(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 756 375**

(51) Int. CI.:

G06K 19/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.09.2009 PCT/FR2009/001096**

(87) Fecha y número de publicación internacional: **01.04.2010 WO10034897**

(96) Fecha de presentación y número de la solicitud europea: **15.09.2009 E 09752394 (8)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 2364485**

(54) Título: **Procedimiento y dispositivo de autentificación de códigos geométricos**

(30) Prioridad:

23.09.2008 FR 0805214
27.11.2008 FR 0806673

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.04.2020

(73) Titular/es:

ADVANCED TRACK AND TRACE (100.0%)
99, Avenue de la Châtaigneraie
92504 Rueil-Malmaison Cedex, FR

(72) Inventor/es:

PICARD, JUSTIN;
SAGAN, ZBIGNIEW;
FOUCOU, ALAIN y
MASSICOT, JEAN-PIERRE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivo de autentificación de códigos geométricos

La presente invención se refiere a un procedimiento y a un dispositivo de autentificación de códigos geométricos. Se aplica, en particular, a los códigos de barras de una dimensión (denominados “1D”), de dos dimensiones (denominados “2D”), incluso de tres dimensiones (“3D”) y al Data Matrix (marca registrada).

El código Data Matrix es una simbología de código de barras bidimensional de alta densidad, que permite representar una cantidad considerable de información sobre una superficie reducida, hasta 2.335 caracteres alfanuméricos ó 3.116 caracteres numéricos, sobre aproximadamente 1 cm^2. El código Data Matrix se encuentra en dominio público. El Data Matrix se presenta en forma de una matriz constituida por puntos o cuadrados yuxtapuestos.

El código Data Matrix responde a la norma ISO IEC16022. Según esta norma, el símbolo Data Matrix puede contener niveles de robustez, conocidos con la denominación de verificación y corrección de error o “ECC” (acrónimo de “Error Check Correction”), diferentes que le permiten ser leído incluso estando parcialmente degradado u ocultado. Existen diversas variantes del Data Matrix admitidas por la norma: desde la ECC000 que no ofrece ninguna robustez si el símbolo está degradado, del mismo modo que los códigos de barras 1D (EAN 13...) hasta la ECC200 que ofrece el nivel de seguridad máximo (lectura posible de un símbolo ocultado hasta aproximadamente el 20%).

El campo principal de aplicación del Data Matrix es el marcado de piezas mecánicas o electrónicas muy pequeñas. Es utilizado, entre otros, por la NASA (acrónimo de “National Agency for Space and Aeronautics” o agencia nacional para la aeronáutica y el espacio), para el marcado de cada una de las piezas que componen los transbordadores espaciales. En las aplicaciones actuales, se utiliza para el franqueo del correo en ciertos países, como Suiza, y, más recientemente, para ciertas aplicaciones de telefonía móvil, llamándose entonces normalmente “Tag” (o etiqueta). Flashcode (marca registrada) es una implementación comercial privativa que utiliza la norma Data Matrix.

El Data Matrix ECC200 forma parte de las normativas adoptadas por la GS1 (acrónimo de “Global Standard” por normativa global) y un aviso reciente de la AFSSAPS (acrónimo de “Agencia Francesa de Seguridad Sanitaria de los Productos para la Salud”) indica que, de aquí a 2011, todos los medicamentos sometidos a una autorización de comercialización deberán constar, además de los avisos legales actuales, de un código 2D Data Matrix que contenga un cierto número de informaciones predefinidas.

El Data Matrix ha sido concebido para maximizar la cantidad de datos almacenables en forma de imagen, de tal manera que la descodificación por parte de máquinas, o lectores, de estos datos (sobre la base de una captura de imagen) sea rápida y fiable. Sin embargo, no se ha concebido para proteger los datos almacenados, a pesar de que esta problemática aparece cada vez más.

Así, la descodificación del Data Matrix se realiza según una normativa abierta, y no incorpora ninguna clave criptográfica para cifrar y/o aplicar una firma digital a los datos. No obstante, los datos del mensaje almacenado se pueden cifrar o firmar digitalmente antes de ser modulados para formar el Data Matrix. De este modo, se pueden garantizar el origen y la integridad de un mensaje, sin que le resulte posible a nadie falsificar un mensaje legítimo (modificar su contenido) o hacerse pasar por el autor de un mensaje legítimo.

