respectivamente a partir de los símbolos gráficos legibles por seres humanos de sub-bloque HrGS (j) y la representación legible por máquina de la clave de trayectoria de verificación de sub-bloque MrVPK (j).

Como es obvio a partir del ejemplo anterior, el valor de nodo raíz R se puede recuperar por último a partir de cualquier valor de nodo hoja dado al calcular un valor de troceo de una concatenación de este valor de nodo hoja dado con solo los valores de nodo especificados en la clave de trayectoria de verificación de sub-bloque correspondiente. Por lo tanto, el volumen de datos en la información de verificación basándose en una clave de trayectoria de verificación (a leer en el soporte) que es necesaria para recuperar el valor de nodo raíz R es obviamente mucho menor que el volumen de datos necesario para calcular el valor de nodo raíz de referencia H_{ref} basándose solo en la totalidad de los valores de nodo hoja (es decir, al calcular la totalidad de los valores de nodo no hoja de los niveles intermedios del árbol): esto es una ventaja de la invención a la vista de la restricción de un tamaño limitado disponible en una representación legible por máquina de datos (como, por ejemplo, un código de barras bidimensional).

Por lo tanto, de acuerdo con la invención, el enmarañamiento de los valores de troceo de la totalidad de los valores de troceo de sub-bloque originales, debido a la estructura de árbol y al uso de funciones unidireccionales robustas para calcular los valores de nodo del árbol (como las funciones de troceo de SHA-256 en la realización anterior), junto con el valor de nodo raíz R del árbol (que se puede hacer inmutable si se almacena en una cadena de bloques) y la inclusión de datos de corrección de errores legibles por máquina y una clave de trayectoria de verificación legible por máquina asociada en el soporte junto con una representación legible por seres humanos correspondiente de datos gráficos, permiten evitar la falsificación de datos en el soporte marcado con un nivel muy alto de fiabilidad.

Las realizaciones anteriores del método de marcado proporcionan en un soporte (una hoja de papel 100 o visualizador) unos símbolos gráficos legibles por seres humanos junto con unos datos de corrección de errores legibles por máquina correspondientes que pueden ser verificados fácilmente por un usuario. De hecho, de acuerdo con el método de verificación de la invención del cual se muestra un diagrama de flujo ilustrativo en la figura 6, un usuario que tiene un escáner equipado con una unidad de formación de imágenes, una unidad de procesamiento de escáner con una memoria de escáner, y un visualizador de escáner, puede comprobar si los símbolos gráficos legibles por seres humanos HrGS en el soporte se han modificado, o no, con respecto a los originales, o incluso puede recuperar los símbolos gráficos originales. En la siguiente realización ilustrativa del método de verificación, los símbolos gráficos legibles por seres humanos HrGS constituyen un texto proporcionado en el soporte de acuerdo con el método de marcado. Por ejemplo, el texto se puede imprimir en un sustrato (por ejemplo, una hoja de papel, al igual que en la figura 1) o visualizarse electrónicamente en una pantalla. La unidad de formación de imágenes del escáner es

accionable para formar una imagen del texto y la representación legible por máquina correspondiente de datos de corrección de errores MrECD en el soporte. La unidad de procesamiento de escáner se programa para realizar un procesamiento de imagen de una imagen del soporte tomada por la unidad de formación de imágenes para extraer datos de texto y obtener una representación digital de los datos de texto extraídos como un bloque de datos gráficos explorado SGDB correspondiente. La unidad de procesamiento de escáner también se programa para realizar un procesamiento de imagen de una imagen de la representación legible por máquina de datos de corrección de errores MrECD en el soporte tomada por la unidad de formación de imágenes para extraer datos de corrección de errores explorados SECD correspondientes, mediante el uso adicional de un decodificador legible por máquina programado (en la unidad de procesamiento de escáner), y obtener una representación digital de los datos de corrección de errores explorados SECD como un bloque de datos de corrección de errores explorado SECD correspondiente. La unidad de procesamiento de escáner se programa adicionalmente para realizar las operaciones de corrección de errores de bloques de datos mediante el uso de un código de corrección de errores ECC. El escáner puede ser, por ejemplo, un mero teléfono inteligente con una cámara (como unidad de formación de imágenes) y que tiene unas aplicaciones de procesamiento de imagen, de decodificación y corrección de errores accionables para ejecutarse en su unidad de procesamiento.

El proceso de verificación general mostrado en la figura 6, con el ejemplo de soporte marcado de la figura 1, se inicia 600 al:

- explorar (por medio de la unidad de formación de imágenes de escáner), con el escáner, el texto HrGS 610 en el soporte, es decir, el texto 110 en el área de texto 120 de la hoja de papel 100, y obtener un bloque de datos gráficos explorado SGDB 620 correspondiente (es decir, una representación digital del texto explorado); y
- explorar la representación legible por máquina de datos de corrección de errores MrECD 615 en el soporte con el escáner, es decir, el código de barras PDF417 130 en la hoja de papel 100, decodificar la representación legible por máquina de datos de corrección de errores MrECD (con el decodificador legible por máquina programado) para extraer datos de corrección de errores explorados SECD correspondientes, y formar un bloque de datos de corrección de errores explorado SECD correspondiente (es decir, una representación digital de los SECD extraídos); y
- corregir 630 el bloque de datos gráficos explorado SGDB, por medio del código de corrección de errores ECC programado en la unidad de procesamiento de escáner (usando los SECD extraídos del SECD), y obtener un bloque de datos gráficos explorado corregido CSGDB 640, conteniendo el bloque de datos gráficos explorado corregido CSGDB una representación digital de símbolos gráficos legibles por seres humanos corregidos CHrGS correspondientes; y
- en la etapa 650, realizar al menos una de las tres opciones:
 - (a) visualizar 660, en el visualizador de escáner, el bloque de datos gráficos explorado corregido CSGDB como símbolos gráficos legibles por seres humanos corregidos CHrGS correspondientes; o
 - (b) indicar 670, por medio del escáner (por ejemplo, en el visualizador de escáner, o con cualquier alarma visual o de sonido entregada por el escáner), si el bloque de datos gráficos explorado SGDB contiene un error (basándose en un resultado de la corrección 630); o
 - (c) almacenar 680 datos de resultado de exploración que especifican si el bloque de datos gráficos explorado SGDB contiene un error (basándose en un resultado de la corrección 630) en la memoria de escáner.

Entregar un resultado de la opción u opciones (a), (b) y (c) seleccionadas pone fin 690 al proceso de verificación.

La opción (a) permite que el usuario compare visualmente la versión del texto CHrGS visualizado en el visualizador de escáner, que se ha corregido por medio del código de corrección de errores ECC programado usando los datos de corrección de errores explorados SECD (obtenidos a partir de la representación legible por máquina de datos de corrección de errores MrECD), y el texto (no corregido) HrGS según fue explorado en el soporte. Preferiblemente, la diferencia o diferencias del texto visualizado con el texto según fue explorado se pueden resaltar para ayudar al usuario a detectar y ubicar fácilmente cualquier cambio en el texto (por ejemplo, debido a una alteración o fraude).

Con la opción (b), el usuario puede ser alertado en el caso de cualquier diferencia entre el texto corregido CHrGS y el texto HrGS según fue explorado en el soporte.

La opción (c) permite realizar un seguimiento de cualquier diferencia existente entre el texto corregido y el texto según fue explorado en el soporte. Como alternativa, en el caso en el que el escáner está equipado adicionalmente con unos medios de comunicación (por ejemplo, un teléfono inteligente) y se puede conectar a un servidor externo, los datos de resultado de exploración se pueden almacenar en una memoria de servidor por medio de un enlace de comunicación.

