(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 584 309**

(51) Int. Cl.:

***B42D 15/00*** (2006.01)
***B42D 25/29*** (2014.01)
***B42D 25/00*** (2014.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.07.2009** **E 09793943 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.03.2016** **EP 2307204**

(54) Título: **Método para asegurar una imagen con medios gráficos anti-falsificación, método para asegurar un documento de identificación, y documento de identificación seguro**

(30) Prioridad:

**07.07.2008 EP 08290666**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**27.09.2016**

(73) Titular/es:

**GEMALTO SA (50.0%)**
**6, rue de la Verrerie**
**92197 Meudon Cedex, FR y**
**GEMALTO OY (50.0%)**

(72) Inventor/es:

**POHJOLA, TEEMU;**
**MOURTEL, CHRISTOPHE y**
**ROS, FRÉDÉRIC**

(74) Agente/Representante:

**ISERN CUYAS, María Luisa**

**ES 2 584 309 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 asegurar una imagen con medios gráficos anti-falsificación, método para asegurar un documento de identificación, y documento de identificación seguro.

Esta invención se refiere en general a documentos de identificación y a un método para la fabricación de dichos documentos de identificación. Más particularmente, esta invención se refiere a un método para la obtención de una imagen mediante medios de anti-falsificación gráficos y a un método para obtener un documento de identificación con tales medios de anti-falsificación gráficos. La invención también se refiere a un documento de identificación segura que permite detectar, ya sea una modificación fraudulenta de la personalización existente o un documento falsificado fraudulento.

Los documentos de identificación, con o sin chip, tales como permisos de conducir, tarjetas de identidad, tarjetas de socio, distintivos o pases, pasaportes, tarjetas de descuento, tarjetas bancarias, tarjetas monedero, tarjetas de múltiples aplicaciones y otros documentos de valor; y documentos de seguridad tales como billetes de banco, son ampliamente utilizados. Debido a la importancia y el valor asociado a cada uno de estos soportes de datos, a menudo son objeto de copia y alteraciones no autorizadas, y falsificaciones.

Para evitar que este tipo de actividades se lleven a cabo en estos soportes de datos, se han añadido diferentes tipos de características visuales y táctiles de seguridad a estos soportes de datos. Una de estas características de seguridad es un patrón, que se realiza con líneas onduladas que dibujan motivos predeterminados. Tal patrón se superpone a los datos de personalización, por ejemplo, una fotografía, y es comúnmente conocido bajo el nombre de "guilloches". La Figura 1 muestra una ilustración de este tipo de patrón guilloche 10 superpuesto sobre la fotografía 12 del titular del documento de identidad.

Sin embargo, la forma de este tipo de patrón de es predecible porque resulta ser el mismo en todos los documentos de un lote. En consecuencia, es muy fácil para los falsificadores escanear el patrón y reproducirlo en un documento en blanco sobre el que se ha impreso una fotografía fraudulenta, con el fin de fabricar documentos falsificados por completo.

Para evitar tales falsificaciones, una solución consiste en tener en cuenta los datos personalizados del propietario para definir un patrón personalizado para cada documento. Sin embargo, con una solución de este tipo, los policías podrían no ser capaces de hacer una primera verificación por simple inspección visual, y tendrían que depender de un dispositivo de lectura aparte destinado a tal fin. En consecuencia, una solución de este tipo consume tiempo y dinero.

Otra solución para evitar la falsificación consiste en calcular el tono de gris de la imagen original, en la ubicación del píxel guilloche específico, a fin de revertir la luminosidad de este píxel guilloche en comparación con la imagen original de modo que el píxel guilloche se haga perceptible a simple vista. La Figura 2 muestra línea guilloche esquemática 110 insertada en una parte de una imagen 100, en la que la luminosidad de los píxeles objetivo 111, 112, 113 se ha cambiado para formar la línea guilloche 110. En esta figura, la línea guilloche utiliza una escala de grises que contrastan fuertemente con el fondo. Por ejemplo, los píxeles guilloche aparecen claros 111 en una zona oscura 101 de la imagen, y la oscura 112, 113 en una zona clara 102, 103 de la imagen. Sin embargo, este

enfoque no protege contra la personalización ilícita de documentos en blanco ya que no hay manera, con o sin lector, de detectar si el patrón de seguridad (guilloche) se genero usando los algoritmos correctos y tienen el tono de gris correcto. De hecho, un falsificador puede escanear el patrón guilloche y aplicarlo en una imagen fraudulenta mediante la inversión de la luminosidad del píxel guilloche objetivo. Además, incluso si el patrón guilloche ahora es perceptible y resistente a la degradación de la imagen, el contraste puede ser demasiado alto y puede afectar a la percepción de la imagen, ya que no tiene en cuenta el sistema visual humano. El sistema visual humano se define como la forma en que las personas perciben las imágenes, es decir, el proceso que implica no sólo el ojo, sino también las partes de procesamiento de imágenes del cerebro.

La patente GB 2 289 016 describe un método para proteger información visual mediante la validación de un conjunto de píxeles de seguridad encriptados.

Teniendo en cuenta lo anterior, la invención tiene por objeto mejorar las soluciones de la técnica anterior existentes al posibilitar una primera inspección visual de una sola forma de patrón predecible, una detección de personalización ilícita basada en un lector, y mediante el uso del conocimiento del sistema visual humano para mejorar la percepción visual del patrón de seguridad incorporado.

Por lo tanto, un primer problema técnico que se pretende resolver con la invención es proporcionar un método para asegurar una imagen inicial mediante la superposición de una imagen con patrón de seguridad sobre la primera, en el que cada imagen está definida por una pluralidad de píxeles, permitiendo dicho método insertar un patrón de seguridad mediante el uso del conocimiento del sistema visual humano a fin de no alterar la percepción visual de la imagen inicial, para utilizar únicamente un patrón de seguridad predecible de manera que una primera verificación visual sigue siendo posible, y para detectar una personalización ilícita por medio de una lector especializado.

