

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 651 341**

51 Int. Cl.:

B42D 15/00 (2006.01)
G06K 19/08 (2006.01)
G06K 19/10 (2006.01)
H04N 1/32 (2006.01)
B42D 25/00 (2014.01)
B42D 25/23 (2014.01)
B42D 25/309 (2014.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **09.11.2010** **PCT/EP2010/067122**
87 Fecha y número de publicación internacional: **19.05.2011** **WO11058012**
96 Fecha de presentación y número de la solicitud europea: **09.11.2010** **E 10779525 (4)**
97 Fecha y número de publicación de la concesión europea: **05.07.2017** **EP 2499000**

54 Título: **Documento de identidad que incorpora una fotografía de identidad protegido mediante motivos**

30 Prioridad:

12.11.2009 EP 09306087

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2018

73 Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

72 Inventor/es:

DIDELOT, FLORIAN

74 Agente/Representante:

CASANOVAS CASSA, Buenaventura

ES 2 651 341 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 identidad que incorpora una fotografía de identidad protegido mediante motivos.

- 5 La invención se refiere a los documentos de identidad, y en particular la protección de documentos de identidad, tales como carnets de identidad, permisos de conducir o pasaportes, contra la alteración o la fabricación fraudulenta.
- 10 Los documentos de identidad comprenden generalmente una fotografía de identidad de su propietario. Los documentos de identidad también incluyen una serie de entradas alfanuméricas, como el nombre del titular, fecha de nacimiento, altura, dirección, número de documento, fecha de emisión del documento o la identidad de la autoridad que emitió el documento.
- 15 Las fotografías de identidad con frecuencia incluyen guilloses o sobreimpresiones. Estos guilloses forman una red de líneas superpuestas a la fotografía y visible a simple vista. Los guilloses tienen el objeto de hacer perceptible durante una verificación de identidad cualquier modificación fraudulenta de la fotografía. Los guilloses permiten, en particular, proteger contra las modificaciones de la tinta de la fotografía, por ejemplo, cuando se añade una barba o cabello. Por lo tanto, los guilloses permiten implementar de forma flexible controles de seguridad nivel 1 (inspección visual a simple vista) o nivel 2 (inspección visual con un aparato óptico simple tal como una lente de aumento o una lámpara ultravioleta).
- 20 Los guilloses aportan un complemento de seguridad frente a las modificaciones de la imagen y no aportan protección contra las alteraciones de entradas alfanuméricas, para los que se implementan en general otros sistemas de protección de documentos de identidad.
- 25 Las técnicas de marca de agua digital (designadas por el término "watermarking" en Inglés) están diseñados para integrar elementos invisibles a simple vista en una fotografía de pasaporte, estos elementos codifican información predefinida. La marca de agua digital proporciona un nivel de seguridad 3 en una inspección. Por lo tanto, por medio de un equipo de procesamiento y análisis numérico, se analiza la fotografía de identidad para extrapolar los datos que le son impresos. A continuación se realiza una comprobación de la consistencia de estos datos.
- 30 En la práctica, la marca de agua digital tiene un cierto número de inconvenientes. En primer lugar, la marca de agua digital no permite implementar un nivel de seguridad 1 o 2, lo que limita los controles de seguridad del personal con importantes recursos, lo que es delicado por ejemplo para los controles móviles. Por otro lado, la decodificación de la marca de agua digital implica la realización de un gran número de cálculos basados en las transformaciones de Fourier. Estos cálculos son relativamente largos y complejos, haciendo que el proceso de verificación de identidad resulte excesivamente largo. Además, las marcas de agua digitales pueden ser sensibles a la degradación del documento de identidad, daños que pueden ser causados por una falta de atención por parte del titular durante el periodo relativamente largo de validez del documento. El análisis de las marcas de agua digitales degradadas puede conducir entonces a una lectura errónea de las marcas, o incluso a la imposibilidad de lectura durante el control. El control de seguridad deberá entonces recaer sobre otros elementos de autenticación, eliminando inmediatamente la utilidad de la marca de agua digital.
- 35 Los documentos US6095566, US2005/109846, US2005/072846, EP1318486, EP1684494 y GB2451482 forman parte del estado de la técnica.
- 40 La invención tiene como objetivo resolver una o más de estas desventajas. La invención se refiere por tanto a un procedimiento de protección de un documento de identidad que incluye una fotografía de identidad y entradas alfanuméricas relativas al titular del documento de identidad, que comprende las etapas de:
- 45
- 50 - recolección de informaciones alfanuméricas entre las entradas alfanuméricas destinadas a figurar en el documento de identidad;
 - codificar las informaciones alfanuméricas recogidas por propiedades de motivos destinados a figurar en zonas predeterminadas de la fotografía de identidad, siendo los motivos susceptibles de revelar una eventual alteración de la fotografía de identidad;
 - 55 - realizar el documento de identidad de modo que comprenda dichas entradas alfanuméricas, y de manera que incluya una fotografía de identidad sobre la cual figuren de manera visible los motivos con dichas propiedades en dichas zonas predeterminadas.
- 60 La invención se caracteriza por motivos compuestos por líneas superpuestas con la fotografía de identidad y que presentan intersecciones de las líneas, y porque dichas informaciones alfanuméricas recogidas están codificadas por la presencia y la no presencia de intersecciones de motivos en dichas zonas predeterminadas.