Una ventaja del método de verificación anterior es que este permite una comprobación sin conexión (es decir, sin conexión a un dispositivo externo a través de un enlace de comunicación) de la conformidad entre el texto proporcionado en el soporte, como símbolos gráficos legibles por seres humanos, y la versión legible por

seres humanos que se puede obtener a partir de una representación legible por máquina de datos de corrección de errores leídos en el soporte: debido a que dicha versión resulta de una corrección por medio de un código de corrección de errores (similar al ya usado con el método de marcado para determinar los datos de corrección de errores correspondiendo al texto proporcionado en el soporte) del texto como se lee con el escáner en el soporte mediante el uso de los datos de corrección de errores extraídos de la representación legible por máquina como se lee en el soporte y descodificados por medio del escáner. Sin embargo, en el caso en el que el escáner está equipado adicionalmente con unos medios de comunicación (por ejemplo, un teléfono inteligente) y se puede conectar a un servidor externo, algunas o la totalidad de las operaciones anteriormente mencionadas del método de verificación de descodificación, y de realizar la corrección de errores de un bloque de datos se pueden llevar a cabo en el servidor externo (dedicado).

Varias variantes del método de verificación (correlacionadas, respectivamente, con la primera y la segunda variantes del método de marcado usado para proporcionar datos gráficos verificables en el soporte) permiten que un usuario vaya más allá de una mera verificación del texto (o, más en general, los símbolos gráficos) proporcionando en el soporte mediante la comprobación adicional de la autenticidad del texto (y/o los datos legibles por máquina).

En la primera variante del método de verificación de verificar símbolos gráficos legibles por seres humanos HrGS y una representación legible por máquina de datos de corrección de errores proporcionados en el soporte de acuerdo con la primera variante del método de marcado, después de haber llevado a cabo las etapas de dicho método de verificación (véase la figura 6), una función de troceo H se programa adicionalmente en la unidad de procesamiento de escáner para calcular un valor de troceo de un bloque de datos (de la misma forma que se especifica, respectivamente, en la primera variante del método de marcado), el escáner se conecta adicionalmente a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor en donde un valor de troceo de referencia H_{ref} se almacena (como se especifica en la primera variante del método de marcado), y la unidad de procesamiento de escáner calcula adicionalmente, por medio de la función de troceo H programada, un valor de troceo de exploración $H_{exploración}$ como un valor de troceo H (CSGDB) del bloque de datos gráficos explorado corregido CSGDB, o un valor de troceo H (SECDB) del bloque de datos de corrección de errores explorado SECDB, o un valor de troceo H (porción de CDB) de cualquier porción de un bloque de datos CDB $\equiv (CSGDB \oplus SECDB)$ que resulta de una concatenación $(CSGDB \oplus SECDB)$ del bloque de datos gráficos explorado corregido CSGDB y el bloque de datos de corrección de errores explorado SECDB (como se ha explicado anteriormente). El escáner lleva a cabo adicionalmente las siguientes operaciones:

- el escáner obtiene, por medio de su unidad de comunicación (al enviar una solicitud al libro mayor a través del enlace de comunicación y recibir de vuelta una respuesta) el valor de troceo de referencia H_{ref} almacenado en el libro mayor, y
- la unidad de procesamiento de escáner comprueba entonces si el valor de troceo de referencia H_{ref} obtenido concuerda con el valor de troceo de exploración $H_{exploración}$, y realiza al menos una de las operaciones:

- (e) esta indica un resultado de la operación de comprobación (por ejemplo, por medio del visualizador de escáner), o
- (f) esta almacena un resultado de la operación de comprobación en la memoria de escáner.

Cualquier modificación, con respecto al texto (como símbolos gráficos legibles por seres humanos) original (genuino), del texto legible por seres humanos proporcionado en el soporte, o el contenido de sus datos de corrección de errores legibles por máquina proporcionados en el soporte, generará una discordancia entre el valor de troceo de referencia H_{ref} y el valor de troceo de exploración $H_{exploración}$. Por lo tanto, esta variante aumenta el nivel de confianza en la conformidad del texto en el soporte con respecto a su versión original.

La segunda variante del método de verificación, ilustrada con una realización mostrada en la figura 7, es muy conveniente en el caso en el que el conjunto completo de símbolos gráficos se divide en una pluralidad de N subconjuntos (con $N \geq 2$), estando marcado cada subconjunto de símbolos gráficos en una parte de sustrato correspondiente, como, por ejemplo, un texto impreso (de acuerdo con la opción (ii) de la segunda variante del método de marcado) en una pluralidad de páginas (por ejemplo, las N páginas de un informe o un contrato, etc.) o visualizado (de acuerdo con la opción (i) de la segunda variante del método de marcado) en una pantalla en un formato dado (por ejemplo, un documento de texto de N páginas en formato Microsoft Word o pdf), página a página, en donde cada parte marcada de sustrato o cada página visualizada muestra un subconjunto específico de símbolos gráficos legibles por seres humanos y una representación legible por máquina de datos de corrección de errores correspondientes (siendo ambas unas representaciones obtenidas a partir de un sub-bloque de datos gráficos verificables específico correspondiente). En la siguiente realización ilustrativa de la segunda variante del método de verificación (véase la figura 7), los símbolos gráficos legibles por seres humanos HrGS constituyen un texto que se ha proporcionado en el soporte de acuerdo con la segunda variante del método de marcado. Por ejemplo, el texto se puede imprimir en un sustrato (por ejemplo, una hoja de papel, al igual que en la figura 1) o visualizarse electrónicamente en una

pantalla. La unidad de formación de imágenes del escáner es accionable para formar una imagen de cada página de las N páginas de texto en el soporte, es decir, cada uno de los símbolos gráficos legibles por seres humanos HrGS (j) (verificables) y una representación legible por máquina de datos de corrección de errores MrECD (j) correspondientes proporcionada en la j-ésima página ($j = 1, \dots, N$). La unidad de procesamiento de escáner se programa para realizar un procesamiento de imagen de una imagen de una j-ésima página ($j = 1, \dots, N$) en el soporte tomada por la unidad de formación de imágenes para extraer datos de texto explorados de los símbolos gráficos legibles por seres humanos HrGS (j) sometidos a formación de imágenes (es decir, los símbolos gráficos sometidos a formación de imágenes del j-ésimo sub-bloque) y obtener una representación digital de los datos extraídos como un sub-bloque de datos gráficos explorado SGDSB (j) correspondiente. La unidad de procesamiento de escáner también se programa para realizar un procesamiento de imagen de la imagen de la página j en el soporte tomada por la unidad de formación de imágenes, extraer datos de corrección de errores explorados SECD (j) a partir de la representación legible por máquina sometida a formación de imágenes de datos de corrección de errores MrECD (j), mediante el uso del descodificador legible por máquina programado en la unidad de procesamiento de escáner, y obtener una representación digital de los datos de corrección de errores explorados SECD (j) como un sub-bloque de datos de corrección de errores explorado SECD SB (j) correspondiente. La unidad de procesamiento de escáner se programa adicionalmente para realizar las operaciones de corrección de errores de bloques de datos mediante el uso de un código de corrección de errores ECC. El escáner puede ser un mero teléfono inteligente con una cámara (como unidad de formación de imágenes) y que tiene unas aplicaciones de procesamiento de imagen, de descodificación y corrección de errores accionables para ejecutarse en su unidad de procesamiento.

De acuerdo con la realización anterior (la figura 7) de dicha segunda variante del método de verificación, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina se han proporcionado en el soporte de acuerdo con la segunda variante del método de marcado (mostrado en la figura 4), el escáner anterior empieza 700 a ejecutar, para cada página j ($j = 1, \dots, N$) del documento, las siguientes operaciones de:

- explorar 710, con la unidad de formación de imágenes de escáner, unos símbolos gráficos legibles por seres humanos HrGS (j) proporcionados en la página j del soporte, es decir, el texto 110 en el área de texto 120 de la hoja de papel 100, y obtener 720 un sub-bloque de datos gráficos explorado SGDSB (j) correspondiente (es decir, una representación digital de los símbolos gráficos legibles por seres humanos explorados); y
- explorar 715, con la unidad de formación de imágenes de escáner, la representación legible por máquina de datos de corrección de errores MrECD (j) proporcionada en la página j del soporte, es decir, el código de barras PDF417 130 en la hoja de papel 100, descodificar, con la unidad de procesamiento de escáner, la MrECD (j) sometida a formación de imágenes, usar el descodificador legible por máquina programado, extraer datos de corrección de errores explorados SECD (j) correspondientes, y formar un sub-bloque de datos de corrección de errores explorado SECD SB (j) 725 correspondiente como una representación digital de los datos de corrección de errores explorados SECD (j);
- corregir 730, con la unidad de procesamiento de escáner, el sub-bloque de datos gráficos explorado SGDSB (j), mediante el uso del código de corrección de errores ECC programado en la unidad de procesamiento de escáner (y el uso de los SECD (j) extraídos del SECD SB (j)), y obtener 740 un sub-bloque de datos gráficos explorado corregido CSGDSB (j); y
- realizar 750 al menos una de las tres opciones para cada página j:

- (a) visualizar 760, en el visualizador de escáner, una representación visual (es decir, legible por seres humanos) del sub-bloque de datos gráficos explorado corregido CSGDB (j) como símbolos gráficos legibles por seres humanos corregidos CGS (j) correspondientes; o
- (b) indicar 770, por medio del escáner (por ejemplo, en el visualizador de escáner, o con cualquier alarma visual o de sonido entregada por el escáner), si el sub-bloque de datos gráficos explorado SGDB (j) contiene un error (basándose en un resultado de la corrección 730); o
- (c) almacenar 780 datos de resultado de exploración que especifican si el sub-bloque de datos gráficos explorado SGDB (j) contiene un error (basándose en un resultado de la corrección 730) en la memoria de escáner.

Entregar un resultado de la opción u opciones (a), (b) y (c) seleccionadas pone fin 790 a la segunda variante del proceso de verificación de cada página del documento. En el caso en el que el escáner está equipado adicionalmente con unos medios de comunicación (por ejemplo, un teléfono inteligente) y se puede conectar a un servidor externo, los datos de resultado de exploración de la opción (c) se pueden almacenar en una memoria de servidor por medio de un enlace de comunicación.

La invención también comprende tres sub-variantes de la segunda variante anterior del método de verificación. En la totalidad de estas sub-variantes, después de haber realizado las etapas de la realización de la segunda variante del método de verificación mostrado en la figura 7, una función unidireccional, en el presente caso la función de troceo H, se programa adicionalmente en la unidad de procesamiento de escáner

para calcular un valor de troceo de un bloque de datos (de la misma forma que se especifica, respectivamente, en las variantes del método de marcado), y la unidad de procesamiento de escáner calcula adicionalmente, por medio de la función de troceo H programada, N valores de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ ($j = 1, \dots, N$), siendo cada valor de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ un valor de troceo como un troceo H (CSGDSB (j)) del j-ésimo sub-bloque de datos gráficos explorado corregido CSGDSB (j), o un valor de troceo H (SECDSB (j)) del j-ésimo sub-bloque de datos de corrección de errores explorado SECDSB (j), o un valor de troceo H (porción de CDB (j)) de cualquier porción de un bloque de datos CDB (j) $\oplus$ SECDSB (j)) que resulta de una concatenación (CSGDSB (j) $\oplus$ SECDSB (j)) del j-ésimo sub-bloque de datos gráficos explorado corregido CSGDB (j) y el j-ésimo sub-bloque de datos de corrección de errores explorado SECDSB (j). El uso de los valores de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ calculados es específico en cada una de dicha primera, dicha segunda y dicha tercera sub-variantes de la segunda variante del método de verificación, como se detalla posteriormente.

En una realización de la primera sub-variante de la realización de la segunda variante del método de verificación, en donde los símbolos gráficos legibles por seres humanos HrGS (j) y los datos de corrección de errores legibles por máquina MrECD (j) en el soporte se han generado de acuerdo con la primera sub-variante de la segunda variante del método de marcado, la función de troceo y el código de corrección de errores se programan en la unidad de procesamiento de escáner, y el escáner es adicionalmente accionable para leer y decodificar una representación legible por máquina de un valor de troceo de sub-bloque H (j) en el soporte por medio de la unidad de procesamiento de escáner. Además, el escáner se conecta a una unidad de comunicación de escáner accionable para comunicarse, por medio de un enlace de comunicación, con el libro mayor en donde se almacena un valor de troceo agregado de referencia. El escáner calcula (véase anteriormente) los valores de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$, $j = 1, \dots, N$, en el caso en el que ello es posible (es decir, si la totalidad de los HrGS (j) y MrECD (j) son legibles). En el caso en el que no es posible calcular un valor de troceo de sub-bloque de exploración para una cierta página j, por ejemplo, debido a que los HrGS (j) y MrECD (j) en esta j-ésima página no son legibles, el escáner explora y decodifica una representación legible por máquina MrH (j) de un valor de troceo de sub-bloque H (j) en esta j-ésima página del soporte y obtiene un valor de troceo de sub-bloque descodificado DH (j) correspondiente: este valor de troceo de sub-bloque descodificado servirá entonces como valor de troceo de sub-bloque de exploración, es decir, $H_{\text{exploración}}(j) \equiv DH(j)$, para la j-ésima página. Esta representación legible por máquina de un valor de troceo de j-ésimo sub-bloque MrH (j) se asocia con el sub-bloque de datos gráficos verificables VGDSB (j) correspondiendo a símbolos gráficos legibles por seres humanos HrGS (j) y una representación legible por máquina de datos de corrección de errores MrECD (j) proporcionada en el soporte. Como resultado, la totalidad de los valores de troceo de exploración de sub-bloque necesarios para calcular un valor de troceo agregado para la totalidad de las páginas del soporte están disponibles (o bien como valores de troceo de exploración $H_{\text{exploración}}(j)$ calculados o bien según se identifican con valores de troceo descodificados DH (j)). La unidad de procesamiento de escáner ejecuta entonces las operaciones adicionales de:

- calcular un valor de troceo de exploración agregado $H_{\text{exploración}}$ mediante la concatenación de la totalidad de los valores de troceo de exploración obtenidos (el símbolo $\oplus$ representa un operador de concatenación):

$$H_{\text{exploración}} \equiv H_{\text{exploración}}(1) \oplus H_{\text{exploración}}(2) \oplus \dots \oplus H_{\text{exploración}}(N-1) \oplus H_{\text{exploración}}(N).$$

- enviar por medio de la unidad de comunicación de escáner, a través del enlace de comunicación, una solicitud de un valor de troceo agregado de referencia al libro mayor y recibir de vuelta un valor de troceo agregado de referencia H_{ref} ;
- comprobar si el valor de troceo agregado de referencia H_{ref} recibido concuerda con el valor de exploración agregado $H_{\text{exploración}}$, e indicar un resultado de la operación de comprobación (por ejemplo, por medio de un mensaje en el visualizador de escáner). En el caso de concordancia, las páginas son todas ellas genuinas (es decir, se corresponden con las originales), incluso si el texto y los datos de corrección de errores legibles por máquina de alguna página o páginas no eran legibles (sin embargo, las representaciones legibles por máquina de los valores de troceo de sub-bloque son legibles). En el caso de discordancia, se ha modificado al menos una de las páginas (por ejemplo, al menos uno de los símbolos gráficos está alterado o es falso); entonces es posible recuperar una página de este tipo mediante la comprobación de si concuerdan los valores de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ obtenidos a partir de los datos de sub-bloque HrGS (j) y MrECD (j), y los valores de troceo descodificados DH (j) correspondientes, $j = 1, \dots, N$.

Esta sub-variante permite comprobar independientemente, con un escáner, si cada página del documento de N páginas es genuina con la ayuda de la exploración de una mera representación legible por máquina de un valor de troceo de sub-bloque de un tamaño limitado.