Un segundo problema técnico que se pretende resolver con la invención es asegurar un documento de identificación que incorpora una imagen de identificación mediante la inserción de una imagen con patrón de seguridad en la imagen de identificación, previniendo este método una modificación fraudulenta posterior de la personalización que se pretende realizar, lo que resulta fácil de detectar mediante el uso de un lector especializado, y previniendo la confección de un documento de identificación completamente falsificado.

Otro problema técnico que se pretende resolver con la invención es proporcionar un método para verificar la autenticidad de una imagen asegurada por medio de la inserción en la misma de una imagen con patrón de seguridad insertado, permitiendo dicho método detectar todos los tipos de fraude, ya sea una imagen completamente falsificada o una imagen que haya sido modificada posteriormente.

**Resumen**

La solución de la invención al primer problema se refiere al hecho de que el método comprende las siguientes etapas:

- definir una matriz Ωi de píxeles en la imagen inicial, rodeando dichos píxeles de la matriz la posición i de un píxel de la imagen con patrón de seguridad a insertar en la primera inicial,

- determinar un valor característico G(Ωi) de los píxeles dentro de la matriz Ωi y el grado de textura T(Ωi) de la matriz Ωi.

- modificar el tono característico de un píxel de la imagen inicial en la posición i de un píxel del patrón de seguridad a insertar, y rodeado por la matriz Ωi, utilizando una función F que tiene en cuenta el tono característico G(Ωi) de los píxeles dentro de la matriz Ωi y el grado de textura T(Ωi) de la matriz,

- repetir los pasos anteriores para cada píxel de la imagen con patrón de seguridad a insertar en la imagen inicial.

El tono característico puede ser un valor característico para cada píxel, representando este valor, por ejemplo, uno de los siguientes: tono de grises, luminosidad, rojo, verde, azul, cian, magenta, amarillo, negro. Por lo tanto, el valor característico puede ser la escala de grises o las escalas de color. En un ejemplo que funciona bien, el tono característico de los píxeles dentro de la matriz puede ser, aunque no se limita a, el tono de gris medio de la matriz de píxeles. Por lo tanto, teniendo en cuenta el grado de textura y el tono característico de los píxeles vecinos que rodean al píxel objetivo del patrón de seguridad a insertar, se modula la fuerza de inserción de la imagen con patrón de seguridad en la imagen inicial, de modo que la percepción global de la imagen inicial se mejora y no resulta alterada por la imagen patrón insertada. El tono característico, por ejemplo la escala de grises, de cada píxel de la imagen con patrón de seguridad insertada que esta vinculado a los píxeles circundantes de la imagen inicial por una función que se mantiene en secreto, es imposible confeccionar una imagen completamente falsa o modificar de forma fraudulenta la imagen inicial sin conocer esta función.

La solución de la invención al segundo problema técnico se refiere al hecho de que el método para la aseguración de un documento de identificación comprende las etapas del método para asegurar una imagen inicial mediante una imagen con patrón de seguridad y la imagen de identificación y su imagen con patrón de seguridad insertada se imprimen de forma simultanea en un solo paso en el documento de identificación.

De acuerdo con otro aspecto de la invención, se proporciona un documento de identificación seguro que tiene impresa una imagen de identificación y una imagen con patrón de seguridad, estando insertada la imagen con patrón de seguridad en la imagen de identificación, estando definidas dichas imágenes por una pluralidad de píxeles, caracterizados porque tono característico de cada píxel i de la imagen con patrón de seguridad esta vinculado, por una función F, a una matriz Ωi de píxeles definidos en la imagen de identificación, dichos píxel es de la matriz Ωi rodeando la posición i de un píxel del patrón de seguridad insertado, teniendo en cuenta dicha función F el tono característico G(Ωi) de los píxeles dentro de la matriz Ωi, y el grado de textura T(Ωi) de la matriz Ωi.

La solución de la invención al tercer problema técnico se refiere al hecho de que el método comprende las siguientes etapas:

- determinar, para cada píxel insertado de la imagen con patrón de seguridad, una matriz Ωi de píxeles en la imagen inicial, rodeando la posición i de dicho píxel insertado,

- ejecutar el algoritmo que calcula el tono característica $G'i_c$ del píxel i teniendo en cuenta el tono característico G(Ωi) de los píxeles dentro de la matriz Ωi, y el grado de textura T(Qi) de la matriz,

- comparar el resultado $G'i_c$ obtenido con el valor del tono característico $G'i_r$ escaneado de dicho píxel insertado,

- repetir las operaciones para todos los píxeles de toda la imagen con patrón de seguridad y, dependiendo de si el resultado de la comparación esta dentro de los limites aceptables predeterminados, emitir un veredicto sobre la autenticidad de la imagen segura.

**Breve descripción de los dibujos**

La invención se entenderá mejor con referencia a los dibujos, en los que:

La Figura 1, ya descrita, es un dibujo de una imagen combinada que incluye una imagen del retrato del titular de un documento de identidad y una imagen con patrón de seguridad formado por un conjunto de líneas guilloches,

La Figura 2, ya descrita, es un dibujo esquemático que muestra una parte ilustrativa de una imagen inicial que se cambia en algunos píxeles para insertar una línea guilloche de acuerdo con un método conocido,

La Figura 3 es un dibujo que muestra una parte ilustrativa de una imagen inicial en la que se insertan algunos píxeles de una línea guilloche de acuerdo con un método de la presente invención,

La Figura 4 es un diagrama de flujo que muestra una secuencia de pasos para asegurar una imagen inicial mediante una imagen con patrón de seguridad de acuerdo con la invención,

La Figura 5 es el diagrama de flujo de la figura 4 con etapas adicionales opcionales para asegurar una imagen inicial mediante la inserción de una imagen con patrón de seguridad,

La Figura 6 es un diagrama de flujo que muestra una secuencia de pasos para verificar la autenticidad de una imagen que ha sido asegurada de acuerdo con la invención.