No obstante, las técnicas criptográficas no ofrecen ninguna protección contra la reproducción exacta en su forma original, o “clonación”, de los datos de un Data Matrix. Sin embargo, en numerosas aplicaciones de antifalsificación, es esencial poderse proteger contra estas copias en su forma original, ya que el falsificador puede, sin dificultad, hacer una copia perfecta de un documento, embalaje u otro objeto que conste de un Data Matrix, si el mismo no contiene elementos anticopia. Ciertas aplicaciones de trazabilidad (en inglés: “track and trace”) permiten realizar un seguimiento, en todos los niveles de la cadena de distribución, de los productos por el código identificador contenido en el Data Matrix: así, pueden determinar la presencia de duplicados si un código identificador se encuentra más de una vez, o incluso determinar anomalías en la distribución si el código identificador apunta a un producto que debería encontrarse en otro lugar de la cadena de distribución.

Está claro que una trazabilidad unitaria en todos los niveles de la cadena de distribución es una ayuda contra la falsificación, incluso si, al final, la misma no permite determinar cuál de dos productos aparentemente idénticos es el original. No obstante, en la mayoría de los casos, un sistema de trazabilidad de este tipo es demasiado costoso, incluso llana y simplemente imposible de implementar debido a que el mismo debe estar centralizado para que dos productos que lleven el mismo Data Matrix encontrados en dos lugares diferentes se puedan identificar como tales.

Esta es la razón por la que los titulares de derechos que utilizan Data Matrix, usan normalmente otros medios para asegurarse de la autenticidad de un documento o producto. Por ejemplo, varias soluciones se basan en etiquetas protegidas, que combinan un autentificador tal como un holograma o un OVD (acrónimo de “Optically Variable Device” por dispositivo ópticamente variable) colocado en las proximidades del Data Matrix.

Lamentablemente, los medios utilizados son en general costosos y poco eficaces. Costosos porque varias de las tecnologías de autentificación requieren tecnologías avanzadas para la construcción de efectos ópticos. Poco eficaces porque, cada vez más, los efectos ópticos se pueden imitar con una precisión suficiente a un coste menor. Además, estos efectos no protegen intrínsecamente el código de identificación. Por ejemplo, si un conjunto de documentos que contiene el medio de autentificación es robado, se le pueden aplicar códigos Data Matrix arbitrarios.

El Data Matrix se puede "proteger" contra copias marcándolo, por ejemplo, con tintas especiales. No obstante, los falsificadores logran agenciarse tintas especiales cada vez más fácilmente, y esta solución no es verdaderamente segura, aún siendo costosa. Así, para muchas aplicaciones, los Data Matrix se marcan por ablación láser.

El documento US 2008/0252066 propone la impresión de códigos de barras 2D multicolor, cuya lectura y/o autentificación requieren la iluminación del código impreso por diferentes fuentes luminosas y/o filtros espectrales. Lamentablemente, la utilización de diversas tintas es costosa y compleja en cuanto a producción, y requiere medios especializados de captura de imagen para la detección, lo cual limita las posibilidades de autentificación. Por otra parte, un planteamiento de este tipo no ofrece una seguridad considerable contra un adversario determinado, el cual puede encontrar fácilmente los tipos de tintas utilizados, y determinar los códigos impresos con la iluminación espectral adecuada.

El documento US 2008/110990 propone la aplicación de una rotación al cabezal de impresión, cuyo efecto, posteriormente, puede ser detectado y medido sobre la base de una captura de imagen de una impresión de un código de barras. No obstante, este documento admite implícitamente que el procedimiento que describe no permite detectar más que las copias realizadas con un medio de impresión que no permita la rotación del cabezal de impresión. Así, esta invención, no ofrece una protección real contra falsificaciones realizadas con el mismo medio de impresión, y es restrictiva ya que impone la utilización de un medio de impresión particular, lo cual limita considerablemente su utilización.