Según otra variante, los motivos impresos en la fotografía de identidad son visibles a simple vista.

Según otra variante, el procedimiento comprende el análisis de los colores o la intensidad de las zonas predeterminadas de la fotografía de identidad, y comprende la realización de los motivos con un contraste de color o de intensidad en comparación con la fotografía de identidad en las áreas predeterminadas.

5 Según otra variante, el documento de identidad incorpora un chip, comprendiendo el procedimiento una etapa de escritura de entradas alfanuméricas, de informaciones alfanuméricas recogidas, de la ubicación de las zonas predeterminadas y/o de la fotografía de identidad en el chip.

10 Según aún otra variante, la etapa de codificación de las propiedades de los motivos está precedida de una etapa de cifrado de la información recogida.

Según una variante, las zonas predeterminadas de la fotografía de identidad presentan una densidad variable en diferentes ubicaciones de la fotografía de identidad.

15 Según otra variante, las zonas predeterminadas presentan una densidad menor a nivel de los ojos de la fotografía de identidad.

Según otra variante, el procedimiento comprende las etapas de:

20 - analizar numéricamente la fotografía de identidad para extraer estadísticas de imagen;
- codificar en algunas de las áreas predeterminadas las estadísticas de imagen extraídas por las propiedades de los motivos.

25 La invención también se refiere a un sistema de comprobación de autenticidad de un documento de identidad, que comprende:

30 - un dispositivo de captura digital de imágenes;
- un módulo de procesamiento adaptado para determinar informaciones alfanuméricas en una imagen captada y capaz de identificar las propiedades de los motivos en las áreas predeterminadas de una imagen capturada, siendo los motivos susceptibles de revelar una eventual alteración de la fotografía de identidad;
- un módulo de autenticación, indicando al módulo de procesamiento las áreas predeterminadas a analizar para la identificación de las propiedades de los motivos en estas áreas, decodificando la información codificada por las propiedades de tales motivos, comparando la información de la imagen capturada con la información decodificada, y generar una señal representativa de la autenticidad en función del resultado de la comparación.

35 Según una variante, el sistema comprende además un dispositivo de lectura de un chip del documento de identidad, comparando el módulo de autenticación la información decodificada con la información almacenada en el chip y generando una señal representativa de la autenticidad en función del resultado de esta comparación.

40 La invención también se refiere a un documento de identidad realizado siguiendo el procedimiento antedicho. Otras características y ventajas de la invención se extraerán claramente de la descripción que se ofrece a continuación, a título indicativo y no limitativo, en referencia a los dibujos adjuntos, en los que:

45 - la figura 1 es una representación esquemática de un documento de identidad según la invención;
- la figura 2 representa una matriz de puntos de intersección de motivos para la codificación de la información alfanumérica;
- la figura 3 representa esquemáticamente un ejemplo de procedimiento de edición de una fotografía de identidad que codifica la información digital por medio de motivos;
- las figuras 4 a 6 representan diferentes variantes de trazados de motivos;
50 - la figura 7 representa un ejemplo de procedimiento de fabricación de una tarjeta según la invención;
- la figura 8 representa un ejemplo de procedimiento de comprobación de la autenticidad del documento de identidad;
- la figura 9 representa un sistema de verificación de la autenticidad de un documento de identidad.