**Descripción detallada**

En lo sucesivo, una realización de la presente invención se describirá en el contexto de una tarjeta de identidad (ID) y un método para producirla. Sin embargo, ha de entenderse que la invención es utilizable con cualquier soporte de datos que incluye, pero no se limita a, un permiso de conducir, una credencial o un pase, un pasaporte, una tarjeta de descuento, una tarjeta de socio, una tarjeta bancaria, una tarjeta de crédito, una tarjeta monedero, una tarjeta multi-aplicación, y otros documentos de seguridad y de valor a los que se les suministra información o datos de tal manera que no puedan ser fácilmente imitados por medios comunes.

Una imagen con patrón de seguridad, como líneas guilloche, tiene que ser resistente a la degradación de la imagen y no afectar a la percepción de la imagen inicial, en la que se inserta. Tiene que ser añadida a la imagen inicial como una capa adicional perceptible y controlada. La imagen inicial es, por ejemplo, la fotografía del titular de la tarjeta. El Sistema Visual Humano esencialmente se traduce en el hecho de que cada valor de píxel de una imagen puede ser cambiado solamente en una cierta cantidad para que no afecte a la calidad de la imagen. Este límite se denomina "distorsión justo apreciable" o valor JND. Si la distorsión de un píxel no se encuentra fuera del limite definido por este valor JND, la degradación del píxel es imperceptible. La línea guilloche tiene que ser añadida como una capa adicional perceptible en la imagen original de la identificación sin afectar el reconocimiento y percepción del rostro. Es la condición necesaria. El mecanismo básico existente que consiste en invertir la luminosidad del patrón, para cada píxel guilloche en una imagen (ya descrita respecto de la figura 2), no alcanza estos dos objetivos en conflicto. La percepción humana no está sólo basada en la diferencia de gradiente, sino que depende del nivel de luminosidad. Así, por ejemplo, si un tono medio de gris es de alrededor de 20, en los píxeles vecinos, y si el píxel objetivo en la posición i se cambia a 50, la percepción será muy diferente que para un tono de gris medio de 200, cambiado a 230, mientras la diferencia entre los dos valores es de 30 y el mismo en los dos casos. En consecuencia, la fuerza de inserción de los píxeles guilloche en una posición determinada tiene que ser modulada de acuerdo con el grado de textura y la luminosidad de su vecindad, con el fin de generar un conjunto de reglas. Estas reglas permiten determinar un rango de valores aceptables. Para cada valor, se hace posible estimar el nivel de percepción.

La Figura 3 muestra un dibujo esquemático de una parte ilustrativa de una imagen inicial 210 en la que se inserta una imagen con patrón de seguridad 220 de acuerdo con la invención. Esta figura se explicará junto con la figura 4, que es un diagrama de flujo que muestra una secuencia de pasos para asegurar la imagen inicial 210 mediante la imagen con patrón de seguridad 220. La imagen inicial 210 es, por ejemplo, la imagen del retrato del titular de un documento de identidad, tal como una tarjeta de identidad o un pasaporte. En una primera etapa del proceso de aseguración, el paso de copia de los datos de la imagen del retrato 300 consiste en copiar los datos de la imagen del retrato desde un archivo JPEG a otro archivo en una memoria del sistema de personalización para obtener una copia memorizada de la imagen del retrato. Esta imagen inicial del retrato está definida por una pluralidad de píxeles 211 a 218. La imagen con patrón de seguridad 220, que tiene que ser insertada en la imagen inicial, puede ser por ejemplo, pero no se limita a, una línea de guilloche. Esta imagen con patrón de seguridad 220 también está definida por una pluralidad de píxeles 221 a 224. La inserción de esta segunda imagen 220 en la imagen inicial consiste de hecho en la modificación de algunos píxeles 221-224 de la imagen inicial 210 de manera que la segunda imagen 220 pueda ser percibida en la primera. La modificación puede consistir en la reversión de la luminosidad de cada píxel que constituye la línea guilloche 220. Sin embargo, la inserción de la segunda imagen alterará la percepción de la imagen inicial ya que se requiere que ambas sean visibles. No obstante, la degradación de la imagen inicial 210 por la inserción de la segunda imagen debe ser minimizada. De hecho, la fotografía por ejemplo, debe permanecer lo mas reconocible como sea posible, ya que ésta es la función principal de tener una fotografía en el documento en primer lugar. En otras palabras, el patrón insertado no debería ocultar la imagen por tener una malla demasiado densa de líneas ni un contraste demasiado alto entre el patrón insertado y la imagen original subyacente. En consecuencia, la fuerza de inserción de la segunda imagen 220 en la imagen inicial210 tiene que ser controlada.

El siguiente paso 310 del proceso consiste en la lectura del siguiente píxel guilloche desde el archivo de imagen de líneas guilloche, que esta memorizado en el sistema de personalización. A continuación, la secuencia pasa a una etapa de decisión "EOF?" 320, en la que el procesador del sistema de personalización determina si se ha alcanzado el final-del-archivo del archivo de imagen de líneas guilloche. Si se determina en esta etapa de decisión 320 que el final-del-archivo no se ha alcanzado, la secuencia de personalización procede a continuación a determinar la fuerza de inserción de cada píxel 221 -224 de las líneas guilloche 220 a ser insertado en la imagen de retrato 210, de modo que sea perceptible sin alterar el reconocimiento visual de la primera imagen 210.