El documento WO 2008/003964 propone métodos que permiten introducir un segundo nivel de información en los códigos de barras 1D y 2D haciendo variar los elementos portadores de información para que representen el segundo nivel de información, por ejemplo, aumentando o disminuyendo el tamaño de las celdas de un Data Matrix, o recortando, o no, los extremos de sus celdas negras. Este planteamiento resuelve una parte de los defectos de la técnica anterior, ya que el segundo nivel de información, que se puede utilizar para la autentificación, se introduce en el momento de la impresión, lo cual resulta práctico y poco costoso. Es seguro frente a falsificadores que ignoran la implementación de este procedimiento, y que no se dedican más que a duplicar el código de barras reproduciendo la información de primer nivel. Sin embargo, el segundo nivel puede ser copiado fácilmente en su forma original por un falsificador que tenga conocimiento de su presencia. En relación con esto, este documento indica que el segundo nivel de información puede ser copiado por un medio de impresión de buena calidad, incluso si la sensibilidad a la copia está aumentada al máximo (véase la página 12, líneas 9 a 12 de este documento).

La presente invención pretende remediar estos inconvenientes. En particular, se refiere a métodos que permiten incluir un segundo nivel de información, con el mismo procedimiento de impresión que imprime el código de barras, de manera que este segundo nivel de información es física y matemáticamente imposible de copiar, por contraposición a las enseñanzas del documento previamente citado.

A este efecto, según un primer aspecto, la presente invención tiene como objetivo un procedimiento de autentificación de un código con zonas geométricas de formas y/o colores variables en función de un mensaje, según la reivindicación 1.

Así, la presente invención permite autentificar directamente un código de barras 2D, sobre la base de una imagen del mismo, mediante medios puramente digitales, aunque dejando inteligible este código de barras 2D.

Cabe recordar aquí que los códigos digitales autentificadores, denominados también en lo sucesivo "CNA", son imágenes digitales que, una vez marcadas sobre un soporte, por ejemplo por impresión o modificación local del soporte, presentan propiedades en general medibles automáticamente a partir de una imagen captada, que son modificadas durante su copia. Los códigos digitales autentificadores se basan en general en la degradación de por lo menos una señal sensible a la copia, siendo adaptada dicha señal por elementos de imagen a las características medibles sensibles a la copia.

Así, una zona geométrica que consta de una parte del código digital autentificador presenta una característica de marcado variable adaptada para quedar globalmente deteriorada durante una copia de dicha zona geométrica.

Ciertos tipos de códigos digitales autentificadores pueden contener también información que permite identificar o realizar un seguimiento del documento que la contiene. Los CNA son extremadamente ventajosos para la detección de copias. En efecto, son extremadamente poco costosos de producir, muy fáciles de integrar, y pueden ser leídos por una máquina que tenga medios de captura de imágenes, aún pudiendo ofrecer una gran seguridad contra las copias. Gracias a la implementación de la presente invención, un código con zonas geométricas, por ejemplo de barras, está vinculado de manera indisociable a un CNA.

Se observa que la presente invención presenta ventajas con respecto a la simple yuxtaposición de un código con zonas geométricas y de un CNA. Por una parte, este último planteamiento supondría la impresión de dos códigos en dos momentos diferentes sobre el documento, lo cual consumiría espacio y haría que el procedimiento de producción de los documentos protegidos fuese más complejo. Por otra parte, la autentificación requeriría la captura de dos imágenes, una del CNA y otra del código con zonas geométricas, lo cual haría que el procedimiento se lectura resultase menos práctico. Finalmente, un falsificador que logre agenciarse un cierto número de documentos dotados del CNA antes de la impresión del Data Matrix, o que logre agenciarse la placa de impresión o un archivo que contenga el CNA de origen, estaría en condiciones de generar documentos “auténticos”, clonando Data Matrix auténticos asociados al CNA.

Cabe observar que la etapa de formación de una imagen puede constar, por ejemplo, de una impresión, de una ablación de material, de una transferencia sólida o de una modificación física o química local, por ejemplo bajo el efecto del calor.

Según características particulares, la etapa de formación de una imagen afecta, debido a contingencias físicas de la formación de imágenes, a la representación del código digital autentificador en una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado.

