

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 960 203**

51 Int. Cl.:

G07D 7/20 (2006.01)

G07D 7/206 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **03.06.2016** **PCT/EP2016/062651**

87 Fecha y número de publicación internacional: **07.12.2017** **WO17207064**

96 Fecha de presentación y número de la solicitud europea: **03.06.2016** **E 16727992 (6)**

97 Fecha y número de publicación de la concesión europea: **16.08.2023** **EP 3465637**

54 Título: **Método para autenticar un documento**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
01.03.2024

73 Titular/es:

**VERIDAS DIGITAL AUTHENTICATION
SOLUTIONS, S.L. (100.0%)
Polígono Talluntxe II, Planta Primera M10
31192 Tajonar, Navarra, ES**

72 Inventor/es:

**AZANZA LADRÓN, EDUARDO;
BARBADILLO VILLANUEVA, GUILLERMO;
SANCHEZ YOLDI, MIKEL;
ISLA URTASUN, MIGUEL y
GOÑI LÓPEZ, SONIA**

74 Agente/Representante:

CONTRERAS PÉREZ, Yahel

ES 2 960 203 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

Método para autenticar un documento

5 CAMPO DE LA INVENCIÓN

La presente descripción se refiere a métodos, dispositivos y productos de programas informáticos para autenticar un documento. La presente descripción también se refiere a un método de autenticación para autenticar la identidad de una persona.

10 ANTECEDENTES

En los últimos años, el registro y pago digitales han aumentado por todo el mundo. Los dispositivos portátiles, p. ej. teléfonos móviles, están reemplazando el escritorio personal como una herramienta de pago. Al mismo tiempo, los delincuentes están desarrollando nuevos tipos de fraude para acceder a los datos personales desde internet. El proceso de autenticación es la etapa más sensible que han de afrontar los usuarios. A modo de resumen, este proceso consiste en verificar que la persona es quién realmente se supone que es y analizar que los datos del usuario son correctos. Estos dos tipos de validaciones se denominan validación personal y validación de DI (por ejemplo, un documento de identidad).

20 Hay cuatro reglas para controlar:

1. Si se valida un DI y el portador también, entonces el proceso de autenticación es correcto.
2. Si se valida un DI pero el portador no, entonces el proceso de autenticación no es correcto. Este caso ocurre, por ejemplo, cuando un delincuente roba un DI real e intenta utilizarlo.
3. Si no se valida un DI pero el portador sí, entonces el proceso de autenticación no es correcto. Este caso ocurre, por ejemplo, cuando un falsificador modifica un DI e intenta utilizarlo.
4. Si no se valida un DI ni el portador, entonces el proceso de autenticación no es correcto.

30 El proceso de autenticación se puede realizar en base a cualquiera de los tres tipos de medidas de seguridad que están presentes en el documento (DI). Las medidas de seguridad del tipo uno son aquellas que se pueden controlar mediante el ojo humano. Las medidas de seguridad del tipo dos son aquellas que se pueden controlar mediante un sensor específico. Finalmente, las medidas de seguridad del tipo tres son aquellas que están implementadas, pero sólo son conocidas por el fabricante.

35 En relación a la validación del documento, por ejemplo, el documento de identidad o un billete de banco, es un asunto realmente difícil debido a los siguientes factores:

- Diferencias entre países.
- Diferencias en forma. Los bordes de corte del documento tienen grandes tolerancias.
- Diferencias en impresión. Cada documento (DI) se completa en diferentes secciones.
- Estado físico: documentos DI rotos, errores de impresión (tinta eliminada), documentos doblados, olvido del chip, etc.

45 Los documentos de identidad tales como carnets de identidad se fabrican normalmente utilizando varios procesos de fabricación que se llevan a cabo en diferentes máquinas situadas en diferentes edificios gubernamentales. La última etapa es la impresión de los datos del usuario tales como nombre, apellido o fecha de nacimiento. Los diferentes procesos de fabricación tienen una variabilidad que provoca diferencias significativas entre diferentes documentos del mismo tipo.

50 En relación a la validación personal, el procedimiento más común se basa en tomar una foto o vídeo de un usuario y compararlo con una foto o un vídeo obtenido previamente. Sin embargo, este procedimiento de validación personal podría quebrarse mostrando una foto o vídeo del usuario (víctima) obtenida a partir de redes sociales frente al dispositivo de la cámara.

55 Por lo tanto, es necesario obtener un proceso de autenticación para validar tanto el documento como la persona, que sea más seguro y más robusto de implementar que los procesos de autenticación conocidos.

60 El documento US2003/099379 divulga un método de autenticación para autenticar un documento que comprende: recibir una o más imágenes obtenidas del documento; detectar uno o más elementos del documento; obtener por lo menos un parámetro de los elementos detectados, mediante el procesamiento de las una o más imágenes obtenidas del documento usando un método de procesamiento de imágenes; determinar por lo menos una meta-característica mediante la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia de uno o más elementos pre-obtenidos; determinar un indicador de autenticidad del documento mediante la verificación de si la por lo menos una meta-característica satisface por lo menos un umbral predefinido asociado con la por lo menos una meta-característica.

OBJETO DE LA INVENCION

En un primer aspecto, está provisto un método de autenticación para autenticar un documento.

5 Este método de autenticación para autenticar el documento puede comprender:
 recibir una o más imágenes obtenidas del documento;
 detectar uno o más elementos del documento;
 obtener por lo menos un parámetro de los elementos detectados, mediante el procesado de la una o más
 10 imágenes obtenidas del documento utilizando un método de procesamiento de imagen;
 determinar por lo menos una meta-característica mediante la comparación de por lo menos un parámetro de
 los elementos detectados con por lo menos un parámetro de referencia de uno o más elementos pre-obtenidos;
 determinar un indicador de autenticidad del documento mediante la verificación de si la por lo menos una meta-
 característica satisface por lo menos un umbral predefinido asociado a la por lo menos una meta-característica, en el
 15 que
 una meta-característica es por lo menos una medición de una diferencia de por lo menos un parámetro de un
 elemento detectado relativo a por lo menos un parámetro de referencia de por lo menos un modelo de referencia; el
 modelo de referencia comprendiendo el uno o más elementos pre-obtenidos.

20 Este método de autenticación para autenticar un documento, por ejemplo un documento DI o similar, es más seguro
 y más robusto que las soluciones de la técnica anterior puesto que se basa en analizar meta-características que son
 una medida de seguridad más fuerte que las medidas de seguridad típicamente implementadas.

Una "meta-característica" es una medición de la desviación o diferencia de por lo menos un parámetro de un
 25 elemento detectado en relación al mismo parámetro (por lo menos un parámetro de referencia) de un modelo de
 referencia, que puede ser inherente a una tolerancia de fabricación aleatoria de un proceso utilizado para fabricar el
 elemento que se ha de detectar en el documento, o puede ser creado a propósito. Las meta-características se
 refieren a todos los parámetros de los elementos que forman un documento midiendo desviaciones (diferencias) de
 30 estos elementos con respecto a un modelo de referencia. Dichas tolerancias serán más grandes o más pequeñas
 dependiendo del elemento y el proceso de fabricación empleado. De este modo, cualquier elemento sometido a un
 proceso de fabricación para ser comprendido en el documento puede ser "meta-caracterizable", es decir puede
 contener meta-características.

Según la presente invención ciertos parámetros se utilizan como medida de seguridad del documento que no son
 35 propiamente medidas de seguridad. Esto es, por ejemplo la diferencia en el espaciado entre caracteres, la alineación
 entre campos de texto, la intensidad de color, etc. no han sido puestos en la forma en la que están para ser medidas
 de seguridad impresas. Sumas de comprobación, la presencia del CLI, la tinta OVI, el kinegrama, etc. son elementos
 de seguridad que han sido definidos como tal. Esto dificulta el trabajo de un falsificador que puede obtener
 40 información sobre las medidas de seguridad que se han desarrollado explícitamente, pero que tiene más dificultad
 en obtener información de una medida de seguridad que no es tal, salvo que conozca las tolerancias de fabricación,
 lo cual es simplemente muy difícil.

Otra ventaja de utilizar el presente método basado en analizar meta-características es que dichas meta-
 45 características pueden ser una medida de seguridad cuyo orden de magnitud de trabajo es la micra. Las distancias
 relativas entre caracteres, o la diferencia de altura entre ellos solo pueden explicarse utilizando medidas inferiores a
 un milímetro. Esto difiere de otras medidas de seguridad cuyo orden de trabajo se basa en milímetros, o incluso
 centímetros, tales como las anteriormente mencionadas CLI, el kinegrama, etc. La precisión en la falsificación de
 texto de un documento falsificado debería ser del orden de una décima de milímetro, es sin duda una tarea muy
 50 compleja y puede ser virtualmente imposible salvo que el falsificador haya obtenido máquinas sofisticadas similares
 a aquellas utilizadas por las agencias gubernamentales.

Además, las meta-características pueden ser una medida de seguridad que controle las modificaciones más
 comunes hechas por los falsificadores. Algunas de estas son fecha de nacimiento alterada, o la suplantación por la
 55 técnica del raspado y posterior escritura de identidad falsa.

En algunos ejemplos del método de autenticación, la comparación de por lo menos un parámetro de los elementos
 detectados con por lo menos un parámetro de referencia de elementos pre-obtenidos puede comprender:
 obtener por lo menos un parámetro de referencia mediante el cálculo de por lo menos un elemento estadístico
 de por lo menos un parámetro de elementos pre-obtenidos de una pluralidad de documentos; en el que
 60 el umbral predefinido comprende el por lo menos un elemento estadístico.