Para ello, la fuerza de inserción de cada píxel 221-224 de la línea guilloche 220, en la primera imagen, se modula de acuerdo con primero, la luminosidad, o, por ejemplo, el nivel medio de gris, y segundo, el nivel de textura de una matriz Ωi de los píxeles que rodean el píxel objetivo a insertar, con el fin de generar un conjunto de normas que permitan la determinación de un rango de valores de nivel de características aceptables, tales como valores de nivel de gris en los ejemplos ilustrados. En consecuencia, el siguiente paso 330 del proceso consiste en definir una matriz Ωi de píxeles XxY alrededor de la posición i de un píxel guilloche 222 a insertar, pero sin este píxel i guilloche objetivo. En el ejemplo ilustrado en la figura 3, la matriz Ωi, que se representa con líneas mas gruesas, se compone de seis píxeles 211, 212, 213, 214, 215 y 216 de la primera imagen, que rodean, pero no comprenden, el píxel objetivo 222 en una ubicación i. En el ejemplo de la figura 3, la matriz comprende píxeles 3x3. En el campo de la impresión, las imágenes sufren del ataque conocido "imprimir y escanear". En consecuencia, es preferible determinar una matriz que defina un área pequeña alrededor del píxel objetivo, a fin de que la impresión de las dos imágenes no degrade demasiado la calidad de las imágenes numéricas. Incluso si la matriz comprende dos píxeles que rodean el píxel objetivo, esto puede funcionar, pero los resultados son menos precisos que si la matriz contiene píxeles 8x8, por ejemplo. Por otra parte, la matriz no debe contener demasiados píxeles a fin de no enlentecer demasiado el tiempo de procesamiento de imágenes. Con el fin de tener una línea guilloche que sea visible en la primera imagen pero que no altera la percepción visual de esta primera imagen, debe ser tenida en cuenta no sólo la luminosidad, sino también la textura de los píxeles de la matriz.

Cada píxel 211 a 216 de la matriz Ωi tiene su propio nivel característico, por ejemplo, su propio nivel de gris, o su propia luminosidad. Para la determinación del nivel característico del píxel objetivo 222 en la posición i, el nivel característico G(Ωi) de todos los píxeles dentro de la matriz Ωi se calcula en la etapa 340. Este nivel característico puede ser un numero característico para cada píxel, representando este numero por ejemplo, uno de los siguientes: nivel de gris, luminosidad, rojo, verde, azul, cían, magenta, amarillo, negro. Por lo tanto, el nivel característico puede ser o bien escala de grises o escalas de colores o parametrización de imágenes en color. En un ejemplo de buen trabajo, como se ilustra en las figuras 3 y 4, el nivel característico de los píxeles dentro de la matriz puede ser, aunque no se limita a, el nivel medio de gris de la matriz de píxeles. El nivel medio de textura T(Ωi) de la matriz Ωi también se determina en la etapa 350. La textura se define, en el campo de la imagen, como una mezcla de diferentes colores o colores negros, grises y blancos que dan la impresión de que la imagen es mas o menos uniforme. Si la imagen parece no ser uniforme, como el cabello por ejemplo, se define como siendo texturizada, por el contrario sí parece ser homogénea, no es texturizada. Teniendo en cuenta esta definición, es posible definir los niveles de textura, por ejemplo cuatro niveles de textura, en donde se definirá el nivel de D como el mas texturizado, mientras que el nivel A se define como el menos texturizado, por ejemplo. Si

la fotografía tiene una zona muy texturizada, como el cabello por ejemplo, ha de tenerse en cuenta el nivel de textura con el fin de que el píxel 222 insertado de la línea guilloche, en la posición i, sea perceptible para el ojo humano.

El orden de estas etapas 340 y 350 de definición del nivel y textura característicos de la matriz no es relevante; se puede invertir indiferentemente sin perturbar el proceso.

La fuerza de inserción en una ubicación dada es modulada de acuerdo con el nivel de textura y la luminosidad de su entamo, con el fin de generar un conjunto de reglas. Estas reglas permiten determinar un rango de valores aceptables. Para cada valor, es posible estimar el nivel de percepción. Técnicamente, es posible definir una función F, que toma como entrada los niveles característicos del entorno G(Ωi) (por ejemplo niveles de gris de 0 a 255) y los niveles de textura T(Ωi) (por ejemplo, de A a D), y establece como niveles característicos de salida admisibles para cada píxel guilloche (por ejemplo un nivel de gris de 180 a 255 y de 0 a 80) y para cada uno de estos niveles admisibles, un nivel de percepción para el ojo humano (una resistencia de 1 a 5, por ejemplo).

A continuación, después de haber definido el nivel característico, por ejemplo el nivel medio de gris G(Ωi), y el nivel de textura T(Ωi) de la matriz (Ωi), se puede utilizar una función F, que se mantiene en secreto y que toma como entrada los valores definidos G(Ωi) y T G(Ωi), para calcular la modificación del nivel característico Gi' del píxel objetivo i de una línea guilloche comparada con su nivel característico original de Gi, de modo que se haga perceptible en la primera imagen sin alterar el reconocimiento de la primera imagen. Este cálculo se hace en la etapa 360.

Para la definición de la función F, es posible utilizar la lógica difusa usando una base de datos de un numero representativo de todas las matrices posibles Ωi en combinación con todos los patrones guilloches que tienen un nivel de gris uniforme. La base de datos puede almacenar para cada matriz Ωi varias informaciones: el nivel medio de gris G(Ωi), un parámetro de textura T(Ωi), un nivel de gris de guilloche Gi(Ωi), y un parámetro de percepción visual S(Ωi). El parámetro de textura T(Ωi) se calcula sobre la matriz Ωi y puede corresponder, por ejemplo, a la variación del nivel de gris en la matriz Ωi. En otro ejemplo, el parámetro de textura T(Ωi) puede corresponder a medios del segundo al séptimo rango de la transformada de Fourier de la matriz Ωi. El parámetro de percepción visual S(Ωi) se determina con un panel de personas que indican un nivel de percepción del guilloche en la matriz, como un ejemplo 1 correspondiente a "no perceptible" y 5 correspondiente a "muy perceptible".

Estando definida la base de datos, se puede realizar una combinación de acuerdo con métodos de lógica difusa para determinar el nivel del píxel Gi(Ωi) de la matriz correspondiente Ωi. Esto se hace mediante la combinación de diferentes niveles de gris de guilloche de la base de datos de la matriz Ωi que tienen el mismo nivel medio de gris G(Ωi), el mismo o cercano parámetro de textura T(Ωi) y un mismo nivel de percepción S(Ωi).

También es posible tener una separación de la base de datos en dos partes, una para el nivel de gris aditivo para el guilloche y la otra para el nivel de gris de sustracción para el guilloche. Con este método de cálculo de la función F, el secreto de la función F reside en el secreto de la base de datos.