55 La figura 1 representa un ejemplo del documento de identidad 1 según una realización de la invención. El documento de identidad 1 comprende un soporte 7, hecho de material sintético, material fibroso o una combinación de material sintético y material fibroso. El documento de identidad 1 incorpora una fotografía de identidad 3 de su titular. El documento de identidad 1 también incluye informaciones alfanuméricas de personalización 4 visibles, tales como el nombre y apellido del titular, su fecha de nacimiento o el número del documento de identidad. El documento de identidad 1 también incluye la firma 5 de su titular. Ventajosamente, un chip 2 también puede ser fijado en o sobre el soporte 7 de manera conocida. El chip comprende típicamente un microcontrolador provisto de una interfaz de comunicación, de un procesador de tratamiento, de una memoria no volátil y de una memoria RAM. Los motivos 6 visibles están presentes en la fotografía de identidad 3. Los motivos 6 forman en este caso los guilloses. Los guilloses 6 se realizan ventajosamente en la fotografía de identidad 3 de modo que toda tentativa de modificación de los motivos provoque un deterioro en la apariencia de esta fotografía 3. Los motivos 6 son por tanto susceptibles de revelar una alteración eventual del aspecto de la fotografía de identidad.

La figura 2 muestra una parrilla o matriz 61 que define un conjunto de áreas puntuales o áreas de codificación 62 en las que las propiedades de los motivos codifican la información de las informaciones alfanuméricas 4 de codificación. Las áreas 62 se encuentran en posiciones predefinidas, en las intersecciones de un entramado rectangular en el ejemplo ilustrado. Las propiedades de los motivos en las zonas puntuales 62 permiten codificar la información alfanumérica recogida de las entradas alfanuméricas 4. En el ejemplo detallado a continuación, las propiedades de los motivos 6 en calidad de codificación de la información alfanumérica serán la presencia o no de una intersección entre las líneas de motivos en las zonas puntuales 62.

La figura 3 proporciona un ejemplo simplificado de un proceso que conduce a la formación de motivos 6 en la fotografía de identidad 3 del documento de identidad 1. En una primera etapa, se selecciona el nombre 41 del titular entre las entradas alfanuméricas 4. Se codifica el nombre 41 del titular para formar un código binario 42 en un número de bits predefinido. Cada bit del código 42 corresponde a una zona puntual 62 de la parrilla 61. Se genera una matriz de puntos de intersección 63 conservando las zonas de puntos 62 que definen los puntos de intersección de las líneas de los motivos. Un valor 1 de la código binario 42 será codificado por un punto de intersección 63 en un área puntual 62 asociada, mientras que un valor 0 del código binario 42 será codificado por la ausencia de puntos de intersección la zona puntual 62 asociada. Seguidamente, se trazan líneas de motivos 64, de modo que se cruzan varias líneas 64 en los puntos de intersección 63, y de modo que a lo sumo una línea pase por cada zona puntual 62 desprovista del punto de intersección 63. En el ejemplo ilustrado, las líneas 64 son rectilíneas. Las líneas de los motivos 6 de podrán trazar por ejemplo de forma conocida mediante un método de triangulación Delaunay entre los puntos de intersección 63. Los motivos 6 generados son entonces superpuestos en la fotografía de identidad 3. Los motivos 6 se pueden superponer en la fotografía de identidad 3 en forma digital, antes de fijar la fotografía de identidad 3 transformada en el soporte 7. Cuando los motivos 6 se añaden a la fotografía de identidad 3 antes de su transferencia al soporte 7, el coste adicional de dicha protección adicional es extremadamente reducido. También se puede considerar vincular los motivos formados por cualquier medio adecuado a una fotografía de identidad 3 ya impresa en el soporte 7.