En una realización de la segunda sub-variante de la segunda variante del método de verificación, los símbolos gráficos legibles por seres humanos HrGS (j), ($j = 1, \dots, N$) y los datos de corrección de errores

legibles por máquina MrECD (j) en la página j (de un documento de N páginas) en el soporte se han generado de acuerdo con la segunda sub-variante de la segunda variante del método de marcado, opción (iii), el escáner se conecta a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor que contiene el valor de troceo agregado de referencia H_{ref} (como valor de nodo raíz de un árbol, véase la figura 5), la función de troceo (la misma que se usa para calcular los N valores de troceo de sub-bloque $H(j)$ y el valor de troceo agregado de referencia H_{ref} correspondiente) se programa en la unidad de procesamiento de escáner. El escáner es adicionalmente accionable para leer y decodificar una representación legible por máquina MrVPK (j) ($j = 1, \dots, N$) de una clave de trayectoria de verificación VPK (j) de sub-bloque en el soporte y calcular un valor de troceo de exploración agregado $H_{exploración}$ a partir de un par de valor de troceo de sub-bloque $H(j)$ y clave de trayectoria de verificación VPK (j) de sub-bloque correspondientes explorados en el soporte (en el presente caso, se considera el caso $N = 8$, con un árbol binario correspondiendo al ejemplo de la figura 5 para un documento de 8 páginas). Después de haber calculado, con la función de troceo (véase anteriormente), el valor de troceo de sub-bloque de exploración $H_{exploración}(j)$, ($j \in \{1, \dots, N\}$) a partir de los datos gráficos verificables explorados en la página j del documento de N páginas y de acuerdo con la segunda sub-variante de la segunda variante del método de marcado (es decir, con la misma elección seleccionada de H (CSGDSB (j)), o H (SECDDB (j)) o H (porción de CDB (j)) para calcular un valor de troceo de sub-bloque, usados como nodos hoja del árbol), el escáner ejecuta las operaciones adicionales de:

- explorar una representación legible por máquina MrVPK (j) de una clave de trayectoria de verificación VPK (j) de sub-bloque en una j-ésima página del soporte (correspondiendo a un j-ésimo sub-bloque de datos gráficos explorado corregido CSGDSB (j)), y extraer una clave de trayectoria de verificación de sub-bloque explorada SVPK (j) correspondiente por medio de la unidad de procesamiento de escáner;
- calcular, con la unidad de procesamiento de escáner, un valor de troceo agregado de exploración $H_{exploración}$ con el valor de troceo de sub-bloque de exploración $H_{exploración}(j)$ calculado y la clave de trayectoria de verificación de sub-bloque explorada SVPK (j) obtenida al explorar la j-ésima página del documento, como se explica posteriormente:

.Si $j = 1$ (la primera página del documento), y como se ha explicado anteriormente con respecto a la realización de la segunda sub-variante de la segunda variante del método de marcado (véase también el árbol binario ilustrativo en la figura 5), el valor de troceo de sub-bloque $H_{exploración}(1)$ que se ha obtenido como se ha indicado anteriormente (es decir, a partir del primer sub-bloque de datos gráficos explorado corregido CSGDB (1) y/o el primer sub-bloque de datos de corrección de errores explorado SECDDB (1)) se considera como el valor del primer nodo hoja a (1, 1) del árbol binario (se selecciona el mismo ordenamiento de los nodos y ordenamiento de concatenación de árbol que en la realización anterior de la segunda sub-variante de la segunda variante del método de marcado), la clave de trayectoria de verificación de sub-bloque explorada SVPK (1) extraída contiene tres valores de nodo: $SVPK(1) = \{a(1, 2), a(2, 2), a(3, 2)\}$, por lo tanto, el valor de troceo de exploración $H_{exploración}$ que se puede obtener a partir de la exploración de los datos gráficos verificables de la primera página se calcula como

$$H_{exploración} = H(H(H(a(1, 1) \oplus a(1, 2)) \oplus a(2, 2)) \oplus a(3, 2))$$

$$= H(H(H(H_{exploración}(1) \oplus a(1, 2)) \oplus a(2, 2)) \oplus a(3, 2))$$

.Si $j = 2$, con $SVPK(2) = \{a(1, 1), a(2, 2), a(3, 2)\}$,

$$H_{exploración} = H(H(H(a(1, 1) \oplus H_{exploración}(2)) \oplus a(2, 2)) \oplus a(3, 2))$$

.Si $j = 3$, con $SVPK(3) = \{a(1, 4), a(2, 1), a(3, 2)\}$,

$$H_{exploración} = H(H(a(2, 1) \oplus H(H_{exploración}(3) \oplus a(1, 4))) \oplus a(3, 2))$$

.Si $j = 4$, con $SVPK(4) = \{a(1, 3), a(2, 1), a(3, 2)\}$

$$H_{exploración} = H(H(a(2, 1) \oplus H(a(1, 3) \oplus H_{exploración}(4))) \oplus a(3, 2))$$

.Si $j = 5$, con $SVPK(5) = \{a(1, 6), a(2, 4), a(3, 1)\}$

$$H_{exploración} = H(a(3, 1) \oplus H(H(H_{exploración}(5) \oplus a(1, 6)) \oplus a(2, 4)))$$

.Si $j = 6$, con $SVPK(6) = \{a(1, 5), a(2, 4), a(3, 1)\}$

$$H_{exploración} = H(a(3, 1) \oplus H(H(a(1, 5) \oplus H_{exploración}(6)) \oplus a(2, 4)))$$

. Si $j = 7$, con $SVPK(7) = \{a(1, 8), a(2, 3), a(3, 1)\}$,

$$H_{\text{exploración}} = H(a(3, 1) \oplus H(a(2, 3) \oplus H(H_{\text{exploración}}(7) \oplus a(1, 8))))$$

5

. Si $j = 8$, con $SVPK(8) = \{a(1, 7), a(2, 3), a(3, 1)\}$,

$$H_{\text{exploración}} = H(a(3, 1) \oplus H(a(2, 3) \oplus H(a(1, 7) \oplus H_{\text{exploración}}(8))))$$

- 10 - a continuación, obtener el valor de troceo agregado de referencia H_{ref} (es decir, el valor de nodo raíz R del árbol) almacenado en el libro mayor, por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo agregado de referencia H_{ref} obtenido concuerda con el valor de troceo agregado de exploración $H_{\text{exploración}}$, para $j = 1, \dots, N$; e
- indicar un resultado de la operación de comprobación (por ejemplo, en el visualizador de escáner).

15

Esta sub-variante del método de verificación permite detectar cualquier error en cada página de un documento con solo una pequeña cantidad de datos, debido a que cualquier variación en un contenido de una página da como resultado una discordancia entre el valor de troceo agregado de referencia H_{ref} y el valor de troceo de exploración $H_{\text{exploración}}$ obtenido a partir de los datos gráficos verificables explorados en esta página. Además, este método es robusto debido a que la versión corregida de los datos gráficos explorados se usa para calcular los valores de troceo de sub-bloque $H_{\text{exploración}}(j)$ de una j -ésima página, $j = 1, \dots, N$.

20

En una realización de la tercera sub-variante de la segunda variante del método de verificación, se usa el mismo árbol binario de un documento de $N = 8$ páginas así como la misma forma de calcular los valores de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ ($j = 1, \dots, N$) y valores de troceo de exploración $H_{\text{exploración}}$ al igual que en el ejemplo anterior de la segunda sub-variante de la segunda variante del método de verificación. En esta realización, los símbolos gráficos legibles por seres humanos $HrGS(j)$ y los datos de corrección de errores legibles por máquina $MrECD(j)$ en el soporte se han generado de acuerdo con la segunda sub-variante de la segunda variante del método de marcado, opción (iv), el valor de troceo agregado de referencia H_{ref} se almacena en la memoria de escáner, y el escáner también es accionable para leer y decodificar una representación legible por máquina de una clave de trayectoria de verificación $VPK(j)$ de sub-bloque en el soporte y calcular un valor de troceo agregado $H_{\text{exploración}}(j)$ a partir de un par de valor de troceo de sub-bloque y clave de trayectoria de verificación de sub-bloque correspondientes. De acuerdo con esta realización, después de haber realizado las etapas de dicha segunda variante del método de verificación y de haber calculado un valor de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ ($j = 1, \dots, N$) como se ha mencionado anteriormente, el escáner ejecuta las etapas adicionales de:

25

- explorar, con el escáner, una representación legible por máquina $MrVPK(j)$ de una clave de trayectoria de verificación $VPK(j)$ de sub-bloque en la j -ésima página proporcionada en el soporte (correspondiendo a un j -ésimo sub-bloque de datos gráficos explorado corregido $CSGDSB(j)$, por ejemplo, obtenido a partir de los datos gráficos verificables explorados proporcionados en la j -ésima página del documento), y extraer una clave de trayectoria de verificación de sub-bloque explorada $SVPK(j)$ correspondiente por medio de la unidad de procesamiento de escáner;

40

- calcular un valor de troceo agregado de exploración $H_{\text{exploración}}$ con el valor de troceo de sub-bloque de exploración $H_{\text{exploración}}(j)$ calculado y la clave de trayectoria de verificación de sub-bloque explorada $SVPK(j)$ obtenida al explorar la j -ésima página del documento (véase anteriormente, el cálculo detallado en relación con la segunda sub-variante de la realización de la segunda variante del método de verificación);

45

- obtener el valor de troceo agregado de referencia H_{ref} almacenado en la memoria de escáner;

- comprobar, por medio de la unidad de procesamiento de escáner, si el valor de troceo agregado de referencia H_{ref} obtenido concuerda con el valor de troceo de exploración agregado $H_{\text{exploración}}$ para la j -ésima página ($j = 1, \dots, N$); e

50

- indicar un resultado de la operación de comprobación (por medio del visualizador de escáner).