A continuación, el nivel característico, es decir el nivel de gris en el ejemplo ilustrado, del píxel guilloche 222 en la posición i en los datos de imagen retrato 210 se modifica, por lo que el píxel guilloche se hace visible sin alterar la percepción de la fotografía 210. Las etapas de la secuencia descrita de este modo se repiten para cada píxel del archivo de imagen de las líneas guilloche hasta que se ha alcanzado el final del archivo. Entonces, la imagen de identificación y el patrón de seguridad insertado se imprimen simultáneamente en una sola etapa (etapa 380) y el archivo de datos de imagen del retrato se elimina de los medios de memoria del sistema de personalización (etapa 390).

En una variante, también es posible tener en cuenta, corno entradas de la función secreta F, algunas expectativas del cliente. Así, el cliente puede esperar que la fuerza de inserción dependa de la localización en la fotografía. Por ejemplo, podría querer una inserción débil del guilloche en el centro de la cara, y una fuerte alrededor del centro de la cara, débil y fuerte representando la fuerza de inserción, es decir, puede ser mas o menos visible pero siempre sin que afecte al reconocimiento de la cara.

La forma de realización descrita de este modo permite hacer una primera inspección visual muy rápidamente, ya que el mismo patrón de seguridad puede usarse para asegurar imágenes de ID de todo tipo de documentos. Entonces, se puede realizar una segunda verificación mediante el uso de un lector dedicado que tenga un algoritmo apropiado para verificar que el patrón de seguridad insertado se ha hecho con el verdaderamente aceptable nivel característico, es decir la verdaderamente aceptable escala de grises en el ejemplo ilustrado.

Otra realización del proceso de personalización y asegurado de la primera imagen consiste en la adición de etapas facultativas que consigan que la falsificación resulte aún más difícil. La primera forma de realización que ha sido descrita solamente se basa en la dependencia no trivial de los píxeles del entorno. En este segundo modo de realización se añaden las etapas facultativas extra 351, 352 y 361.

Después de haber definido el nivel de textura T(Ωi) de la matriz Ωi, un paso adicional 351 consiste en la aplicación de una máscara en el nivel de textura, mediante el uso de una clave secreta K y un algoritmo secreto de cifrado, con el fin de proporcionar un aleatorio R(Ωi). Este paso adicional permite seleccionar una solución de representación entre una pluralidad de posibilidades, y para llenar un grado de libertad, mediante el uso de un algoritmo secreto, que depende de los píxeles del entorno.

Otro paso adicional 352, consiste en calcular un parámetro de fuerza Si, teniendo en cuenta el valor Aleatorio R(Ωi), que ha sido calculado, y un valor de Estrategia S(Ωi). El valor Estrategia S(Ωi) se define por las condiciones necesarias en un rango de valores de nivel característico aceptables para obtener un resultado perceptible (es decir, G(Ωi) y T(Ωi) y, opcionalmente, las expectativas de los clientes. Este parámetro S(Ωi) es preferiblemente predeterminado y mantenido en secreto en un área de almacenamiento, tal como, pero no limitado a, una memoria o una base de datos.

En la etapa 361, el nivel característico, es decir, el nivel de gris en el ejemplo ilustrado, de la imagen original en la posición i del píxel guilloche objetivo es modificado de acuerdo con la función Gi' = Gi + Si, en donde Gi' es el nivel de gris modificado del píxel i, Gi es el nivel de gris original del píxel i en la primera imagen, y Si = F(Estrategia (Ωi), Aleatorio (Qi)).

Para ser perceptible "agradable", se necesitan algunas optimizaciones de procesamiento de imágenes para mejorar la percepción global (en especial la continuidad) de los guilloches en la imagen final. La parte Aleatoria no se calcula píxel por píxel sino zonas por zonas (es decir, la matriz Ωi). La imagen tiene que ser cortada en pequeñas zonas de algunos píxeles en las que el comportamiento tiene que ser sustancialmente similar. La estrategia impone algunas restricciones para el guilloche, y toma también en cuenta las posibles expectativas del cliente. Así, una línea guilloche puede ser, por ejemplo, débil en el centro de la cara mientras que es más fuerte fuera hacia los bordes de la foto. Una combinación de la estrategia y de la parte aleatoria proporciona un guilloche visible, que resulta difícil de reproducir, en particular cuando la obra no es uniforme.

Tras la autenticación de documentos (véase el diagrama de flujo de la figura 6), se utiliza un lector especifico para detectar (etapa 420) la matriz Ωi de píxeles XxY en la primera imagen; alrededor de la posición i de cada píxel guilloche, para ejecutar el algoritmo anterior (etapas 430-450), y comparar (etapa 460) el resultado obtenido en la etapa de cálculo 450 para el valor de nivel característico escaneado (es decir, el valor de nivel de gris en el ejemplo ilustrado) de cada uno de los píxeles guilloche (etapa 410). Si la comparación está dentro del rango predeterminado de valores aceptables (etapas 490-492) para todo el guilloche, la personalización es considerada autentica (etapa 492). Si no, se considera falsificada (etapa 491). La comparación se hace píxel por píxel, pero el resultado de la autenticación se hace después de haber hecho la comparación de los píxeles de todo el patrón de seguridad.

El lector utilizado para la autenticación comprende un dispositivo de escáner, que puede ser, pero no limitado a, un escáner o una cámara o un teléfono móvil equipado con dicha cámara, etc. La imagen escaneada debe ser de suficiente alta resolución para poder analizar todos los píxeles. A continuación, el lector debe comprender también medios de cálculo para el análisis de los píxeles escaneados. El cálculo del nivel característico $Gi_c$ (es decir, el nivel de gris calculado en el ejemplo) de un píxel i del guilloche insertado se hace del nivel medio de gris G(Ωi) de la matriz, y mediante el uso de la función secreta F(Ωi).