El parámetro de referencia puede utilizarse como una medida de seguridad que solo puede ser determinada
 contando con una gran base de datos de documentos reales (análisis estadístico). Puede ser fácil para un
 falsificador centrarse en manipular una medida de seguridad si se puede centrar en un simple documento, por
 65 ejemplo, el suyo. Pero es ciertamente más difícil acceder a una base de datos de documentos reales para
 determinar tolerancias de fabricación.

En algunos ejemplos del método de autenticación, la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia de elementos pre-obtenidos puede comprender:

- 5 decodificar por lo menos parte de los elementos detectados para obtener un identificador único del documento;
- 5 acceder por lo menos a una base de datos de parámetros de referencia de elementos pre-obtenidos mediante el uso del identificador único obtenido del documento.

10 Utilizar el identificador único del documento y compararlo con un documento emitido con el mismo identificador unívoco (análisis de singularidad) permite reducir el umbral permisible para la validación con valores umbrales de tolerancias de fabricación mucho más inferiores.

En algunos ejemplos del método de autenticación el por lo menos un parámetro de referencia de por lo menos un elemento pre-obtenido se obtiene en o después del momento de fabricación del documento al:

- 15 detectar uno o más elementos del documento;
- 15 determinar por lo menos un parámetro de por lo menos un elemento del documento;
- 15 decodificar por lo menos parte de los elementos detectados para obtener un identificador único del documento;
- 15 almacenar el identificador único y el por lo menos un parámetro de por lo menos un elemento del documento en la base de datos como por lo menos un parámetro de referencia.

20 En algunos ejemplos del método de autenticación, el documento que se va a autenticar puede ser por ejemplo un carnet de identidad, carnet de conducir, tarjeta de crédito, débito, negocios, médica, seguros, pasaporte, tickets, etc. o cualquier otra documentación capaz de utilizarse para por ejemplo identificar por lo menos una persona o para utilizarse en transacciones tales como billetes de banco, cheques, etc. o similares.

25 En algunos ejemplos del método de autenticación, el por lo menos un elemento es por lo menos uno de: elemento de patrón y de dibujo, elemento de texto, elemento sensible a la luz, elemento sensible óptico, elemento sensible a la luz infrarroja, elemento sensible a la luz ultravioleta, elemento sensible a los campos magnéticos, elemento sensible a la temperatura.

30 La mayoría de los elementos anteriores se pueden detectar a través de una cámara de visión convencional sin necesariamente requerir alguna iluminación especial, y solo aquellos elementos sensibles a la luz infrarroja, luz ultravioleta, campos magnéticos o temperatura, requieren sensores especiales para ser detectados. Esto hace al presente método extremadamente fácil de implementar.

35 También se divulga un método de autenticación para autenticar una identidad de una persona. El método de autenticación para autenticar la identidad de una persona puede comprender:

- 35 llevar a cabo un método de autenticación para autenticar un documento de la persona tal y como se describe anteriormente, el documento siendo un documento DI;
- 35 recibir una o más primeras imágenes de la cara de la persona;
- 40 recibir una o más segundas imágenes de la cara de la persona incluidas en el documento DI mediante el procesamiento de una o más imágenes del documento DI utilizando un método de procesamiento de imagen, dichas una o más imágenes del documento DI siendo recibidas por el método de autenticación realizado para autenticar el documento DI;
- 45 determinar un indicador de similitud mediante la comparación de la una o más primeras imágenes de la cara y la una o más segundas imágenes de la cara utilizando un método de procesamiento de imagen; y
- 45 autenticar la identidad de la persona dependiendo de un resultado del método de autenticación realizado para autenticar el documento DI y si el indicador de similitud está dentro de un umbral de similitud.

50 Con el método de autenticación citado anteriormente autenticar la identidad de una persona realizando el método de autenticación anteriormente descrito para autenticar un documento DI, no se puede quebrar mostrando una foto o video del usuario (víctima) obtenida a partir de redes sociales frente al dispositivo de la cámara como las soluciones de la técnica anterior.

55 El presente método de autenticación puede ser utilizado por ejemplo:

- 55 - En banca digital como una forma de ganar nuevos clientes de forma remota. También es una forma de actualizar los datos de clientes que el banco ya tiene, por ejemplo cuando expira un carnet de identidad de un cliente.
- 60 - El punto previo puede extenderse al proceso de registro en otras entidades tales como hoteles, transporte, procedimientos notariales, etc.
- 60 - Como una forma de verificar la identidad de una persona y su documento DI por parte de autoridades de seguridad relevantes: policía, militar, seguridad privada, etc.
- 65 - Como una herramienta para controlar personas en fronteras o aeropuertos. Específicamente, podría ser una herramienta utilizada por un ABC (Sistema de control de fronteras automatizado).

En otro aspecto, se divulga un producto de programa informático. El producto de programa informático puede comprender instrucciones de programa para provocar que un sistema informático lleve a cabo un método de autenticación según algunos ejemplos divulgados en la presente memoria.

5 El producto de programa informático puede materializarse en un medio de almacenamiento (por ejemplo, un CD-ROM, un DVD, una unidad USB, en una memoria de ordenador o en una memoria de solo lectura) o portado en una señal portadora (por ejemplo, en una señal portadora eléctrica u óptica).

10 El programa informático puede estar en la forma de un código fuente, código objeto, una fuente de código intermedia y un código objeto tal como en una forma parcialmente compilada, o en cualquier otra forma adecuada para utilizar en la implementación de los procesos. El portador puede ser cualquier entidad o dispositivo capaz de portar el programa informático.

15 Por ejemplo, el portador puede comprender un medio de almacenamiento, tal como un ROM, por ejemplo un CD ROM o un semiconductor ROM, o un medio de grabación magnético, por ejemplo un disco duro. Además, el portador puede ser un portador transmisible tal como una señal eléctrica u óptica, que puede ser transmitida vía cable eléctrico u óptico o por radio u otros medios.

20 Cuando el programa informático está materializado en una señal que puede transmitirse directamente por un cable u otro dispositivo o medios, el portador puede estar constituido por dicho cable u otro dispositivo o medio.

Alternativamente, el portador puede ser un circuito integrado en el cual el programa informático está embebido, el circuito integrado estando adaptado para llevar a cabo, o para utilizar en el desempeño de los métodos relevantes.

25 BREVE DESCRIPCIÓN DE LOS DIBUJOS

Ejemplos no limitativos de la presente descripción se describirán a continuación, haciendo referencia a los dibujos adjuntos, en los cuales:

30 La figura 1 ilustra un diagrama de flujo de un método de autenticación particularmente para autenticar un documento (DI) según la presente invención.

35 La figura 2 ilustra un diagrama de flujo para comparar por lo menos un parámetro obtenido con por lo menos el mismo parámetro de referencia siguiendo un análisis estadístico.

La figura 3 ilustra un diagrama de flujo para comparar por lo menos un parámetro obtenido con por lo menos el mismo parámetro de referencia siguiendo un análisis de singularidad.

40 La figura 4 ilustra un diagrama de flujo de un método de autenticación particularmente para autenticar una identidad de una persona según la presente invención.

DESCRIPCIÓN DETALLADA DE EJEMPLOS

45 La figura 1 ilustra un diagrama de flujo de un método de autenticación particularmente para autenticar un documento (DI) 100 que puede realizarse utilizando un dispositivo con una cámara. Este dispositivo puede ser cualquier tipo de dispositivo electrónico capaz de tomar fotos tal como un teléfono móvil, una cámara (de acción), una tablet, un reloj inteligente, etc.

50 El documento puede ser por ejemplo un carnet de identidad, carnet de conducir, tarjeta de crédito, débito, negocios, médica, seguros, pasaporte, tickets, etc. o cualquier otra documentación capaz de utilizarse para identificar por lo menos una persona o incluso un billete de banco, cheque, etc. o similares. A pesar de que la presente descripción detallada se refiere a un documento DI debería entenderse que puede aplicarse a cualquier otro documento para ser autenticado. El documento DI es solo un posible ejemplo para implementar la presente invención.

55 El presente método de autenticación puede llevarse a cabo por el propio dispositivo o por el dispositivo en comunicación de datos con por lo menos un servidor. En un primer ejemplo de arquitectura el dispositivo puede ser un dispositivo móvil tal como un teléfono inteligente con una cámara o similar; esta opción es factible debido a la mejora en la capacidad del procesador y otros componentes que han sido desarrollados en los últimos años. En un
60 segundo ejemplo de arquitectura, el dispositivo podría ser un dispositivo móvil con una cámara dotada con medios para establecer una comunicación de datos con un tipo de servidor. De esta manera el dispositivo móvil podría realizar la captura y enviar datos al servidor que podría realizar computación para el dispositivo móvil, esto es, el servidor recibe los datos capturados/obtenidos. Además, el servidor también podría tener una base de datos o estar en comunicación de datos con una base de datos. Una vez los datos han sido debidamente procesados se podrían
65 enviar de vuelta al dispositivo. La comunicación entre el dispositivo y el servidor podría implementarse mediante cualquier sistema conocido en la técnica siendo sin cables o por cable.