El uso de motivos 6 para codificar información de las entradas alfanuméricas 4 permite realizar una comprobación de autenticidad en un lapso de tiempo reducido. Por ejemplo, la identificación de las intersecciones de las líneas 64 en las áreas predeterminadas permitirá comparar los datos codificados en los motivos 6 con las entradas alfanuméricas 4 simplemente en base a la captura digital de la fotografía de identidad 3 seguida de su tratamiento de la imagen, como se detalla a continuación. Si hay inconsistencia entre los datos extraídos de la fotografía de identidad 3 y las entradas alfanuméricas 4, se podrá deducir una alteración o una fabricación fraudulenta del documento de identidad 1.

Para reforzar aún más la seguridad de dicha documento de identidad 1, también es posible codificar otras informaciones por medio de los motivos 6. Se puede considerar principalmente codificar información estadística concerniente a la fotografía de identidad, con el fin de poder identificar las tentativas de fraude por adición o supresión de detalles presentes entre los motivos, por ejemplo un lunar, induciendo entonces una alteración de las estadísticas de la fotografía. La información estadística puede por ejemplo referirse a una caracterización textural o espectral de la fotografía de identidad 3.

Diferentes entradas alfanuméricas se pueden recoger para ser codificadas mediante motivos en la fotografía de identidad 3. Las entradas alfanuméricas recogidas para ser codificadas pueden ser fragmentos de diferentes campos de información. Por ejemplo, se podrá recopilar un cierto número de caracteres del nombre, caracteres del apellido, caracteres del número de del documento de identidad y/o caracteres de la fecha o del lugar de nacimiento del titular.

Con el fin de aumentar la fuerza y la velocidad de procesamiento de la información alfanumérica codificada en los motivos 6 en una autenticación, la matriz 61 podrá incluir un número reducido de bits, por ejemplo del orden de 160 bits.

Además, el chip 2 está preferiblemente protegido y almacena las entradas alfanuméricas 4. Así, el chip 2 permite verificar que las informaciones alfanuméricas 4 o los motivos 6 no han sido fraudulentamente alterados, lo que confiere al chip el rol de doble verificador. Tampoco resulta necesario almacenar la fotografía de identidad desprovista de los motivos 6 en el chip 2 para proceder a la decodificación de la información alfanumérica codificada en la fotografía 3.

El uso de motivos visibles permite realizar una comprobación de la autenticidad incluso cuando la lectura del chip 2 resulta imposible. Por ejemplo, en caso de desactivación o deterioro involuntario del chip 2 del documento de identidad 1, las autoridades podrán aceptar contentarse con el decodificado de los motivos 6 presentes en la fotografía de identidad 3. Ventajosamente, el uso de motivos visibles a simple vista desalienta los intentos simples de fraude y permite una comprobación de autenticación visual, incluso en ausencia de equipos de análisis de la fotografía de identidad. Además, los motivos 6 visibles a simple vista no proporcionan una decodificación particularmente resistente al desgaste del documento de identidad 1, que no siempre se guarda en condiciones óptimas de conservación para permanecer utilizable por un período de validez a veces muy largo.

Las intersecciones de los motivos 6 se contrastan de forma ventajosa con respecto a la fotografía de identidad 3, con el fin de permanecer analizable después de una captación y un procesamiento digital. Los motivos 6 podrán así presentar un contraste de color o una diferencia de luminosidad significativa con respecto a la fotografía de identidad en las intersecciones en las áreas de codificación predeterminadas. Este contraste también hace que la autenticación sea más resistente frente a eventuales alteraciones del documento de identidad 1.

En los ejemplos ilustrados en las figuras 4 a 6, los círculos ennegrecidos identifican las áreas predeterminadas que codifican un primer valor binario, los círculos sin rellenar identifican un segundo valor binario. Estos círculos no se transcriben en los motivos presentes en la fotografía de identidad 3. Estos círculos se muestran sólo para facilitar la lectura de las figuras y permitir la visualización de la codificación realizada por medio de las líneas 64.

En el ejemplo de la figura 4, las líneas 64 que forman los motivos 6 no son rectilíneas. Tales líneas 64 hacen que sea más difícil la identificación de las intersecciones consideradas para la codificación por un falsificador potencial. Las líneas 64 también pueden tener curvaturas características, por ejemplo sinusoidales, que permitan discriminar motivos falsificados en un control de nivel 1 o 2.