Esta sub-variante del método de verificación permite detectar, en un modo sin conexión robusto, cualquier error en cada página de un documento con solo una pequeña cantidad de datos, debido a que cualquier variación en un contenido de una página da como resultado una discordancia entre el valor de troceo agregado de referencia H_{ref} y el valor de troceo de exploración $H_{\text{exploración}}$ obtenido a partir de los datos gráficos verificables explorados en esta página. De hecho, el método solo usa datos (de un tamaño limitado) almacenados en la memoria de escáner (es decir, H_{ref}) para comprobar si el valor de troceo agregado de referencia H_{ref} concuerda con el valor de troceo de exploración $H_{\text{exploración}}$.

55

60

Una realización de la variante alternativa del método de verificación, ilustra una aplicación de la invención a la verificación de símbolos gráficos legibles por seres humanos y datos de corrección de errores legibles por máquina correspondientes generados en un ordenador conectado a un visualizador por un procesador

programado para realizar las etapas del método de marcado anteriormente mencionado, opción (i). El ordenador tiene una aplicación de exploración programada en su procesador que es accionable para explorar símbolos gráficos legibles por seres humanos visualizados y datos de corrección de errores legibles por máquina. Por lo tanto, el ordenador visualiza los símbolos gráficos legibles por seres humanos HrGS generados y los datos de corrección de errores legibles por máquina MrECD correspondientes, y la aplicación de exploración que se ejecuta en el procesador informático realiza entonces las siguientes operaciones de:

- explorar los símbolos gráficos legibles por seres humanos visualizados HrGS para obtener un bloque de datos gráficos explorado SGDB, siendo este bloque de datos gráficos explorado una representación digital de los símbolos gráficos legibles por seres humanos explorados;
- explorar los datos de corrección de errores legibles por máquina MrECD visualizados y, por medio de un descodificador legible por máquina de la aplicación de exploración que se ejecuta en el procesador informático, descodificar los datos de corrección de errores legibles por máquina MrECD explorados para obtener datos de corrección de errores explorados SECD correspondientes en un bloque de datos de corrección de errores explorado SECDB;
- corregir el bloque de datos gráficos explorado SGDB con un código de corrección de errores ECC de la aplicación de exploración que se ejecuta en el procesador informático, usando los datos de corrección de errores explorados SECD del bloque de datos de corrección de errores explorado SECDB, para obtener un bloque de datos gráficos explorado corregido CSGDB correspondiente; y
- realizar al menos una de las etapas siguientes:

- (a) visualizar una representación visual del bloque de datos gráficos explorado corregido CSGDB como símbolos gráficos legibles por seres humanos corregidos CHrGS en el visualizador, o
- (b) visualizar una indicación que especifica si el bloque de datos gráficos explorado SGDB contiene un error (basándose en el resultado de la etapa de corrección de SGDB), o
- (c) almacenar datos de resultado de exploración que especifican si el bloque de datos gráficos explorado SGDB contiene un error en una memoria del ordenador.

En la etapa (a), las partes de los símbolos gráficos legibles por seres humanos inicialmente visualizados HrGS (antes de ejecutar la aplicación de exploración) que se han corregido por medio de la aplicación de exploración se resaltan preferiblemente para facilitar la identificación y ubicación de errores en la HrGS inicialmente visualizada por un usuario del ordenador.

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 datos gráficos frente a falsificación y manipulación indebida, que comprende las etapas de:

5 almacenar, en una memoria de una unidad de procesamiento, un bloque de datos gráficos (210, 310) que contiene una representación digital de un conjunto finito dado de símbolos gráficos de los datos gráficos; procesar, con la unidad de procesamiento, la representación digital de símbolos gráficos del bloque de datos gráficos almacenado con un código de corrección de errores programado en la unidad de procesamiento para
10 generar datos de corrección de errores en un bloque de datos de corrección de errores correspondiente (230, 330);
formatear (215, 240; 315, 340) el bloque de datos gráficos y el bloque de datos de corrección de errores con la unidad de procesamiento para proporcionar respectivamente, en un bloque de datos gráficos legibles por seres humanos, una representación legible por seres humanos de los símbolos gráficos del bloque de datos
15 gráficos y, en un bloque de datos de corrección de errores legibles por máquina, una representación legible por máquina de los datos de corrección de errores del bloque de datos de corrección de errores separada de la representación legible por seres humanos de los símbolos gráficos del bloque de datos gráficos, para obtener (250, 350) un bloque de datos gráficos verificables correspondiente que comprende dicho bloque de datos gráficos legibles por seres humanos y dicho bloque de datos de corrección de errores legibles por
20 máquina; y

(i) visualizar símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores del bloque de datos gráficos verificables obtenido en un soporte (100) siendo un visualizador conectado a la unidad de procesamiento, o

25 (ii) marcar (260) en un soporte (100) siendo un sustrato, por medio de un dispositivo de marcado conectado a la unidad de procesamiento y equipado con una unidad de control accionable para controlar la operación de marcar basándose en datos recibidos de la unidad de procesamiento, símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores del bloque de datos gráficos verificables obtenido recibido de la unidad de procesamiento,

30 proporcionando de este modo, en el soporte, unos datos verificables que comprenden los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina correspondientes; comprendiendo además el método:

35 calcular, con una función de troceo programada en la unidad de procesamiento, un valor de troceo de cualquier porción de un bloque de datos que resulta de una concatenación del bloque de datos gráficos y el bloque de datos de corrección de errores; y
almacenar el valor de troceo calculado como un valor de troceo de referencia en un libro mayor.

40 2. Método de acuerdo con la reivindicación 1, en donde la representación legible por máquina de datos de corrección de errores es una cualquiera de una representación alfanumérica o una representación de código de barras (130).

45 3. Método de acuerdo con la reivindicación 1 o 2, en donde los símbolos gráficos son caracteres de texto (110) y el conjunto finito de símbolos gráficos es un alfabeto.

50 4. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde el soporte comprende una pluralidad de partes y el bloque de datos gráficos verificables se divide (410) en una misma pluralidad de sub-bloques de datos gráficos verificables, y los símbolos gráficos legibles por seres humanos y la representación legible por máquina de datos de corrección de errores correspondientes se diseminan, en consecuencia, de forma conjunta en partes correspondientes del soporte, mediante las etapas siguientes:

el bloque de datos gráficos se divide en una pluralidad de sub-bloques de datos gráficos, y cada sub-bloque de datos gráficos se formatea (415) para proporcionar una representación legible por seres humanos de sus
55 símbolos gráficos en un sub-bloque de datos gráficos legibles por seres humanos correspondiente; para cada sub-bloque de datos gráficos, la representación digital de sus símbolos gráficos se extrae y se procesa (420) con el código de corrección de errores para generar (430) datos de corrección de errores correspondientes en un sub-bloque de datos de corrección de errores;