El dispositivo podría estar dotado con por lo menos una fuente de iluminación UV, IR y/o visible y sensores de manera que los elementos en un documento DI puedan ser capturados y verificados bajo diferentes condiciones de iluminación. Dicho/s elemento/s puede/n comprender por lo menos uno de los siguientes clasificados:

- 5
 - Los elementos de patrón y dibujos pueden comprender:
 - Logo.
 - Bandera.
 - Patrones anti-escaneo.
 - Patrones de imagen de fondo.
- 10
 - Códigos de barras.
 - Ojales.
 - Remaches.
 - Huellas dactilares.
 - Guillochés.
- 15
 - Planchettes.
 - Cortes al hilo.
 - Fibras de seguridad.
 - Hilo de seguridad.
 - Marca de agua.
- 20
 - Elementos con tinta sangrante.
 - Imágenes camufladas leíbles con láser (CLR).
 - Micropartículas holográficas OVDot.
 - Laminados iridiscentes.
 - Laminados de sobreimpresión.
- 25
 - Máscara de imagen latente.
 - Imagen codificada latente.
 - Color variable en Moiré (MVC).
 - Chips.
- 30
 - Elementos de textos, dependiendo de la cantidad de los mismos, pueden comprender:
 - Carácter.
 - Palabra (grupo de caracteres).
 - Campo de texto (grupo de palabras).
- 35
 - Elementos de textos, dependiendo del tamaño de los mismos, pueden comprender:
 - Texto, visible al ojo humano, que puede comprender carácter, palabra o campo de texto.
 - Microtexto (no visible o no claramente visible al ojo humano sin ayuda) que puede comprender carácter,
- 40
 - palabra o campo de texto.
 - Nanotexto (tamaño es más pequeño que el microtexto por lo menos en 3 órdenes de magnitud) que puede comprender carácter, palabra o campo de texto.
- 45
 - Elementos sensibles a la luz (sensible a luz visible) que pueden comprender:
 - Ventana transparente.
 - Parche de elemento difractivo para dispositivo de identificación difractiva (DID).
 - Sobreimpresión de laminado brillante.
 - Imágenes de holograma.
- 50
 - Imágenes de cinegrama.
 - Imágenes retrorreflectivas.
 - Patrones con impresión de seguridad en el núcleo (SCP).
 - Imágenes de registros vistos a través.
- 55
 - Elementos sensibles ópticos (sensible a la orientación) que pueden comprender:
 - Imágenes flotantes.
 - Imágenes de holograma.
 - Imágenes de cinegrama.
- 60
 - Imagen latente de filtro (LFI).
 - Imagen latente en giro.
 - Imagen latente PEAK.
 - Imagen latente multicolor.
 - Imagen cambiante mediante láser (CLI).
- 65
 - Imagen múltiple mediante láser (MLI).
 - Elemento de identificación ópticamente variable (FEEL-ID & FUSE-ID).

- Elementos con tinta ópticamente variable (OVI).
 - Elementos con tinta magnética ópticamente variable (OVMI).
 - Imagen impresa ópticamente variable Dynaprint.
- 5
- Elementos sensibles a los infrarrojos (sensible a la luz infrarroja) que puede comprender:
- Elementos con tinta anti-stokes.
 - Números de documento con características IR.
 - Fibras de seguridad con tinta IR-fluorescente.
- 10
- Textos con tintas IR-fluorescentes.
- Elementos sensibles a los ultravioletas (sensible a la luz UV) que pueden comprender:
- Códigos de barras con tintas UV.
 - Números de documento con características UV.
 - Elementos con tinta fotocrómica.
 - HI-lites fluorescentes con luz UV.
 - Elementos con tinta fluorescente con luz UV.
- 15
- Elementos sensibles magnéticos (sensible a campos magnéticos) que pueden comprender:
- Códigos de barras con componentes ferromagnéticos.
 - Números de documento con componentes magnéticos.
- 20
- Elementos sensibles térmicos (sensible a la temperatura) que pueden comprender:
- Elementos con tinta termocrómica.
- 25

30 Los procesos de fabricación que pueden emplearse para crear documentos DI y pueden producir los elementos meta-caracterizables anteriormente mencionados pueden comprender por lo menos uno de los siguientes:

- Impresión en offset.
 - Impresión en iris.
 - Impresión Orlov.
 - Impresión tipográfica.
 - 35 • Impresión de matriz de puntos.
 - Impresión por láser (xerografía).
 - Impresión por chorro de tinta.
 - Impresión por sublimación de tinta.
 - Impresión por transferencia térmica.
 - 40 • Impresión termográfica.
 - Impresión en huecograbado.
 - Impresión serigráfica.
 - Impresión lenticular.
 - Impresión calcográfica.
 - 45 • Borrado mecánico.
 - Perforación mecánica.
 - Borrado químico.
 - Ametalización química.
 - Borrado por láser.
 - 50 • Grabado por láser.
 - Perforación por láser.
 - Ametalización por láser.
 - Estampado de folio.
 - Estampado húmedo.
 - 55 • Estampado seco.
 - Estampado ciego.
 - Litografía por haz de electrones.
 - Tecnología de trama de ranuras.
 - Fabricación aditiva.
- 60

Puede preverse cualquier otro proceso de fabricación adecuado para producir los elementos meta-caracterizables mencionados anteriormente.

65 El método de autenticación para autenticar un documento DI 100 puede comprender algunas etapas que se describirán a continuación:

- Recibir una o más imágenes del documento DI 101. El número de imágenes podría variar dependiendo de la implementación, por ejemplo una imagen del lado frontal del documento DI o una imagen de cada uno del lado frontal y el lado posterior del documento DI etc. Si el dispositivo comprende una cámara entonces la una o más imágenes se obtienen por el propio dispositivo, esto es la cámara toma fotos y las envía a los medios de procesamiento que las reciben, pero si el dispositivo comprende por ejemplo un dispositivo móvil y un servidor entonces el servidor recibe la una o más imágenes obtenidas por el dispositivo móvil. Las imágenes obtenidas pueden almacenarse en una base de datos o similares y pueden ser recibidas por los medios de procesamiento del servidor.

Según un ejemplo, para obtener la una o más imágenes del documento DI el presente método puede comprender determinar cuándo está capturando la cámara una vista completa del documento DI mediante la utilización de un método de procesamiento de imagen basado en inteligencia artificial, entrenado para detectar dicho documento DI y disparar automáticamente la cámara cuando dicho método de procesamiento determina que se muestra dicha vista completa del documento DI. Esta detección automática para documentos DI ayuda al usuario a tomar la foto necesaria bajo las mejores condiciones y eliminar el temblor producido por el movimiento de mano cuando el obturador de la cámara se acciona manualmente.

Si el servidor y el dispositivo son unidades independientes, el servidor podría enviar una instrucción para controlar la cámara del dispositivo.

Una posible solución para realizar una detección automática para documentos DI, puede hacerse por ejemplo a través de Patrón binario local (LBP) o descriptores HAAR.

Cuando se obtiene a través de la cámara la una o más imágenes del documento DI, el presente método puede comprender adicionalmente ajustar una o más condiciones de enfoque e iluminación mediante la regulación de la unidad de iluminación de la cámara. Esto puede hacerse automáticamente por el propio dispositivo con la cámara o recibir la correspondiente instrucción desde el servidor. El usuario no necesita regular las condiciones de iluminación y de enfoque.

Adicionalmente, el método puede comprender regular una unidad de enfoque de la cámara a un modo de enfoque fijado, de manera que el dispositivo pueda obtener una foto adecuadamente enfocada del documento DI.

Por lo menos alguna de la una o más imágenes del documento DI podría obtenerse teniendo en cuenta diferentes orientaciones de la cámara con respecto al documento DI. El usuario puede ser notificado por el dispositivo para cambiar la orientación del dispositivo y/o la cámara a través de cualesquier medios de aviso tales como imagen y/o sonido y/o medios de vibración. Cambiar la orientación de la cámara sobre el documento DI puede revelar elementos sensibles ópticos (sensibles a la orientación) que se han descrito anteriormente.

A fin de corregir la perspectiva del documento se podría aplicar un método de procesamiento de imagen, para tanto imágenes frontales como inclinadas, para detectar los elementos localizados en el documento en una imagen perfectamente sin distorsiones del documento. El método de procesamiento de imagen podría ser cualquiera disponible en el estado de la técnica.

Obtener la una o más imágenes del documento DI puede comprender además obtener por lo menos dos fotos del documento DI en las que por lo menos una está tomada con flash y por lo menos una está tomada sin flash para maximizar los beneficios de iluminar con el flash el documento DI (de manera tal para detectar elementos sensibles a la luz). Las por lo menos dos fotos pueden tomarse en un orden aleatorio, separado por un intervalo de tiempo aleatorio, por ejemplo inferior a 500 milisegundos que puede modificarse adecuadamente.

Para evitar el fraude (sustituir el documento DI falso con otro documento DI iluminado con flash de forma falsa), se pueden tomar y procesar las fotos casi simultáneamente evitando la sustitución del documento DI. Con el fin de afirmar que ambas imágenes pertenecen al mismo documento DI, se pueden comparar diversas características entre ellas, incluyendo texto, datos OCR y patrones.

Como una medida adicional para evitar la sustitución del documento DI entre ambas fotos, el presente método de autenticación puede comprender además generar por lo menos una señal de vídeo entre la captura de la por lo menos una foto tomada con flash y la por lo menos una foto tomada sin flash; y procesar la por lo menos una señal de vídeo utilizando un método de detección de movimiento para detectar si el documento DI ha sido sustituido entre la captura de dicha por lo menos una foto tomada con flash y dicha por lo menos puede comprender además sin flash.

Dependiendo de los requisitos de un documento DI particular, la imagen podría obtenerse teniendo en cuenta la combinación de una orientación particular de la cámara relacionada con el documento DI y el uso del flash para detectar elementos específicos.

Todo esto hace posible trabajar con una calidad de imagen suficiente para estudiar los elementos de un documento DI.

- 5 - Detectar uno o más elementos del documento DI 102 y obtener por lo menos un parámetro de los elementos detectados 103, mediante el procesamiento de las una o más imágenes obtenidas del documento DI utilizando un método de procesamiento de imagen. Esta detección puede realizarse en el propio dispositivo o en el servidor que ha recibido datos del dispositivo.