En el ejemplo de la figura 5, la matriz que define las áreas de intersección tomadas en cuenta para la codificación se ha sufrido una deformación por esferización con respecto a la matriz de la figura 2. Dicha deformación puede usarse ventajosamente para reducir la densidad de líneas en ciertas áreas de la fotografía que deban permanecer poco alteradas para reconocer al titular del documento 1. Así, se podrá reducir la densidad de las líneas de los motivos 6 en la nariz o los ojos del usuario. En el ejemplo de la figura 6, la matriz que define las áreas de intersección tomadas en cuenta para la codificación sufrió una deformación en espiral con respecto a la matriz de la figura 2.

La figura 7 detalla un ejemplo de procedimiento de fabricación de acuerdo con la invención, implementada en la etapa de personalización de un documento de identidad 1. En la etapa 101, se recoge información alfanumérica en las entradas alfanuméricas 4 destinadas a figurar en el documento de identidad 1. La información alfanumérica recogida se escoge entre las entradas alfanuméricas 4 según reglas reproductibles, de manera que la autenticación se puede implementar más tarde. Las informaciones recogidas son obtenidas a continuación en forma digital en una etapa 102, para ser sometidas a un procesamiento digital.

En la etapa 103, la informaciones recogidas están sujetas a una función resumen para generar una secuencia binaria. La función resumen permite generar una secuencia binaria de un tamaño predefinido. Por lo tanto, incluso si la información recogida es relativamente larga, la secuencia binaria generada tendrá el tamaño adecuado para su codificación por una matriz 61. Una función resumen también permite cifrar la informaciones recogidas.

En la etapa 104, la secuencia binaria hace las veces de un procedimiento de cifrado, de una manera conocida. El cifrado genera una secuencia binaria cifrada. La capacidad de un falsificador para determinar cómo codificar en la fotografía las entradas alfanuméricas que quiere imprimir en la tarjeta, se reduce. En la etapa 105, la secuencia binaria cifrada se transforma en una matriz de puntos de intersección 63, como se muestra en la figura 3. En una etapa 106, se procede al trazado de las líneas de motivos de manera que forman las intersecciones en los puntos 63. El rastreo se realiza de modo que las otras zonas de puntos 62 de la matriz no contienen intersecciones de líneas de motivos.

En una etapa 107, se realiza una deformación de los motivos y de las áreas de codificación predeterminadas, como se detalla en el ejemplo de las figuras 5 y 6. La densidad de las zonas de codificación podrá de este modo reducirse en las zonas de la fotografía de identidad que presentan detalles no alterables. En la etapa 108, la intensidad o el color de los motivos se adapta en función de la fotografía de identidad en la que han de ser superpuestos. Se genera así un contraste visual suficiente de los motivos con respecto a la fotografía. Una línea de motivo será clara por ejemplo en una zona oscura de la fotografía.

En una etapa 109, se genera una imagen mediante la superposición de los motivos de la fotografía de identidad. En una etapa 110, la información se almacena en el chip 2 del documento de identidad. Esta información puede contener fotografía de identidad digitalizada, con y/o sin motivos superpuestos, y/o estadísticas de análisis de imagen concerniente a la fotografía de identidad, y/o las entradas alfanuméricas 4. En la etapa 111, el documento de identidad 1 está formado por la colocación de la fotografía de identidad 3 provista de motivos 6 sobre el soporte 7, mediante impresión o por cualquier otro medio apropiado.

La figura 9 representa esquemáticamente un sistema de autenticación 8 de un documento de identidad 1. El sistema de autenticación 8 comprende un terminal 81. Un escáner 82 se encuentra conectado al terminal 81. Un lector de tarjetas de chip 83 también está conectado al terminal 81. Puede ser un lector de tarjetas inteligentes sin contacto, especialmente para leer el chip si se inserta dentro del cuerpo del documento de identidad 1. El terminal 81 está configurado para ejecutar una o más aplicaciones de gestión de autenticación.