El nivel característico, tal como la escala de grises, de los píxeles guilloche se pueden formar bastante generalmente como una suma ponderada de los píxeles vecinos. Los pesos pueden depender de muchos factores tales como los niveles de gris, u otros niveles de color, la textura de la imagen cercana al guilloche, el conocimiento del sistema de visión humana (ojos + cerebro), etc. La función F puede mantenerse en secreto, ya sea en el lector o en un servidor remoto, o en una memoria de un chip en el documento de identidad, etc.

Las realizaciones así descritas incrementan la seguridad de los documentos de identificación y evitan su modificación o fabricación de un documento falsificado por completo.

## REIVINDICACIONES

1. Documento de identificación seguro que tiene una imagen de identificación impresa y una imagen impresa de un patrón de seguridad, la imagen del patrón de seguridad estando insertada en dicha imagen de identificación, cada imagen estando definida por una pluralidad de píxeles, **caracterizado** porque el nivel característico de cada píxel i de la imagen del patrón de seguridad esta vinculada, por una función F, a una matriz Ωi de píxeles definidos en la imagen de identificación, dichos píxeles de la matriz Ωi rodeando el lugar i de un píxel de la imagen del patrón de seguridad a insertar, dicha función F teniendo en cuenta el nivel característico G(Ωi) de los píxeles dentro de la matriz Ωi y el nivel de textura T(Ωi) de dicha matriz m

2. Un método para asegurar la primera imagen mediante la superposición de una imagen del patrón de seguridad en dicha primera imagen en el documento de identificación de la reivindicación 1, en el que dicha imagen es una imagen de identificación impresa, y cada imagen está definida por una pluralidad de píxeles, **caracterizado** porque comprende las siguientes etapas:

- definir una matriz Ωi de píxeles de la primera imagen, dichos píxeles de la matriz rodeando la ubicación i de un píxel de la imagen del patrón de seguridad a insertar en la primera imagen,

- determinar un nivel característico G(Ωi) de los píxeles dentro de la matriz Ωi y el nivel de textura T(Ωi) de la matriz Ωi,

- modificar el nivel característico de un píxel de la primera imagen en la posición i de un píxel del patrón de seguridad a insertar, y rodeado por la matriz Ωi, mediante el uso de una función F que tiene en cuenta el nivel característico G(Ωi) de los píxeles dentro de la matriz Ωi y el nivel de textura T(Ωi) de la matriz,

- repetir las etapas anteriores para cada píxel de la imagen del patrón de seguridad a insertar en la primera imagen.

3. Un método de acuerdo con la reivindicación 2, en el que la función F se mantiene en secreto en un área de almacenamiento.

4. Un método de acuerdo con la reivindicación 2 o 3, en el que una etapa adicional consiste en la aplicación de una máscara en el nivel de textura T(Ωi) de la matriz Ωi, mediante el uso de una clave secreta K y un algoritmo secreto de encriptado, con el fin de proporcionar un aleatorio R(Ωi).

5. Un método para la asegurar un documento de identificación que incorpora una imagen de identificación, dicho método consistiendo en insertar una imagen del patrón de seguridad en la imagen de identificación, **caracterizado** porque la etapa de inserción comprende las etapas del método para asegurar una imagen de acuerdo con las reivindicaciones 2-4, y la imagen de identificación y la imagen del patrón de seguridad insertada en ella se imprimen de forma simultanea en un solo paso.

6. Un método de verificación de la autenticidad de una imagen en una documento de identificación, en el que dicha imagen es una imagen de identificación impresa y se encuentra asegurada por medio de una imagen del patrón de seguridad de acuerdo con

el método de las reivindicaciones 2 a 4, **caracterizado** porque comprende las siguientes etapas:

- definir una matriz Ωi de píxeles en la primera imagen, dichos píxeles de la matriz rodeando la ubicación i de un píxel de la imagen del patrón de seguridad insertada,

- determinar un nivel característico G(Ωi) de los píxeles dentro de la matriz Ωi y el nivel de textura T(Qi) de la matriz Ωi,

- calcular el nivel característico Gic de un píxel de la imagen del patrón de seguridad insertada en la ubicación i, rodeada por la matriz Ωi, usando una función F que tiene en cuenta el nivel característico G(Ωi) de los píxeles dentro de la matriz Ωi y el nivel de textura T(Ωi) de la matriz Ωi,

- comparar el nivel característico Gic calculado del píxel en la ubicación i con el nivel característico Gir leído del píxel escaneado en la misma ubicación i,

- repetir las etapas anteriores para cada píxel de la imagen del patrón de seguridad, y

- entregar el resultado de la autenticación después de haber realizado la comparación de los píxeles de todo el patrón de seguridad.