10 Un ejemplo para detectar uno o más elementos en el documento DI puede comprender realizar un método de procesamiento de imagen mediante el entrenamiento de una o más redes neuronales con un conjunto de imágenes utilizando técnicas de aprendizaje automático de tal forma que la salida de esas redes representa el por lo menos un parámetro de los elementos detectados.

15 Dado un elemento meta-caracterizable es posible obtener por lo menos una meta-característica de dicho elemento. A modo de ejemplo, se pueden citar diferentes tipos de parámetros de los elementos detectados: alineación, espaciado, anchura, altura, color, textura, exceso/defecto de material... dichas diferencias contra un modelo de referencia son las denominadas meta-características.

- 20 • La por lo menos una meta-característica puede comprender por lo menos una medida de la diferencia en el parámetro desviación de la "alineación" entre la desviación de la alineación de por lo menos dos elementos diferentes de los elementos detectados y la desviación de la alineación de los mismos por lo menos dos elementos diferentes del modelo de referencia.

25 Dada una imagen de un documento DI, es posible medir la diferencia en alineación entre dos elementos meta-caracterizables que idealmente formarían una línea recta. Esta línea recta de referencia se toma del modelo de referencia. Esta diferencia en alineación se llama "meta-alineación".

30 Hay una relación directa entre la distancia medida en píxeles y la distancia medida en micras puesto que el número de micras por píxel se pueden predeterminedar o ser previamente conocidos en base a la resolución de la cámara, por tanto podría ser posible determinar y medir una desalineación entre elementos mediante el procesamiento de la cantidad de píxeles involucrados. Se determina la posición relativa de los elementos entre cada uno de ellos y entonces se calcula la desviación relativa.

35 Por ejemplo, un carnet de identidad español 2.0 debería tener los campos de texto nombre, apellido, fecha de nacimiento y fecha de validez idealmente alineada. Sin embargo, el campo IDESP puede estar desalineado con los campos anteriores porque se ha imprimido en un proceso diferente. Por lo tanto, procesar los píxeles de la imagen capturada/obtenida puede proporcionar la información para determinar y medir la desalineación entre campos de texto de un carnet de identidad.

- 40 • La por lo menos una meta-característica puede comprender por lo menos una medición de la diferencia en el parámetro "espaciado" entre la diferencia en espacio de por lo menos dos elementos diferentes de los elementos detectados y la diferencia en espacio de los mismos por lo menos dos elementos diferentes del modelo de referencia.

45 Dada una imagen de un documento DI, es posible medir el espaciado entre dos elementos meta-caracterizables independientemente de los que sean. Esta separación se compara frente a un valor de referencia (parámetro) tomado del modelo de referencia. Por ejemplo, es posible medir la distancia entre campos de texto, la distancia entre cada carácter, la distancia entre un chip y el CLI, etc. Esta diferencia entre espaciados se denomina "meta-espaciado". Tal como se describe anteriormente puede ser posible determinar y medir un espacio mediante el procesamiento de la cantidad de píxeles involucrados. El número de micras por píxel puede conocerse previamente.

- 50 • La por lo menos una meta-característica puede comprender por lo menos una medición de la diferencia del parámetro "altura" y/o "anchura" a partir de un modelo de referencia altura y/o anchura de por lo menos uno de los elementos detectados.

55 Dada una imagen de un documento DI, es posible medir la anchura y altura de un elemento meta-caracterizable mediante el conteo y determinar los píxeles involucrados que pertenecen o no a los elemento/s. Esta anchura y altura se comparan frente a un valor de referencia (parámetro) tomado a partir del modelo de referencia. Estas diferencias en anchura/altura se denominan "meta-anchura" y "meta-altura" respectivamente. Por lo tanto, procesar los píxeles de la imagen capturada puede proporcionar la información para determinar y medir la altura y anchura de los elementos meta-caracterizables.

- 60 • La por lo menos una meta-característica puede comprender por lo menos una medición de la diferencia del parámetro "relacionado con color y/o relacionado con textura" a partir de un color-modelo y/o textura-modelo de (un parámetro de) referencia de por lo menos uno de los elementos detectados. Estas diferencias se denominan "meta-color" y "meta-textura" respectivamente.

En algunos documentos es posible definir un intervalo válido para la tinta utilizada en la impresión de algunos elementos, por ejemplo, colores de caracteres de texto. Sin embargo, trabajar con valores absolutos de colores es complicado debido a la dependencia de estos valores a la iluminación. En otros instantes, se puede definir el intervalo de colores que se utiliza en un elemento cuando se ha imprimido con un gradiente de color. Este caso es más fácil de cuantificar puesto que mide diferencias en color, tono, o intensidad en regiones específicas de la imagen. Para medir estas diferencias en color y/o textura, se pueden utilizar técnicas del estado de la técnica.

A veces, los elementos no están imprimidos sólidamente o en gradiente, pero contienen una textura específica que se ha imprimido voluntariamente o incluso involuntariamente. En el último caso, estas texturas que pueden verse en algunos elementos debido a procesos de impresión con tinta que lleva a cabo la operación de la máquina están incluidas.

- La por lo menos una meta-característica puede comprender por lo menos una medición de la diferencia de exceso/deficiencia del parámetro "material de impresión" a partir de un modelo de impresión de referencia en por lo menos uno de los elementos detectados.

El proceso de fabricación del elemento meta-caracterizable depende de la máquina utilizada y las tolerancias de este proceso. Pero también depende de otros factores que pueden influir en la tinta depositada en el papel. El proceso de absorción de tinta por el documento depende del espesor del papel, que también tiene tolerancias. La temperatura y humedad del ambiente en el momento de la impresión influyen en la velocidad de secado de la tinta. La cantidad de tinta en el depósito de la máquina impresora puede afectar el volumen de tinta expelida en el proceso de impresión. Todos estos factores resultan en impresiones únicas, donde los elementos del mismo tipo (por ejemplo dos caracteres del mismo rango, dos imágenes de patrón similar, etc.) son diferentes entre sí por exceso o defecto de tinta en estos elementos respecto al modelo de impresión de referencia.

Utilizando técnicas de procesamiento de imágenes de procesamiento de imagen, es posible evaluar estos excesos y defectos en material, de manera que pueden caracterizar cada elemento individual y singularmente, y distinguirlo de otros elementos del mismo tipo. Esta diferencia entre el modelo de impresión de referencia y el elemento real puede denominarse "meta-material". El meta-material de un elemento de imagen es una función definida en cada uno de los $n \times m$ píxeles del elemento de imagen y almacena, en cada pixel, información dependiendo de si el píxel del elemento corresponde a un exceso de material, un defecto en material o un pixel cuyo valor coincide con el modelo de impresión de referencia del elemento.

A partir de lo anterior se deriva: por ejemplo, que no hay dos caracteres "A" en un documento DI que sean iguales o que no hay dos caracteres "1" en un documento DI que sean iguales. O por lo menos, la similitud es mínima. La caracterización de un elemento del documento DI a través del exceso y defecto de tinta en relación a su modelo de impresión de referencia es una medida de seguridad para evaluar la similitud entre elementos del mismo tipo en el documento DI.

Por ejemplo, tres caracteres de valor "1" imprimidos en el mismo documento DI. El primero puede tener un exceso aparente de tinta en su lado derecho. Al segundo le puede faltar tinta en su parte superior. El tercero puede no contener defectos de material tan destacados como los dos anteriores. Por lo tanto, mediante técnicas de procesamiento de imagen, se pueden determinar y medir los excesos y defectos de tinta en relación a su modelo de impresión de referencia.

La precisión de las meta-características depende de la resolución de la cámara utilizada. Cuanto mayor es la resolución mayor es la precisión. A continuación, se presenta una tabla resumen que muestra un ejemplo de la dependencia de la precisión con la resolución:

Tamaño (mm)	1
Precisión en mediciones en píxeles	4

Resolución	MPx	Altura píxeles	Micras por píxel	Desviación detectada en micras
2048x1536	3	38	26	104
3264x2448	8	60	17	68
4032x3014	12	74	14	56
7680x4800	35	118	8	32

La tabla anterior muestra un estudio para una altura del carácter de texto de 1 mm fotografiado a diferentes resoluciones. Cuanto mayor es la resolución, menores son las micras representadas en un píxel. Si se considera que

la capacidad para detectar desviaciones mediante técnicas de procesamiento de imagen es por ejemplo 4 píxeles, entonces la máxima precisión que se puede obtener, se obtiene al multiplicar por cuatro el número de micras por píxel.

- 5 El estudio previo muestra que incluso con cámaras de resolución 3MPX se pueden detectar desviaciones mayores que aproximadamente 100 micras. Esto es una ventaja sobre otros sistemas de seguridad que son más dependientes de la resolución de la cámara.

- 10 El estudio previo fue desarrollado para una distancia dada entre la cámara y el documento DI. Si la distancia disminuye, el número de micras por píxel también disminuye, aumentando la precisión. Independientemente de la altura, la idea fundamental del estudio es mostrar la dependencia de las meta-características con la resolución de la cámara y es posible obtener buena precisión, incluso una décima de un milímetro, para cámaras de baja resolución.

- 15 - Determinar por lo menos una meta-característica 104 mediante la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia. Esta meta-característica puede adoptar cualquier valor absoluto y si no hay diferencia esa cantidad será cero. Esta determinación puede realizarse por el propio dispositivo o por el servidor que ha recibido datos del dispositivo.