60 cada sub-bloque de datos de corrección de errores se formatea para proporcionar (440), en un sub-bloque de datos de corrección de errores legibles por máquina correspondiente, una representación legible por máquina de datos de corrección de errores correspondientes separada de la representación legible por seres humanos de símbolos gráficos del sub-bloque de datos gráficos legibles por seres humanos correspondiente, para obtener (450) un sub-bloque de datos gráficos verificables correspondiente que comprende dicho sub-bloque de datos gráficos legibles por seres humanos y dicho sub-bloque de datos de corrección de errores legibles
65 por máquina; y

en la etapa (i), visualizar (460) símbolos gráficos legibles por seres humanos y una representación legible por

máquina correspondiente de datos de corrección de errores de cada sub-bloque de datos gráficos verificables obtenido en el visualizador, o

en la etapa (ii), marcar (470) en el sustrato, por medio del dispositivo de marcado, símbolos gráficos legibles por seres humanos y una representación legible por máquina correspondiente de datos de corrección de errores de cada sub-bloque de datos gráficos verificables recibido por la unidad de control a partir de la unidad de procesamiento,

proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son verificables por un usuario; en donde (1):

un valor de troceo de sub-bloque se calcula por medio de una función de troceo programada en la unidad de procesamiento para cualquier porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos y dicho sub-bloque de datos de corrección de errores;

para cada valor de troceo de sub-bloque, se calcula una representación legible por máquina correspondiente de dicho valor de troceo de sub-bloque;

asociada con cada sub-bloque de datos gráficos verificables, la representación legible por máquina correspondiente del valor de troceo de sub-bloque se proporciona adicionalmente en la parte correspondiente del soporte;

un valor de troceo agregado de referencia de la totalidad de los valores de troceo de sub-bloque se determina como una concatenación de la totalidad de los valores de troceo de sub-bloque calculados; y

el valor de troceo agregado de referencia se almacena en un libro mayor, proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son verificables por un usuario; o alternativamente (2):

un valor de troceo de sub-bloque se calcula por medio de una función de troceo programada en la unidad de procesamiento para cualquier porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos y dicho sub-bloque de datos de corrección de errores;

un valor de troceo agregado de referencia de la totalidad de los valores de troceo de sub-bloque se determina como un valor de nodo raíz de un árbol que tiene los valores de troceo de sub-bloque calculados como valores de nodo hoja, comprendiendo el árbol unos nodos dispuestos de acuerdo con un ordenamiento de nodos dado en el árbol, comprendiendo dicho árbol unos niveles de nodo desde los nodos hoja al nodo raíz, correspondiendo cada valor de nodo no hoja del árbol a un valor de troceo de una concatenación de los valores de nodo respectivos de sus nodos secundarios de acuerdo con un ordenamiento de concatenación de árbol, correspondiendo el valor de nodo raíz a un valor de troceo de una concatenación de los valores de nodo de los nodos de un penúltimo nivel de nodos en el árbol de acuerdo con dicho ordenamiento de concatenación de árbol;

para cada valor de troceo de sub-bloque, se determina una clave de trayectoria de verificación de sub-bloque asociada como una serie de valores de troceo de nodos no hoja seleccionados del árbol necesarios para recuperar el valor de nodo raíz a partir de dicho valor de troceo de sub-bloque;

se incluye una representación legible por máquina de cada clave de trayectoria de verificación de sub-bloque, asociada con el sub-bloque de datos gráficos y el sub-bloque de datos de corrección de errores respectivamente correspondientes, en el sub-bloque de datos gráficos verificables, formateándose adicionalmente el sub-bloque de datos gráficos verificables para proporcionar una representación legible por máquina de dicha clave de trayectoria de verificación de sub-bloque separada de la representación legible por seres humanos del sub-bloque de datos gráficos asociado y la representación legible por máquina del sub-bloque de datos de corrección de errores asociado; y

(iii) el valor de troceo agregado de referencia se almacena en un libro mayor, proporcionando de este modo, en el soporte, para cada sub-bloque de datos gráficos del bloque de datos gráficos, unos símbolos gráficos legibles por seres humanos correspondientes junto con unos datos de corrección de errores legibles por máquina correspondientes que son verificables por un usuario.

5. Método de verificación de símbolos gráficos legibles por seres humanos proporcionados junto con una representación legible por máquina de datos de corrección de errores en un soporte, que se han generado de acuerdo con el método de una cualquiera de las reivindicaciones 1 a 3, que comprende las etapas de:

explorar (610, 710) con un escáner, equipado con una unidad de formación de imágenes, teniendo una unidad de procesamiento de escáner una memoria de escáner y conectada a un visualizador de escáner, símbolos gráficos legibles por seres humanos en el soporte para obtener (620, 720), por medio de un procesamiento de imagen de los símbolos gráficos legibles por seres humanos explorados, un bloque de datos gráficos explorado que es una representación digital de dichos símbolos gráficos legibles por seres humanos explorados;

explorar (615, 715), con el escáner, una representación legible por máquina de datos de corrección de errores en el soporte para obtener (625, 725), por medio de un decodificador legible por máquina

programado en la unidad de procesamiento de escáner, datos de corrección de errores explorados correspondientes en un bloque de datos de corrección de errores explorado, siendo el bloque de datos de corrección de errores explorado una representación digital de dichos datos de corrección de errores explorados;

5 corregir (630, 730) el bloque de datos gráficos explorado con un código de corrección de errores programado en la unidad de procesamiento de escáner, usando los datos de corrección de errores explorados del bloque de datos de corrección de errores explorado, para obtener un bloque de datos gráficos explorado corregido correspondiente; y

10 (a) visualizar (660, 760) una representación visual del bloque de datos gráficos explorado corregido como símbolos gráficos legibles por seres humanos corregidos correspondientes en el visualizador de escáner y comparar la representación visual visualizada del bloque de datos gráficos explorado corregido con los símbolos gráficos legibles seres humanos proporcionados en el soporte y resaltar cualquier diferencia entre la representación visual del bloque de datos gráficos explorado corregido con los símbolos gráficos legibles por
15 seres humanos explorados, o
(b) indicar (670, 770), por medio del escáner, si el bloque de datos gráficos explorado contiene un error, o
(c) almacenar (680, 780) datos de resultado de exploración que especifican si el bloque de datos gráficos explorado contiene un error en la memoria de escáner; comprendiendo el método estando programada la función de troceo en la unidad de procesamiento de escáner, y estando conectado el escáner a una unidad
20 de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, comprendiendo el método las etapas adicionales de:

calcular, con la función de troceo programada en la unidad de procesamiento de escáner, un valor de troceo de exploración de la porción según el método de las reivindicaciones 1 a 3 de un bloque de datos que resulta
25 de una concatenación del bloque de datos gráficos explorado corregido y el bloque de datos de corrección de errores explorado;

obtener el valor de troceo de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo de referencia obtenido concuerda con el valor de troceo de exploración; y

30 (e) indicar un resultado de la operación de comprobación, o
(f) almacenar un resultado de la operación de comprobación en la memoria de escáner.

6. Método de acuerdo con la reivindicación 5, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con el
35 método de la reivindicación 1, en donde:

la operación de explorar los símbolos gráficos legibles por seres humanos en el soporte comprende la exploración de los símbolos gráficos de sub-bloque del sub-bloque de datos gráficos correspondiente para obtener, por medio de un procesamiento de imagen, un sub-bloque de datos gráficos explorado
40 correspondiente como una representación digital de los símbolos gráficos de sub-bloque explorados; la operación de explorar los datos de corrección de errores legibles por máquina en el soporte comprende la exploración de los datos de corrección de errores del sub-bloque de datos de corrección de errores correspondiente para obtener un sub-bloque de datos de corrección de errores explorado correspondiente; la operación de corregir el bloque de datos gráficos explorado comprende corregir los datos gráficos del sub-bloque de datos gráficos explorado, usando el sub-bloque de datos de corrección de errores explorado
45 correspondiente, para obtener un sub-bloque de datos gráficos explorado corregido correspondiente; y la operación (a) de visualizar una representación visual del bloque de datos explorado corregido comprende visualizar una representación visual del sub-bloque de datos gráficos explorado corregido; la operación (b) de indicar si el bloque de datos gráficos explorado contiene un error comprende indicar si el
50 sub-bloque de datos gráficos explorado contiene un error; la operación (c) de almacenar datos de resultado de exploración comprende almacenar si el sub-bloque de datos gráficos explorado contiene un error.