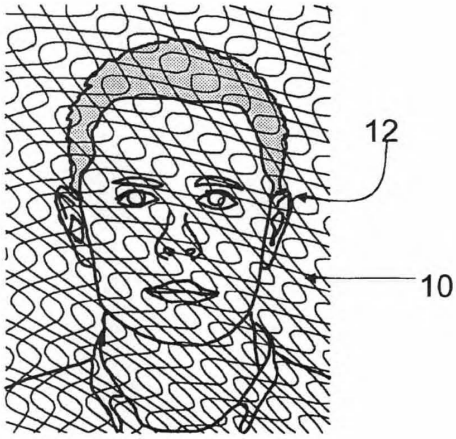


Figura 1

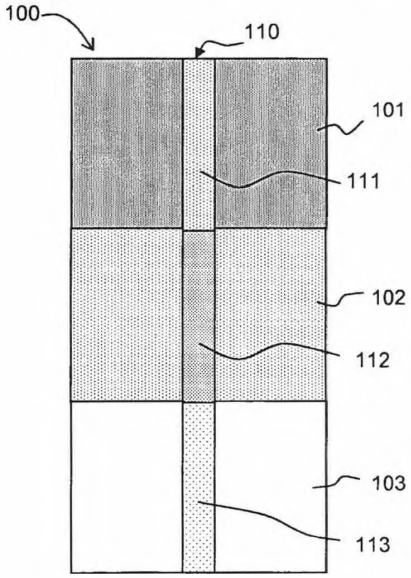


Figura 2

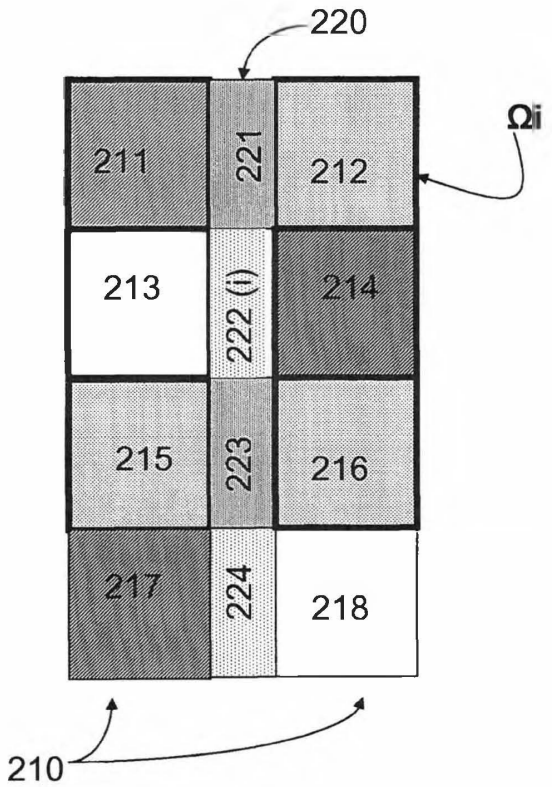


Figura 3

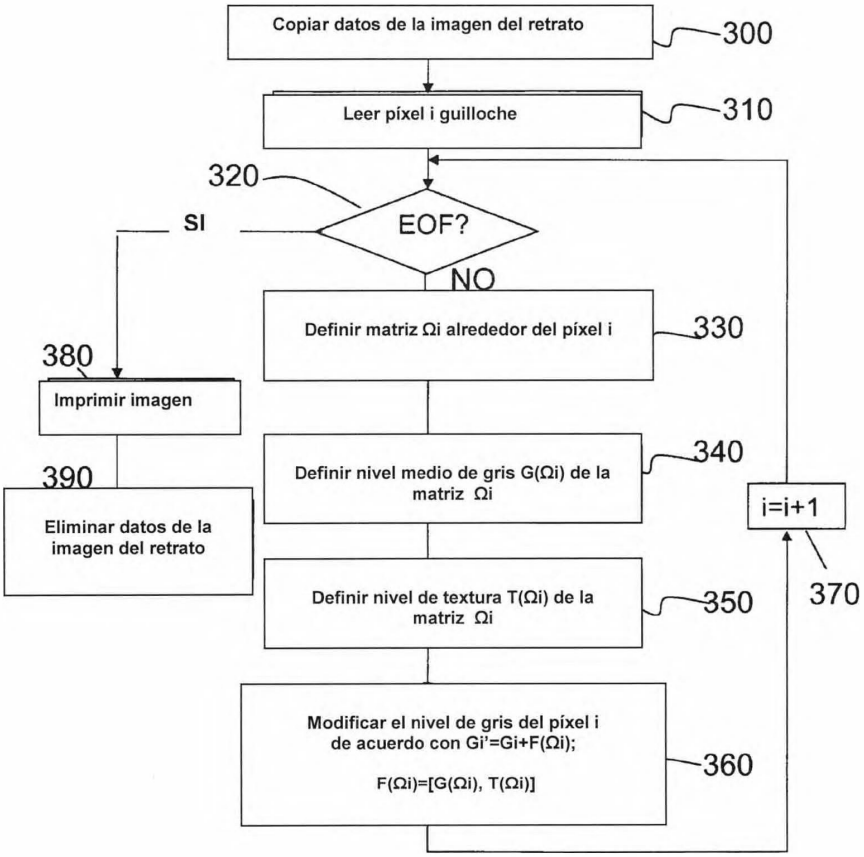
Copiar datos de la imagen del retrato
300
Leer píxel i guilloche
310
320
EOF?
SI
NO
Definir matriz Ωi alrededor del píxel i
330
380
Imprimir imagen
Definir nivel medio de gris G(Ωi) de la matriz Ωi
340
390
Eliminar datos de la imagen del retrato
i=i+1
370
Definir nivel de textura T(Ωi) de la matriz Ωi
350
Modificar el nivel de gris del píxel i de acuerdo con Gi'=Gi+F(Ωi);
F(Ωi)=[G(Ωi), T(Ωi)]
360