Un ejemplo de procedimiento de autenticación se detalla en la Figura 8. En una etapa 201, el documento de identidad se escanea con el escáner 82. En particular, la fotografía de identidad 3 y las entradas alfanuméricas 4 son digitalizadas. Una aplicación de decodificación ejecutada en el terminal 81 controla un cierto número de operaciones

- de procesamiento de imágenes. En una etapa 202, una aplicación de procesamiento de imágenes identifica las entradas alfanuméricas 4. En una etapa 203, una aplicación de procesamiento de imágenes determina la presencia o no de intersecciones de líneas de motivos 6 en las ubicaciones predeterminados proporcionadas por la aplicación de decodificación. En una etapa 204, un código binario es extrapolado en función de los lugares para los que se han identificado las intersecciones de motivos 6. En una etapa 205, la aplicación de decodificación recoge las informaciones alfanuméricas entre las entradas alfanuméricas identificadas, conforme a un protocolo de codificación estandarizado. En una etapa 206, la aplicación de decodificación genera un código binario a partir de la información alfanumérica aplicando dicho protocolo de codificación estandarizado. En una etapa 207, se comparan el código binario surgido de las informaciones alfanuméricas y el código binario extrapolado de los motivos. En una etapa 208, las entradas alfanuméricas almacenadas en el chip 2 también son ventajosamente leídas por el lector 83. En una etapa 209, se genera un código binario a partir de información alfanumérica leída en el chip 2. En una etapa 210, se comparan los códigos binarios surgidos del chip 2 con el código binario extrapolado de los motivos 6. En una etapa 211, el resultado de la autenticación se visualiza en la pantalla 84.
- Por lo tanto, a partir de un documento de identidad 1 en el que los motivos codifican la información alfanumérica concerniente al titular, se puede realizar una autenticación suplementaria a partir del protocolo de codificación estandarizado difundido a las autoridades. También es concebible que el tipo de codificación y las ubicaciones de las zonas de codificación de la fotografía de identidad se identifiquen en el chip 2.
- En las formas de realización descritas en las figuras 1 a 6, las propiedades de los motivos en las áreas de codificación se limitan a la presencia o no de una intersección de motivos. Sin embargo, también se pueden utilizar otras propiedades de manera independiente o en combinación con las intersecciones de motivos. Puede considerarse especialmente el realizar una codificación basada en la posición de la intersección en dichas áreas, basada en el color de la intersección de los motivos, basada en los ángulos entre los motivos en la intersección o basada en las formas de los motivos en la intersección. Se puede también contemplar la realización de una codificación independiente de las intersecciones de los motivos, basada en el color o el contraste de los motivos en comparación con la fotografía de identidad en el fondo, o una codificación basada en el grosor de las líneas de los motivos en las zonas de codificación.
- El color o la luminosidad de los motivos se adaptan ventajosamente al fondo sobre el que se superponen. Así, se podrá prever que los motivos presenten un contraste de color o de luminosidad con respecto a la fotografía de identidad. Los motivos resultarán así fácilmente diferenciables a simple vista durante la observación de la fotografía de identidad. El color o la luminosidad de un motivo también podrá variar a lo largo de su longitud en función del fondo sobre el que se superpone.
- El uso de motivos de acuerdo con la invención no excluye el uso de otros motivos de seguridad suplementarios, tales como marcas de agua.
- El documento de identidad 1 ilustrado se refiere al caso de una tarjeta inteligente de acceso seguro. La invención, por supuesto, se aplica a cualquier otro tipo de documento de identidad, como un permiso de conducir, un pasaporte o documento nacional de identidad.

REIVINDICACIONES

1. Procedimiento de protección de un documento de identidad (1) que comprende una fotografía de identidad (3) y entradas alfanuméricas (4) relativas al titular del documento de identidad, que comprende las etapas de:

- recogida de entradas alfanuméricas (4) de las entradas alfanuméricas destinadas a figurar en el documento de identidad;
- codificar las informaciones alfanuméricas recogidas por propiedades de motivos destinadas a figurar en las áreas predeterminadas de la fotografía de identidad (3), siendo los motivos susceptibles de revelar una eventual alteración de la fotografía de identidad;
- realizar el documento de identidad de modo que incluya las citadas entradas alfanuméricas (4), y de manera que incluya la fotografía de identidad (3) sobre la que figuran de forma visible los motivos (6) con dichas propiedades en dichas áreas predeterminadas,

caracterizado porque los motivos están constituidos de líneas superpuestas con la fotografía de identidad y presentan intersecciones de las líneas, y porque las citadas informaciones alfanuméricas recogidas son codificadas por la presencia o no presencia de intersecciones de los motivos en dicha áreas predeterminadas (62).