- 20 - Determinar un indicador de autenticidad del documento DI 105 mediante la verificación de si por lo menos una meta-característica satisface por lo menos un umbral predefinido asociado a la por lo menos una meta-característica. Esta determinación puede realizarse por el propio dispositivo o por el servidor que ha recibido datos del dispositivo. La información que determina el indicador de autenticidad se puede enviar al dispositivo o puede estar disponible en el propio servidor. Esta información puede indicar si el documento DI es auténtico o no.

- 25 Comparar por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia podría hacerse siguiendo dos opciones diferentes (respectivamente mostradas en las figuras 2 y 3): análisis estadístico y análisis de singularidad. En cualquier caso los parámetros de referencia se han de pre-obtener a fin de calcular las meta-características medidas.

- 30 El análisis estadístico (figura 2) de un conjunto de documentos no falsificados hace posible obtener parámetros por las tolerancias de fabricación de cada elemento del documento. De este modo, para cada elemento se puede calcular por ejemplo la desviación de la alineación relativa a cualquier otro elemento, las dimensiones (anchura y altura), el espaciado con otros elementos, el color y textura, y la caracterización de exceso y defecto de material.

- 35 La media y desviación estándar (elementos estadísticos) de cada uno de los parámetros citados anteriormente (de 1 a M) de los elementos pre-obtenidos son medidas calculadas que pueden utilizarse como parámetros de referencia, por ejemplo, la media se puede denominar avg_param y la desviación estándar dev_param. Los parámetros de referencia pueden obtenerse a partir de elementos pre-obtenidos 201. El/los elemento/s estadístico/s utilizados como un/os parámetro/s de referencia puede/n comprender por lo menos uno de: media, mediana, moda, desviación estándar o la combinación de los mismos. Puede preverse cualquier otro elemento estadístico, pero en el presente ejemplo la media (o simplemente "media" a partir de ahora) y la desviación estándar se utilizarán ejemplarmente.

- 45 La cantidad predeterminada N de documentos DI no falsificados utilizados para llevar a cabo el análisis estadístico puede variar dependiendo de la precisión buscada, pero a mayor cantidad de documentos DI analizados, se obtiene más precisión. Con este análisis varios parámetros-referencia esto es de avg_param1, dev_param1 a avg_paramM, dev_paramM podrían almacenarse en una base de datos DB 202. Esta base de datos DB puede almacenarse en el propio dispositivo o en un servidor o similar.

- 50 Una vez se ha realizado el análisis estadístico, sus resultados se utilizan después como herramienta para validar la autenticidad de cualquier documento DI. Ahora, para cualquier documento DI a validar (documento DI_Y), que no se ha utilizado en el análisis estadístico, es posible calcular las meta-características de por lo menos uno de sus elementos. Esto es, es posible calcular la diferencia de por lo menos un parámetro (por ejemplo del parámetro1' al parámetroM') de por lo menos un elemento obtenido del documento DI a validar con respecto al parámetro de referencia estadísticamente inferido. La/s meta-característica/s (meta-característica1...meta-característicaM) se calculan 204 entonces mediante la comparación del por lo menos un parámetro-referencia de los elementos pre-obtenidos con por lo menos el mismo parámetro (parámetro1' to parámetroM'). Dichos parámetros se obtienen a partir del/ los elemento/s del documento DI_Y 203. Por ejemplo, el umbral predefinido asociado a la por lo menos una meta-característica utilizada para determinar un indicador de autenticidad del documento DI 105 puede ser una combinación de la media avg_param1...avg_paramM y la desviación estándar dev_param1...dev_paramM asociada a cada parámetro1...parámetroM, o por lo menos una de la media y la desviación estándar.

- 65 En la figura 3 también se ilustra una segunda y alternativa opción que se denomina análisis de singularidad. Este análisis consiste en varias etapas. Primera, se toma una foto de un documento DI (documento DI_X) como un modelo de referencia en el instante temporal t1, para obtener el/los parámetro/s de su/s elemento/s 301. Entonces, se obtiene un valor que identifica singularmente este documento DI de referencia frente otros documentos DI del mismo tipo, por ejemplo, el número de ID, un número de serie u otro valor único (identificador único) que puede estar

presente en el documento DI. Posteriormente, para cada elemento meta-caracterizable se puede calcular la alineación relativa a cualquier otro elemento, dimensiones (anchura y altura), espaciado con otros elementos, medida de color y textura y exceso y defecto de material del documento capturado en t1. Estos valores calculados se utilizan como parámetros de referencia (parámetro1 a parámetroM) y se pueden almacenar con el identificador único en una base de datos DB 302 en el propio dispositivo o en un servidor o similar. Posteriormente en un instante t2 (tras el instante t1) se realiza el mismo procedimiento descrito anteriormente, obtenido por lo menos un parámetro (del parámetro1' al parámetroM') del documento DI (documento DI_Y) a validar 303. El identificador único del documento DI a validar se decodifica a partir de los elementos detectados. Esta decodificación puede ser realizada por el propio dispositivo y/o el servidor.

El conjunto de parámetros (o uno de ellos) que se obtuvieron en los instantes temporales t1 y t2 se puede comparar (esto es una meta-característica) y verificar que son cercanos a cero y no superan cierto umbral (la meta-característica es cercana a cero).

De este modo, la comparación de por lo menos un parámetro de los parámetros obtenidos con por lo menos el mismo parámetro de referencia puede comprender:

decodificar por lo menos parte de los elementos detectados para obtener un identificador único #ID del documento DI, por ejemplo el número ID en el instante t2;

acceder por lo menos a una base de datos DB o repositorio de parámetros de referencia de elementos pre-obtenidos mediante el uso del identificador único #ID citado anteriormente del documento DI.

Tal y como se ha descrito anteriormente esa base de datos DB podría localizarse en el propio servidor o puede localizarse aparte.

Este análisis de singularidad permite determinar un indicador de autenticidad del documento DI a validar basado en si la/s meta-característica/s calculada/s (meta-característica1...meta-característicaM) 304 está/n dentro de un umbral predeterminado asociado a la/s meta-característica/s particular/es (con respecto al parámetro de referencia del documento DI capturado en t1).

Puede verse a partir de la descripción anterior que la necesidad de detectar un elemento único como el número de documento DI está motivada por la necesidad de saber frente a qué comparar. Sucede un caso cuando se realiza la fotografía del documento DI modelo en el instante temporal t1 en la comisaría en el momento de fabricación o emisión del documento. Los parámetros (alineación, espaciado...) se almacenan entonces en una base de datos (en un dispositivo y/o un servidor) junto con el número de documento DI que corresponde. Si un usuario quiere realizar el método de la presente invención con un documento DI (documento DI_Y) a validar en un instante temporal t2, una aplicación para validar su autenticidad puede tomar la foto, leer (decodificar entre los elementos) el número de DI y obtener el parámetro de referencias para ese número de DI. Entonces, se calculan las meta-características y se utilizará un umbral de autenticidad para determinar si el documento es válido.

Considerando con detenimiento tanto el análisis estadístico como el análisis de singularidad, se puede entender que en el primer análisis las diferencias en parámetros para comparar (meta-características), tienen el mismo orden que las tolerancias de fabricación. Sin embargo, en el segundo análisis, las meta-características pueden ser mucho más pequeñas que las tolerancias de fabricación, puesto que se produce la comparativa entre los parámetros de referencia en t1 y los parámetros obtenidos en t2 que caracterizan dos documentos DI con el mismo identificador único. En otras palabras, en el segundo análisis no se trata del documento leído en el instante temporal t2 que tiene una variabilidad que está limitada por tolerancias de fabricación. Es, más bien, que la variabilidad detectada es la misma que el documento leído en el instante temporal t1.

En cualquier caso el indicador de autenticidad puede asumir por ejemplo una decisión positiva sobre la autenticación del documento DI si la cantidad de la desviación asociada al parámetro (meta-característica) es inferior a o igual que un umbral pre-determinado. De otra forma, el indicador de autenticidad puede asumir por ejemplo una decisión negativa sobre la autenticación del documento DI si la cantidad de la desviación es más alta que el umbral pre-determinado.

Se pueden determinar indicadores de autenticidad adicionales del documento DI que complementan los indicadores de autenticidad calculados con el análisis de meta-características. El método de autenticación puede comprender adicionalmente entonces:

determinar por lo menos un indicador de autenticidad adicional del documento DI verificando si por lo menos una validación de autenticidad satisface por lo menos un requisito predefinido asociado a por lo menos una validación de autenticidad.

La validación de autenticidad puede comprender por lo menos uno de: validaciones lógicas de texto, validaciones de micro-escrituras, validaciones de por lo menos un elemento sensible óptico, y validaciones de por lo menos un elemento sensible a la luz o combinaciones de los mismos.

Por lo tanto la validación puede ser sobre elementos de seguridad que cambian su comportamiento con condiciones de iluminación y de inclinación. Además, se estudian micro-escrituras en este grupo. Se realizan las validaciones lógicas en realización a la información obtenida en los campos de texto OCR.

5 El ojo humano no puede detectar y leer las micro-escrituras (MW) presentes en el documento DI sin la ayuda de un cristal de aumento. Las MW se utilizan ampliamente en documentos de seguridad evidentes, ya que solo pueden obtenerse mediante técnicas de impresión de alta calidad de la industria. Es improbable que una falsificación de un documento DI pudiese tener estas micro-escrituras tan bien impresas como el documento DI original.

10 Podrían haber micro-escrituras tanto en el lado anverso como el lado reverso de los documentos DI. Se localizan todo tipo de micro-escrituras (positiva y negativa por ejemplo) en ambos lados.