**Figura 4**

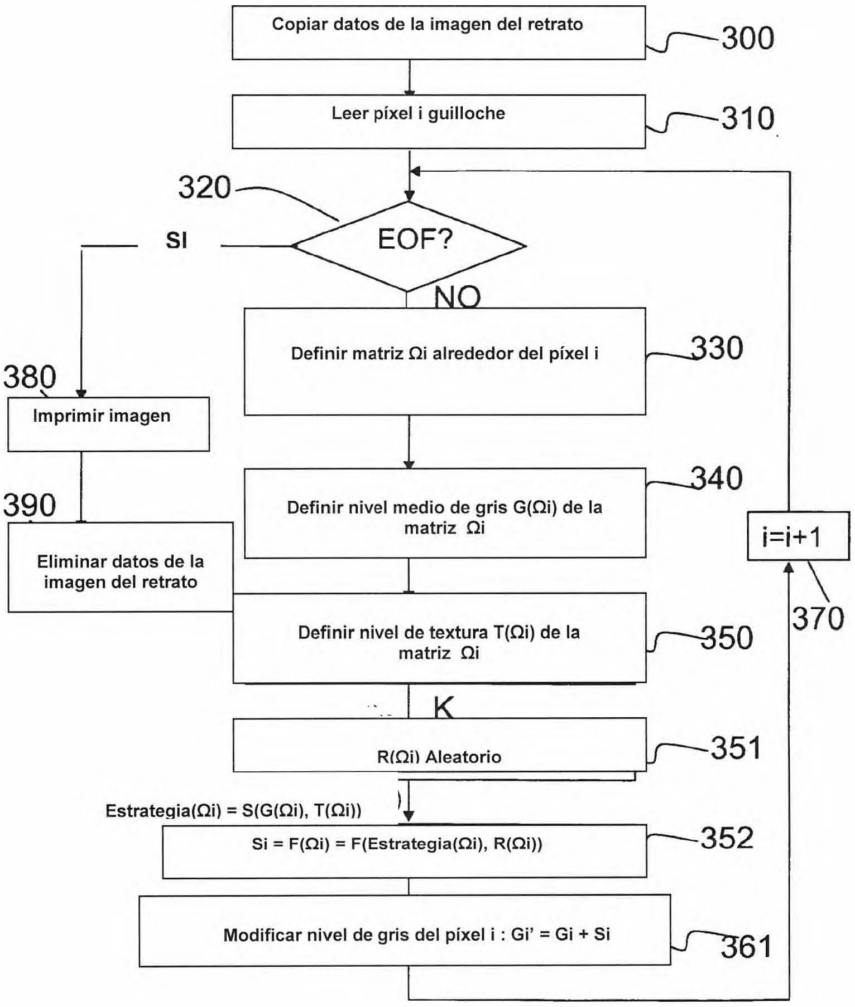
Copiar datos de la imagen del retrato
300
Leer píxel i guilloche
310
320
EOF?
SI
NO
Definir matriz Ωi alrededor del píxel i
330
380
Imprimir imagen
Definir nivel medio de gris G(Ωi) de la matriz Ωi
340
390
Eliminar datos de la imagen del retrato
i=i+1
370
Definir nivel de textura T(Ωi) de la matriz Ωi
350
K
R(Ωi) Aleatorio
351
Estrategia(Ωi) = S(G(Ωi), T(Ωi))
Si = F(Ωi) = F(Estrategia(Ωi), R(Ωi))
352
Modificar nivel de gris del píxel i : Gi' = Gi + Si
361

Figura 5

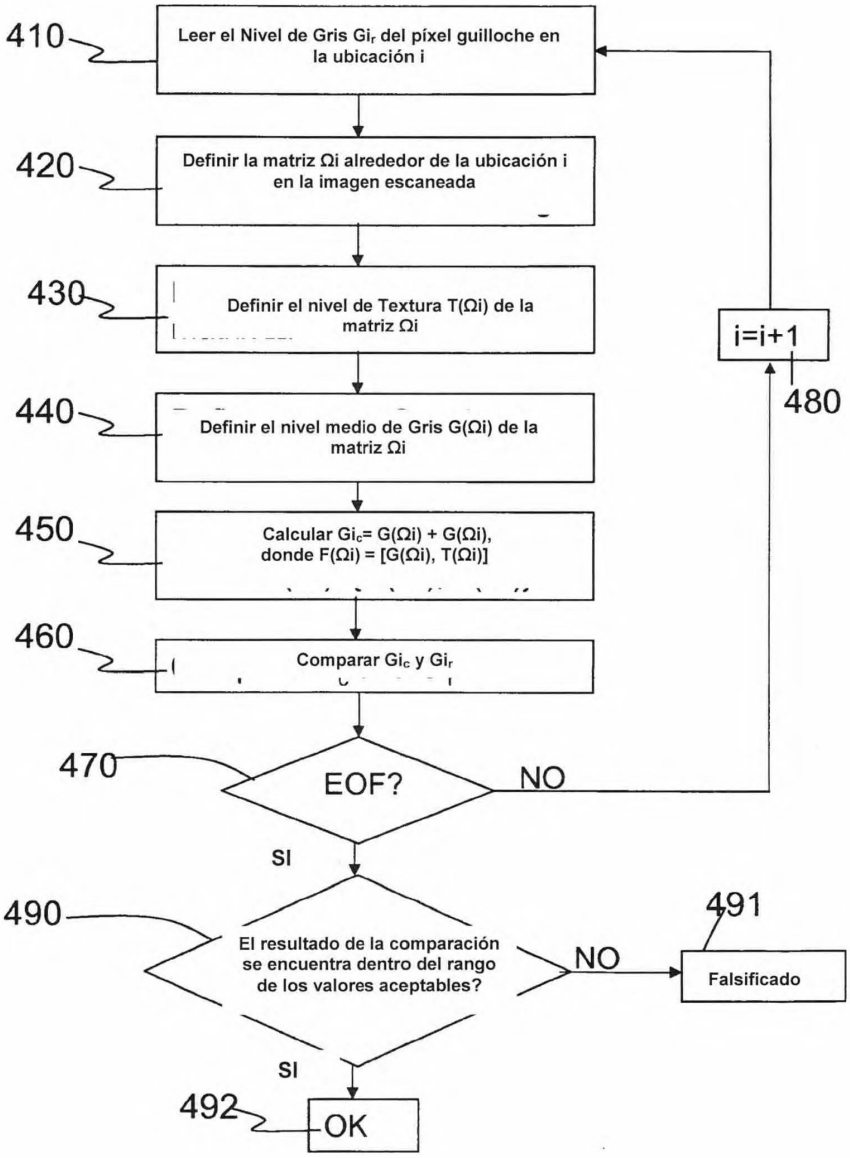
410
Leer el Nivel de Gris Gi$_r$ del píxel guilloche en la ubicación i
420
Definir la matriz Ωi alrededor de la ubicación i en la imagen escaneada
430
Definir el nivel de Textura T(Ωi) de la matriz Ωi
440
Definir el nivel medio de Gris G(Ωi) de la matriz Ωi
450
Calcular Gi$_c$= G(Ωi) + G(Ωi), donde F(Ωi) = [G(Ωi), T(Ωi)]
460
Comparar Gi$_c$ y Gi$_r$
470
EOF?
NO
SI
490
El resultado de la comparación se encuentra dentro del rango de los valores aceptables?
NO
491
Falsificado
SI
492
OK
i=i+1
480

Figura 6