2. Procedimiento de protección de un documento de identidad de acuerdo con la reivindicación 1, en el que el color o la luminosidad de los motivos se adapta ventajosamente al fondo sobre el que se superponen.

3. Procedimiento de protección de un documento de identidad de acuerdo con la reivindicación 1, en el que los motivos (6) presentan un contraste de color o luminosidad con respecto a la fotografía de identidad (3) a fin de ser fácilmente visible a simple vista.

4. Procedimiento de protección de un documento de identidad de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende el análisis del colorido o de la intensidad de las zonas predeterminadas de la fotografía de identidad, y que comprende la realización de los motivos (6) con un contraste de color o de intensidad con respecto a la fotografía de identidad en las áreas predeterminadas.

5. Procedimiento de protección de un documento de identidad de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el documento de identidad (1) comprende un chip (2), comprendiendo el procedimiento una etapa de escritura de las entradas alfanuméricas, las informaciones alfanuméricas recogidas, de las ubicaciones de las áreas predeterminadas, y/o de la fotografía de identidad en el chip.

6. Procedimiento de protección de un documento de identidad de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la etapa de codificación mediante las propiedades de motivos está precedida por una etapa de cifrado de las informaciones recogidas.

7. Procedimiento de protección de un documento de identidad de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que las zonas predeterminadas de la fotografía de identidad (3) presentan una densidad variable en diferentes localizaciones de la fotografía de identidad.

8. Procedimiento de protección de un documento de identidad de acuerdo con la reivindicación 7, en el que las zonas predeterminadas presentan una densidad menor a nivel de los ojos de la fotografía de identidad (3).

9. Procedimiento de protección de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende las etapas de:

- analizar digitalmente la fotografía de identidad para extraer estadísticas de imagen;
- codificar en ciertas áreas predeterminadas las estadísticas de imagen extraídas por las propiedades de motivos.

10. Sistema de comprobación de autenticidad de un documento de identidad (1), caracterizado porque comprende:

- dispositivo de recopilación (82) digital de imagen;
- un módulo de procesamiento capaz de determinar las informaciones alfanuméricas en una imagen recopilada y capaz de identificar las propiedades de los motivos en las áreas predeterminadas de una imagen capturada, siendo los motivos susceptibles de revelar una eventual alteración de la fotografía de identidad;
- módulo de autenticación (81), que indica al módulo de procesamiento de las zonas predeterminadas a analizar para la identificación de las propiedades de los motivos en esas zonas, decodificando las informaciones codificadas por las propiedades de tales motivos, comparando las informaciones emanadas de la imagen captada con las informaciones descodificadas, y generando una señal representativa de la autenticidad en función del resultado de la comparación, y en el que los motivos se componen de líneas superpuestas con la fotografía de identidad y presentan intersecciones de líneas, estando codificadas dichas informaciones por la presencia y la no presencia de intersecciones de las líneas en dichas áreas predeterminadas (62).

- 5 11. Sistema de comprobación de autenticidad de un documento de identidad (1), que comprende además un dispositivo de lectura (83) de un chip (2) del documento de identidad (1), comparando dicho módulo de autenticación (81) las informaciones decodificadas con las informaciones almacenadas en el chip y generando una señal representativa de la autenticidad en función del resultado de esta comparación.