7. Método de acuerdo con la reivindicación 6, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en el soporte se han generado de acuerdo con el método de la primera realización (1) de la reivindicación 4, estando programados la función de troceo y el código de corrección de errores en la unidad de procesamiento de escáner, y siendo adicionalmente accionable el escáner para leer y descodificar una representación legible por máquina de un valor de troceo de sub-bloque en el soporte por medio de la unidad de procesamiento de escáner, estando conectado el
60 escáner a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, que comprende las etapas adicionales de:

calcular para cada parte del soporte, con la función de troceo programada en la unidad de procesamiento de escáner y de acuerdo con las operaciones llevadas a cabo para calcular un valor de troceo de sub-bloque, un
65 valor de troceo de sub-bloque de exploración de cualquier porción de un sub-bloque de datos que resulta de una concatenación de dicho sub-bloque de datos gráficos explorado corregido y dicho sub-bloque de datos

de corrección de errores explorado;

en el caso en el que no es posible calcular un valor de troceo de sub-bloque de exploración para una parte del soporte, explorar y descodificar una representación legible por máquina de un valor de troceo de sub-bloque en dicha parte del soporte para obtener un valor de troceo de sub-bloque descodificado correspondiente, y usar este valor de troceo de sub-bloque descodificado como valor de troceo de sub-bloque de exploración para esta parte del soporte;

5 calcular un valor de troceo de exploración agregado como una concatenación de la totalidad de los valores de troceo de sub-bloque de exploración;

10 obtener el valor de troceo agregado de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo agregado de referencia obtenido concuerda con el valor de troceo de exploración agregado; e indicar un resultado de la operación de comprobación por medio del escáner.

15 **8.** Método de acuerdo con la reivindicación 6, en donde los símbolos gráficos legibles por seres humanos y los datos de corrección de errores legibles por máquina en cada parte del soporte se han generado de acuerdo con el método de la segunda realización (2) de la reivindicación 4, almacenándose el valor de troceo agregado de referencia en el libro mayor, estando conectado el escáner a una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con el libro mayor, y siendo adicionalmente accionable el escáner para leer y descodificar una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque en una parte correspondiente del soporte y calcular un valor de troceo agregado a partir de un par de valor de troceo de sub-bloque y clave de trayectoria de verificación de sub-bloque correspondientes, que comprende las etapas adicionales de:

25 calcular, con la función de troceo programada en la unidad de procesamiento de escáner y de acuerdo con las operaciones llevadas a cabo para calcular un valor de troceo de sub-bloque, un valor de troceo de sub-bloque de exploración de cualquier porción de un sub-bloque de datos que resulta de una concatenación del sub-bloque de datos gráficos explorado corregido y el sub-bloque de datos de corrección de errores explorado;

30 explorar, con el escáner, una representación legible por máquina de una clave de trayectoria de verificación de sub-bloque, correspondiendo al sub-bloque de datos gráficos explorado corregido seleccionado, en una parte correspondiente del soporte, y extraer una clave de trayectoria de verificación de sub-bloque explorada correspondiente;

calcular un valor de troceo agregado de exploración con el valor de troceo de sub-bloque de exploración calculado y la clave de trayectoria de verificación de sub-bloque explorada;

35 obtener el valor de troceo agregado de referencia almacenado en el libro mayor por medio de la unidad de comunicación de escáner y el enlace de comunicación, y comprobar si el valor de troceo agregado de referencia obtenido concuerda con el valor de troceo agregado de exploración; e indicar un resultado de la operación de comprobación por medio del escáner.

40 **9.** Escáner equipado con una unidad de formación de imágenes, una unidad de procesamiento de escáner, un visualizador de escáner y una unidad de comunicación de escáner accionable para comunicarse por medio de un enlace de comunicación con un libro mayor, en donde la unidad de procesamiento de escáner se programa para hacer el escáner accionable para implementar las etapas del método de acuerdo con una cualquiera de las reivindicaciones 5-8.