A modo de ejemplo, un carnet de identidad español 2.0 tiene un kinegrama. En este kinegrama, se muestra el escudo español en color o las letras "DNI" y "ESP" que intercambian su posición dependiendo de donde ha impactado el flash. El kinegrama y la foto frontal de la cara se superponen haciendo más difícil la falsificación de la imagen y kinegrama. Tomado esto en cuenta, fotos con flash y sin flash se estudian para verificar la coherencia de la cara frontal. Además, hay varios relieves que solo se muestran cuando el flash impacta en el documento; uno tiene la palabra "ESPAÑA" escrita en él y otro tiene la palabra "DNI" repetida varias veces a lo largo de todo el borde y podría leerse con las técnicas de micro-escrituras.

20 Iluminar con flash la ventana CLI produce 3 efectos: el color del fondo cambia, el texto aparece más contrastado y se descubren varias líneas verticales. El número de líneas y la variación del color siguen ciertas normas y los caracteres en la CLI han de coincidir con la fecha de vencimiento (mediante una diferencia de años, dependiendo de la edad del portador) y la primera consonante de apellidos y nombre. Por último, pero no por ello menos importante, en la parte superior izquierda, por debajo de la bandera española, hay un texto impreso con Tinta Ópticamente Variable (OVI) que cambia de color. Iluminarla con flash produce este efecto y la correcta variación en el color se estudia para certificar la originalidad del documento.

30 Localizar los campos de interés (nombre, apellido, fecha de nacimiento...) del documento DI no es fácil debido a las tolerancias del corte de la fabricación (bordes) y elementos de impresión. Aquí, se utilizan procedimientos iterativos que en cada etapa pueden reducir el error en localizar el campo, como un método de procesamiento de imagen. Tras localizar los ítems necesarios, unos filtros adaptativos pueden ser la clave para el reconocimiento de caracteres. Un pre-procesado y limpieza adecuados pueden realizarse a fin de procesar caracteres. De nuevo, se pueden ejecutar operaciones iterativas independientemente para cada campo particular hasta que se cumplan las condiciones esperadas. Por ejemplo, limpiar el fondo, técnicas de contraste adaptativo y desenfoque y nitidez de bordes se pueden utilizar en esta etapa para leer cada región. La posición de cada carácter, de cada palabra, de cada grupo de palabras se determina para validación de documentación DI.

40 Además, el método de autenticación puede comprender procesar la una o más imágenes obtenidas del documento DI utilizando un método de Reconocimiento Óptico de Caracteres (OCR) para extraer texto en un formato de soporte informático a partir de la una o más imágenes del documento DI. A partir de este texto extraído en un formato de soporte informático se puede realizar una o más validaciones lógicas, para obtener un indicador de corrección lógica del texto. La una o más validaciones lógicas del texto extraído en formato de soporte informático puede comprender detectar palabras en el texto extraído y comparar las palabras frente a diccionario pre-definido.

45 Nombres, apellidos, etc. pueden variar mucho en longitud o en el número de palabras que los forman. La forma más sencilla de decidir si un campo leído es correcto, es compararlo frente a un diccionario. Para comparar palabras se utiliza un algoritmo basado en n-gramas. Se evalúa cada grama y la palabra con la máxima similitud métrica se selecciona como la correcta. Hay varias bases de datos cada una con un diccionario, uno para cada campo (nombre, apellido, provincia y ciudad). Estas bases de datos podrían actualizarse dinámicamente para tener en cuenta la frecuencia de aparición de las palabras y pueden estar almacenadas en el dispositivo y/o servidor y/o un repositorio vinculable a ellas. Adicionalmente, se localizan varios campos tanto en el lado anverso como en el reverso y se pueden comparar el uno con el otro. Además, también hay varias sumas lógicas en el lado reverso que se pueden utilizar para decidir cuál es la suposición correcta. Todo este trabajo previo proporciona un reconocimiento OCR casi perfecto

55 Se puede verificar si el indicador de corrección lógico del texto está dentro de un umbral de corrección lógico, el cual puede predefinirse para cada caso. Esta verificación se hace para determinar el indicador de autenticidad del documento DI.

60 Si el documento DI comprende un chip que contiene datos, el presente método de autenticación puede comprender adicionalmente recibir u obtener dichos datos a partir del o con el propio dispositivo si dicho dispositivo es capaz de comunicarse. Alternativamente, el dispositivo o el servidor puede estar en comunicación de datos con un lector para recuperar datos del chip. Estos datos almacenados en el chip pueden comprender por lo menos unos de datos de texto, datos de imagen, datos de huella dactilar, datos de firma, datos biométricos y todos los datos leíbles mediante OCR entre otra información valiosa. Los datos obtenidos a partir del documento DI utilizando métodos de procesado

de la imagen se pueden comparar con por lo menos un dato almacenado en el chip y entonces determinar el indicador de autenticidad adicional del documento DI.

5 Cabría señalar que la tecnología de Comunicación por Campos Cercanos (NFC) es solo un ejemplo no limitativo para comunicar datos pre-grabados en el documento DI. Se podría utilizar una tecnología basada en RFID o cualquier otra tecnología inalámbrica.

10 Adicionalmente, se puede llevar a cabo un método de autenticación para autenticar una identidad de una persona 400. La figura 4 ilustra un diagrama de flujo del mismo. Tal y como se menciona anteriormente el presente método de autenticación puede llevarse a cabo por el propio dispositivo que tenga una cámara o por el dispositivo en comunicación de datos con por lo menos un servidor.

Este método de autenticación para autenticar una identidad de una persona puede comprender:

15 - Realizar un método de autenticación para autenticar un documento DI 100 de la persona tal como se describe anteriormente.

20 - Recibir u obtener a través de la cámara, una o más primeras imágenes de la cara de la persona 401. Por ejemplo, recibir u obtener estas imágenes puede comprender una foto o vídeo de la cara de la persona. Si se recibe u obtiene un video de la cara, el método también puede comprender obtener un campo de profundidad o campo 3D de las imágenes de la cara de la persona mediante el procesado del vídeo de la cara de la persona recibido/obtenido utilizando un método de procesamiento de imagen. Esta forma de gestionar la cámara es la misma que se describe anteriormente.

25 Adicionalmente, recibir u obtener la una o más primeras imágenes de la cara de la persona puede comprender determinar cuando la cámara está pre-capturando una vista completa de la cara de la persona mediante la utilización de un método de procesamiento de imagen, y disparar automáticamente la cámara cuando se determina que la cámara está pre-capturando dicha vista completa de la cara de la persona.

30 - Recibir u obtener una o más segundas imágenes de la cara de la persona incluidas en el documento DI 402 mediante el procesado de una o más imágenes del documento DI utilizando un método de procesamiento de imagen, dichas una o más imágenes del documento DI siendo recibidas u obtenidas por el método de autenticación llevado a cabo para autenticar el documento DI;

35 - Determinar un indicador de similitud 403 mediante la comparación de la una o más primeras imágenes de la cara y la una o más segundas imágenes de la cara utilizando un método de procesamiento de imagen. Por ejemplo, el indicador de similitud puede determinarse sobre la base de un porcentaje de similitud entre dos imágenes.

40 - Autenticar la identidad de la persona 404 dependiendo de un resultado del método de autenticación realizado para autenticar el documento DI y si el indicador de similitud determinado está dentro de un umbral de similitud. Este umbral puede modificarse adecuadamente a un valor predeterminado.

45 La idea principal para validar la persona es comparar por ejemplo una foto validada de la cara con otra foto no validada de la cara. Entonces se calcula un indicador de similitud. Si el indicador de similitud es mayor que un umbral, entonces la foto no validada se valida. Como consecuencia, el método de validación de la persona es correcto. La validación de la persona, como una parte del proceso de autenticación, necesita una foto validada de la cara. Si el proceso de validación del documento DI es correcto, entonces la foto de la cara imprimida en el documento debe ser correcta, y por ejemplo una foto "selfie" tomada por el dispositivo podría utilizarse para
50 comparar la cara del portador/propietario con la foto validada de la cara del documento DI.

55 Cuando el documento DI comprende un chip de memoria que contiene datos de imagen accesibles mediante comunicación inalámbrica y el dispositivo comprende funcionalidades para establecer una comunicación de datos con el chip de memoria (por ejemplo NFC), el método de autenticación, particularmente para validar la persona, puede comprender además obtener o recibir (desde una fuente externa) una o más terceras imágenes de la cara de la persona a partir del chip del documento DI a través de una comunicación NFC entre el dispositivo y el chip.

60 Tal como se menciona anteriormente, la tecnología NFC es solo un posible ejemplo para almacenar datos pre-grabados en el documento DI. Cualquier otra tecnología se podría utilizar como un protocolo basado en RFID.

En este ejemplo determinar el indicador de similitud comprende además comparar la una o más terceras imágenes de la cara de la persona con la una o más primeras imágenes de la cara de la persona y/o la una o más segundas imágenes de la cara de la persona utilizando el método de procesamiento de imagen.

65 A pesar de que solo se han descrito un número de ejemplos en la presente memoria, también son posibles otras alternativas, modificaciones, usos y/o equivalentes de los mismos. Además, también están cubiertas todas las

posibles combinaciones de los ejemplos descritos. De este modo, el ámbito de la presente divulgación no debería estar limitada por ejemplo particulares, sino que debería determinarse solo a través de una lectura adecuada de las reivindicaciones que siguen a continuación. Si en una reivindicación hay referencias numéricas entre paréntesis relacionadas con los dibujos, son solo para incrementar la inteligibilidad de la reivindicación, y no deberán interpretarse como limitantes del ámbito de la reivindicación.

Además, a pesar de que los ejemplos descritos con referencia a los dibujos comprenden aparatos/sistemas/dispositivos informáticos y procesos realizados en aparatos/sistemas/dispositivos informáticos, la invención también se extiende a programas informáticos, concretamente programas informáticos sobre o en un portador, adaptado para poner el sistema en práctica.

La invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de autenticación para autenticar un documento comprendiendo:
recibir (101) una o más imágenes obtenidas del documento;
5 detectar (102) uno o más elementos del documento;
obtener (103) por lo menos un parámetro de los elementos detectados, mediante el procesado de la una o más imágenes obtenidas del documento utilizando un método de procesamiento de imagen;
determinar (104) por lo menos una meta-característica mediante la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia de uno o más elementos pre-obtenidos;
10 determinar (105) un indicador de autenticidad del documento mediante la verificación de si la por lo menos una meta-característica satisface por lo menos un umbral predefinido asociado a la por lo menos una meta-característica, en el que
una meta-característica es por lo menos una medición de una diferencia de por lo menos un parámetro de un elemento detectado relativo a por lo menos un parámetro de referencia de por lo menos un modelo de referencia; el
15 modelo de referencia comprendiendo el uno o más elementos pre-obtenidos.
2. Un método de autenticación según la reivindicación 1, en el que la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia de elementos pre-obtenidos comprende:
obtener por lo menos un parámetro de referencia mediante el cálculo de por lo menos un elemento estadístico
20 de por lo menos un parámetro de los elementos pre-obtenidos de una pluralidad de documentos; en el que el umbral predefinido comprende el por lo menos un elemento estadístico.
3. Un método de autenticación según la reivindicación 1, en el que la comparación de por lo menos un parámetro de los elementos detectados con por lo menos un parámetro de referencia de elementos pre-obtenidos comprende:
25 decodificar por lo menos parte de los elementos detectados para obtener un identificador único del documento;
acceder por lo menos a una base de datos de parámetros de referencia de elementos pre-obtenidos mediante la utilización del identificador único obtenido del documento.
4. Un método de autenticación según la reivindicación 3, en el que el por lo menos un parámetro de referencia de
30 por lo menos un elemento pre-obtenido se obtiene en o después del momento de fabricación o emisión del documento al:
detectar uno o más elementos del documento;
determinar por lo menos un parámetro de por lo menos un elemento del documento;
decodificar por lo menos parte de los elementos detectados para obtener un identificador único del documento;
35 almacenar el identificador único y el por lo menos un parámetro de por lo menos un elemento del documento en la base de datos como por lo menos un parámetro de referencia.
5. Un método de autenticación según cualquiera de las reivindicaciones 1 a 4, en el que la por lo menos una meta-característica comprende por lo menos una de:
40 por lo menos una medición de una diferencia en un parámetro de desviación de alineación entre la desviación de alineación de por lo menos dos elementos diferentes de los elementos detectados y la desviación de alineación de los mismos por lo menos dos elementos diferentes del modelo de referencia;
por lo menos una medición de una diferencia en un parámetro de espaciado entre la diferencia en espacio de por lo menos dos elementos diferentes de los elementos detectados y la diferencia en espacio de los mismos por lo
45 menos dos elementos diferentes del modelo de referencia;
por lo menos una medición de una diferencia en un parámetro de altura entre por lo menos un elemento detectado y el mismo por lo menos un elemento del modelo de referencia;
por lo menos una medición de una diferencia en un parámetro de anchura entre por lo menos un elemento detectado y el mismo por lo menos un elemento del modelo de referencia;
50 por lo menos una medición de una diferencia en un parámetro de color entre por lo menos un elemento detectado y el mismo por lo menos un elemento del modelo de referencia; o
por lo menos una medición de una diferencia en un parámetro de textura entre por lo menos un elemento detectado y el mismo por lo menos un elemento del modelo de referencia.
- 55 6. Un método de autenticación según cualquiera de las reivindicaciones 1 a 5, en el que el por lo menos una meta-característica comprende por lo menos una medición de una diferencia en un parámetro de exceso o deficiencia de material de impresión entre por lo menos un elemento detectado y el mismo por lo menos un elemento del modelo de referencia.
- 60 7. Un método de autenticación según cualquiera de las reivindicaciones 1 a 6, en el que el por lo menos un elemento es por lo menos uno de: elemento patrón y dibujo, elemento de texto, elemento sensible a la luz, elemento sensible óptico, elemento sensible a los infrarrojos, elemento sensible a los ultravioleta, elemento sensible magnético, elemento sensible térmico.
- 65 8. Un método de autenticación según cualquiera de las reivindicaciones 1 a 7, en el que la una o más imágenes del documento se obtienen mediante una cámara y el método de autenticación comprende además:

determinar cuándo está capturando la cámara una vista completa del documento mediante la utilización del método de procesamiento de imagen basado en inteligencia artificial, entrenado para detectar dicho documento DI, y disparar automáticamente la cámara cuando el método de procesamiento de imagen determina que dicha vista completa del documento está representada.

5 9. Un método de autenticación según la reivindicación 8, en el que el método de autenticación comprende además ajustar una o más condiciones de enfoque e iluminación mediante la regulación de la iluminación de la cámara.

10 10. Un método de autenticación según las reivindicaciones 7 y 9, en el que las una o más imágenes obtenidas del documento son por lo menos dos fotos del documento en el que por lo menos una está tomada con flash y por lo menos una está tomada sin flash de tal forma para detectar elementos sensibles a la luz, las por lo menos dos fotos estando tomadas en orden aleatorio, separadas por un intervalo de tiempo aleatorio.

15 11. Un método de autenticación según cualquiera de las reivindicaciones 1 a 10, en el que el método de autenticación comprende además:
determinar por lo menos un indicador de autenticidad adicional del documento mediante la verificación de si por lo menos una validación de autenticidad satisface por lo menos un requisito predefinido asociado con la por lo menos una validación de autenticidad.

20 12. Un método de autenticación según la reivindicación 11, en el que el documento comprende un chip que contiene datos, el método de autenticación comprendiendo:
recibir datos almacenados del chip;
comparar los datos recibidos del documento con por lo menos un dato almacenado en el chip; y
25 determinar un indicador de autenticidad adicional del documento.

13. Un método de autenticación para autenticar una identidad de una persona comprendiendo:
llevar a cabo un método de autenticación para autenticar un documento de la persona según cualquiera de las reivindicaciones 1 a 12, el documento siendo un documento DI;
30 recibir una o más primeras imágenes de la cara de la persona;
recibir una o más segundas imágenes de la cara de la persona incluidas en el documento DI mediante el procesado de una o más imágenes del documento DI utilizando un método de procesamiento de imagen, dichas una o más imágenes del documento DI siendo recibidas por el método de autenticación realizado para autenticar el documento DI;
35 determinar un indicador de similitud mediante la comparación de la una o más primeras imágenes de la cara y la una o más segundas imágenes de la cara utilizando un método de procesamiento de imagen; y
autenticar la identidad de la persona dependiendo de un resultado del método de autenticación realizado para autenticar el documento DI y si el indicador de similitud está dentro de un umbral de similitud.

40 14. Un método de autenticación según la reivindicación 13, en el que el documento DI comprende un chip de memoria que contiene datos de imagen, el método de autenticación comprendiendo:
recibir una o más terceras imágenes de la cara de la persona a partir del chip del documento DI.
determinar el indicador de similitud comprende además comparar la una o más terceras imágenes de la cara de la persona con la una o más primeras imágenes de la cara de la persona y/o la una o más segundas imágenes de la cara de la persona utilizando el método de procesamiento de imagen.

15. Un dispositivo informático comprendiendo una memoria y un procesador, instrucciones de materialización almacenadas en la memoria y ejecutables por el procesador, las instrucciones comprendiendo funcionalidad para ejecutar un método de autenticación según cualquiera de las reivindicaciones 1 a 14.