Fig. 1

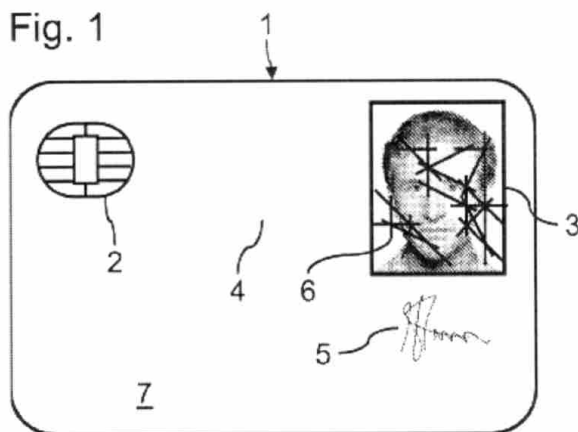


Fig. 2

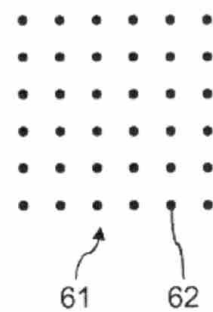


Fig. 3

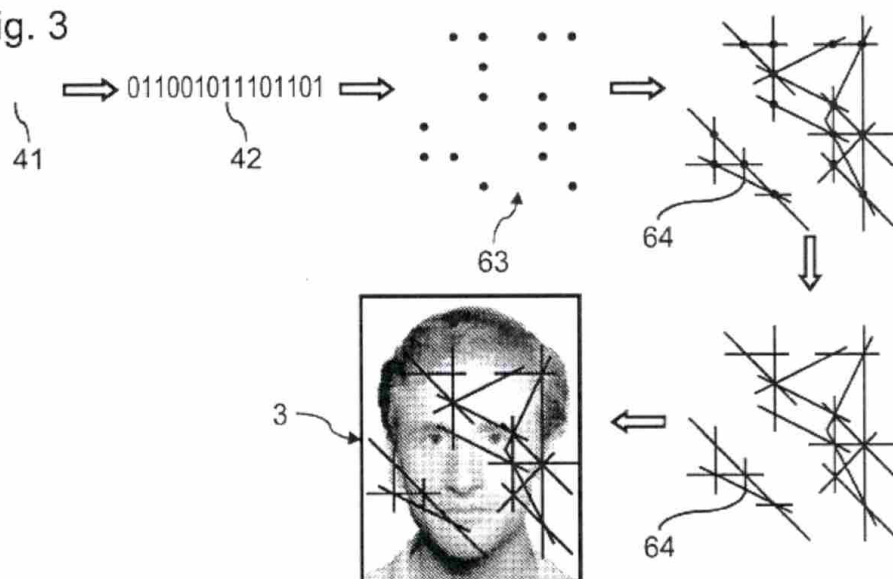


Fig. 4

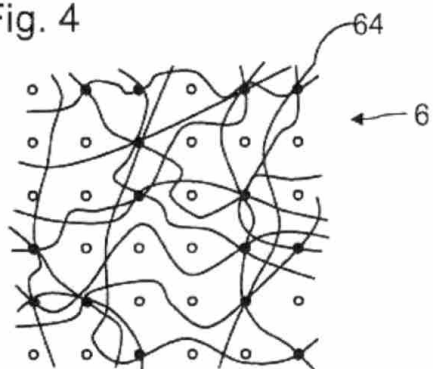


Fig. 5

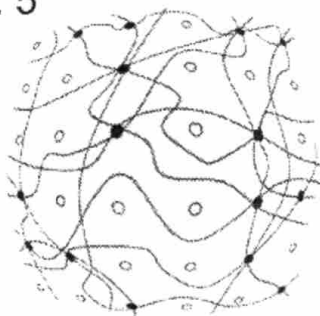


Fig. 6

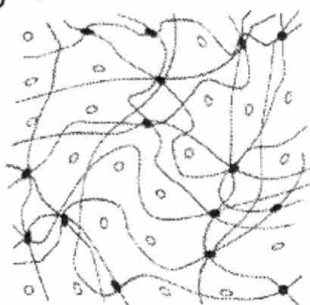


Fig. 7

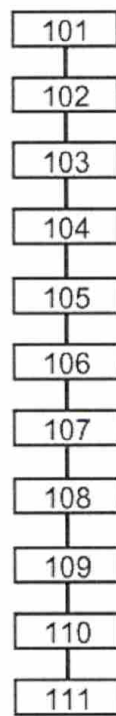


Fig. 8

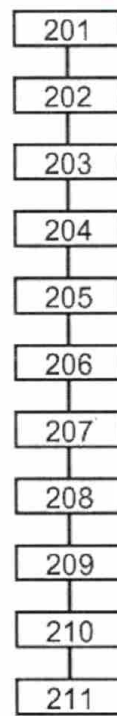


Fig. 9