45

DIBUJOS

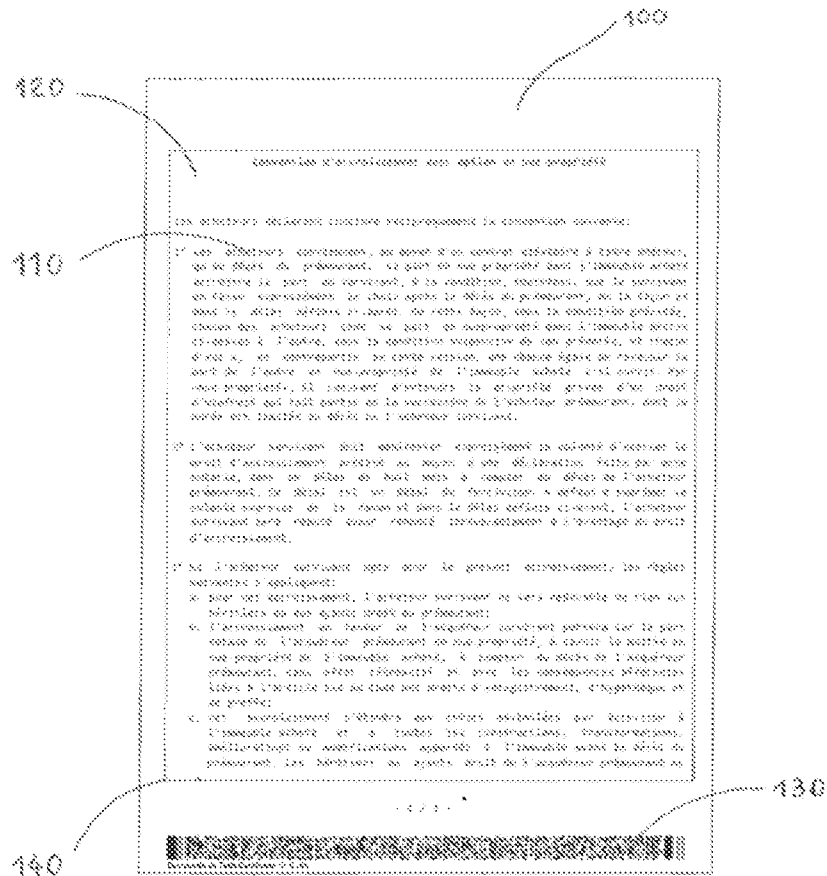


Fig. 1

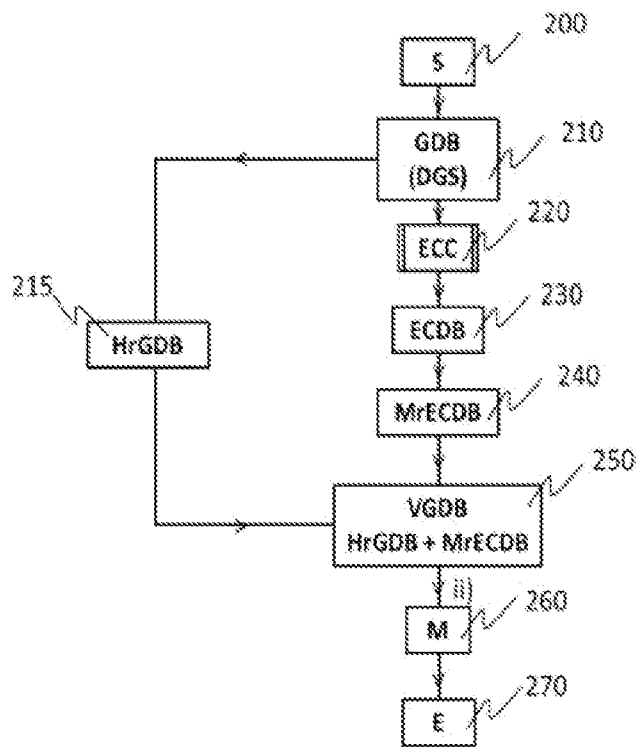


Fig.2

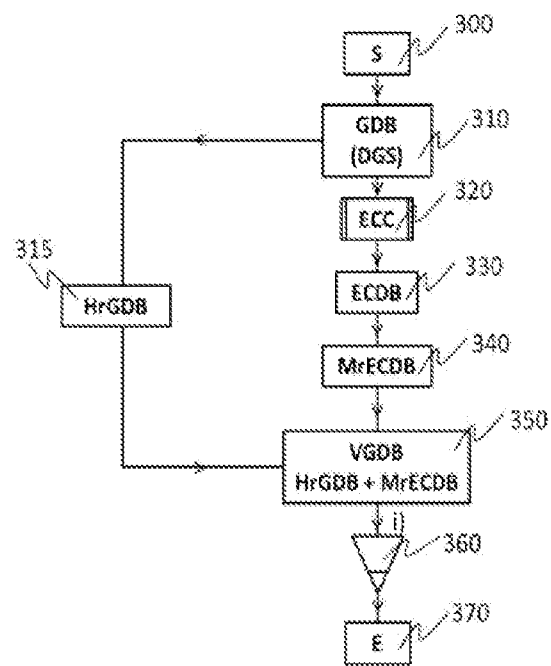


Fig.3

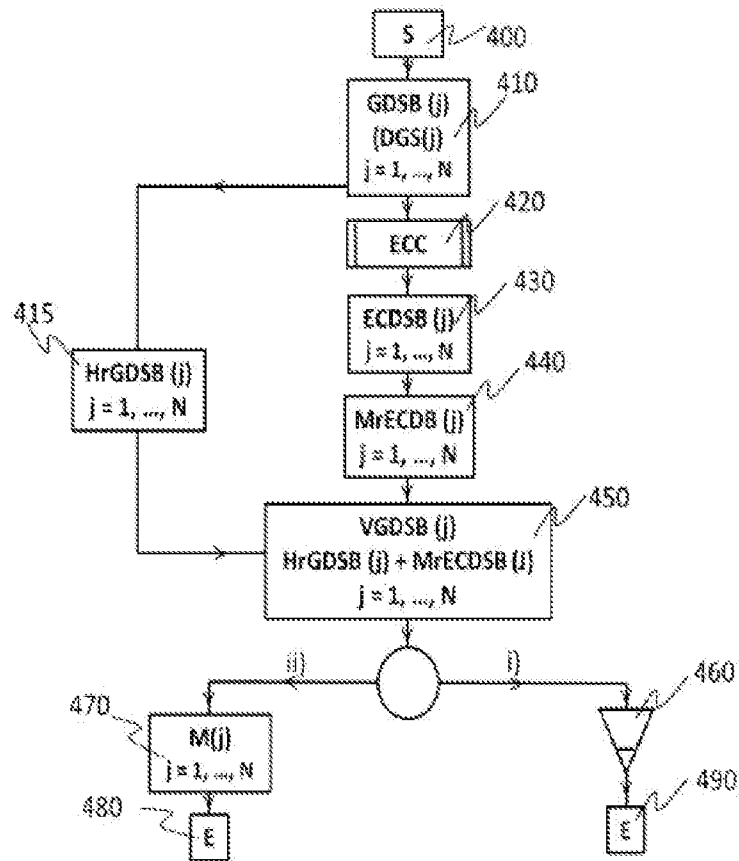


Fig.4

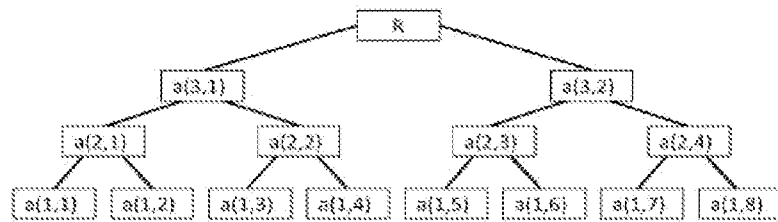


Fig.5

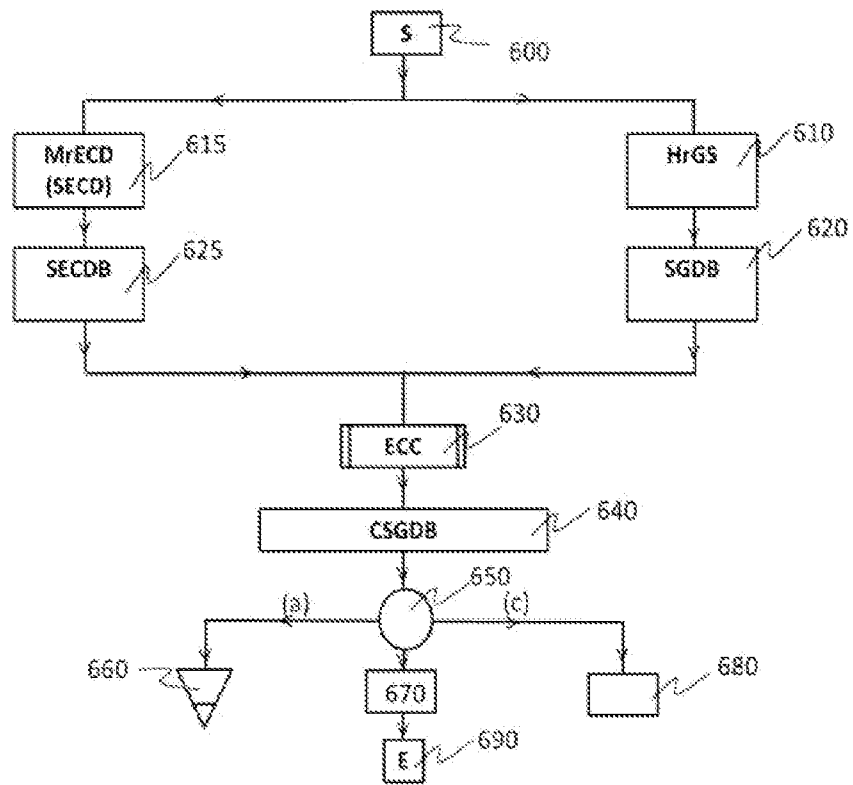


Fig.6

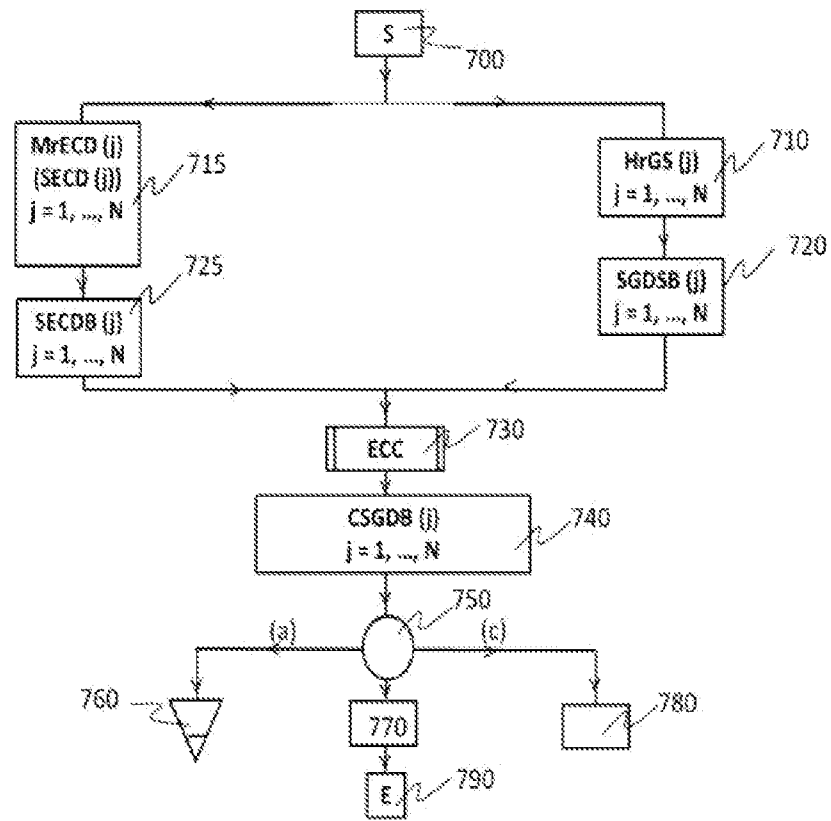


Fig.7