50

Fig.1

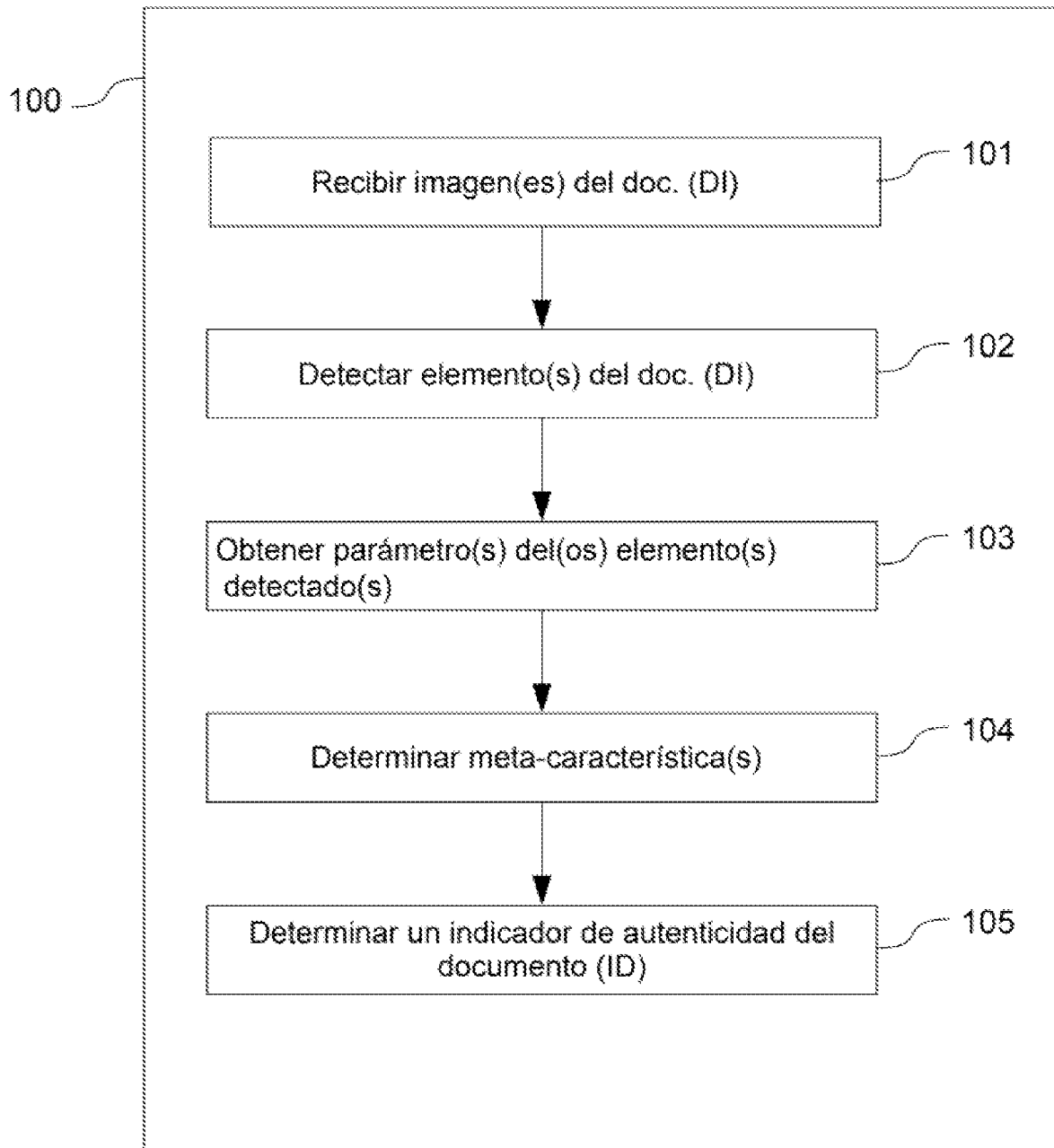


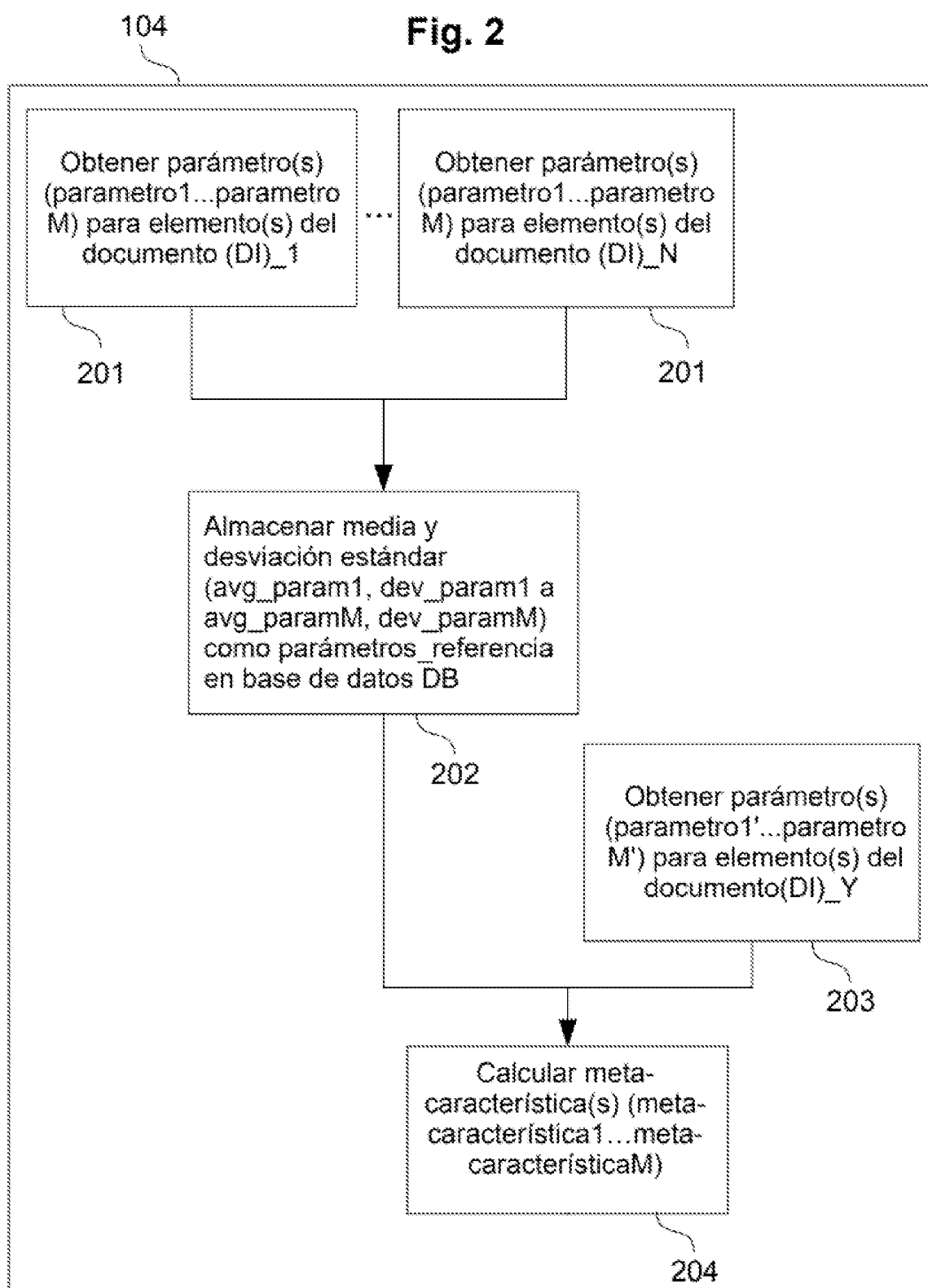
Fig. 2

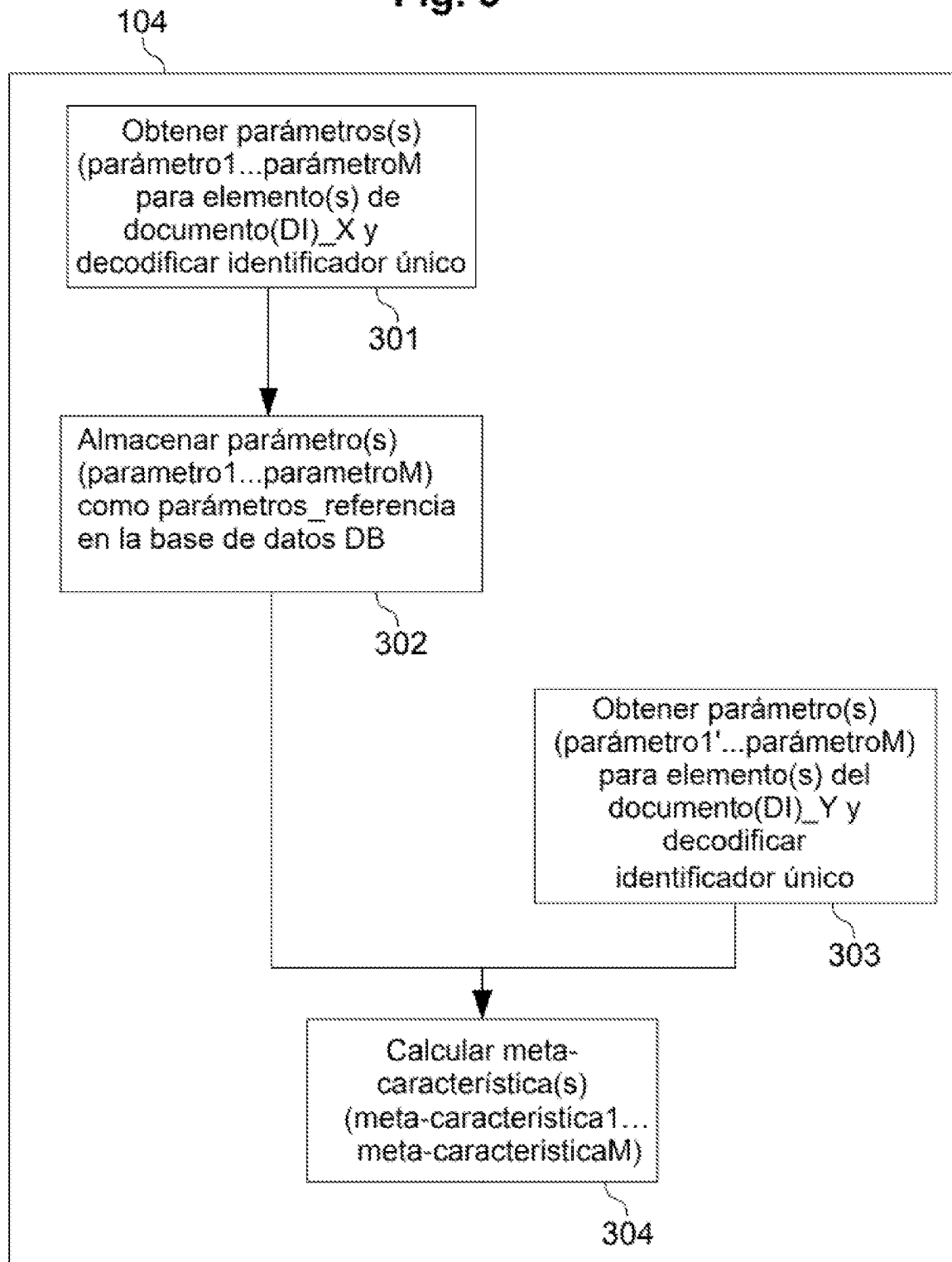
Fig. 3

Fig. 4