Cabe recordar aquí que los códigos digitales autentificadores (“CNA”) están compuestos por diferentes elementos que adoptan valores discretos. En el caso de valores binarios, los elementos se pueden representar por una celda de un color negro (impresa) o blanco (no impresa). Durante la detección, se determina una tasa de errores que se corresponde con la tasa de celdas que contienen un valor incorrecto. Cabe señalar que la tasa de errores está vinculada directamente con la relación de la energía de la señal con respecto a la energía del ruido.

Por ejemplo, el primer valor predeterminado es igual al 10% y el segundo valor predeterminado es igual al 35%.

Según la reivindicación 2, la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, entre dos formaciones del mismo código con zonas geométricas variables, a la representación del código digital autentificador en una variación superior a un tercer valor predeterminado e inferior a un cuarto valor predeterminado.

Por ejemplo, el tercer valor predeterminado es igual al 2% y el cuarto valor predeterminado es igual al 45%.

Según la reivindicación 3, la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador con un ruido de tal manera que la relación de la señal con respecto al ruido de la representación del código digital autentificador es inferior a un quinto valor predeterminado.

Según características particulares, la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador con un ruido de tal manera que la relación de la señal con respecto al ruido de la representación del código digital autentificador es superior a un sexto valor predeterminado.

Por ejemplo, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,05 y el sexto valor predeterminado es igual a 2,63, dando como resultado un rendimiento de detección de copias de por lo menos el 25% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

Por ejemplo, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,11 y el sexto valor predeterminado es igual a 1,8, dando como resultado un rendimiento de detección de copias de por lo menos el 75% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

Por ejemplo, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,32 y el sexto valor predeterminado es igual a 0,93, dando como resultado un rendimiento de detección de copias de por lo menos el 90% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

Según la reivindicación 4, el procedimiento objeto de la presente invención, tal como se ha expuesto brevemente más arriba en la presente, consta, además, de:

- una etapa de determinación de condiciones de formación de dicha imagen y

- una etapa de determinación de características físicas de celdas de por lo menos una parte del código digital autentificador, en función de las condiciones de formación de la imagen.

Según la reivindicación 5, en el transcurso de la etapa de generación de dicho código con zonas geométricas variables, las zonas geométricas variables son barras en general rectangulares paralelas cuya anchura y/o separación varía en función de dicho mensaje.

Así, la presente invención se aplica a códigos de barras de una dimensión.

Según la reivindicación 6, en el transcurso de la etapa de generación de dicho código con zonas geométricas variables, las zonas geométricas variables son zonas cuadradas introducidas en una matriz cuyo color y/o por lo menos una de cuyas dimensiones varía en función de dicho mensaje.

Así, la presente invención se aplica a códigos de barras de dos dimensiones.

Según la reivindicación 7, en el transcurso de la etapa de formación de la imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas, de una parte de dicho código digital autentificador, el código digital autentificador adopta la forma de una variación de por lo menos una dimensión de zonas geométricas variables.

Según la reivindicación 8, en el transcurso de la etapa de formación de la imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas, de una parte de dicho código digital autentificador, cada parte del código digital autentificador introducida en una zona geométrica del código con zonas geométricas variables, adopta la forma de una distribución de celdas rectangulares de por lo menos un orden de magnitud más pequeño que las dimensiones de dicha zona geométrica, presentando una parte de dichas celdas un color diferente del correspondiente de dicha zona geométrica.

Según la reivindicación 9, en cada zona geométrica que consta de una parte del código digital autentificador, la superficie de dichas celdas es inferior a un cuarto de la superficie de dicha zona geométrica.

Según características particulares, el procedimiento objeto de la presente invención, tal como se ha expuesto brevemente más arriba en la presente, consta, además, de una etapa de codificación de una información en dicho código digital autentificador.

Según características particulares, dicha información es función de dicho mensaje y/o dicho mensaje es función de dicha información.

Se refuerza así la autentificación ya que no se puede modificar el mensaje sin modificar la información que lleva el CNA y/o a la inversa.

Según características particulares, dicha información es representativa de una medición de degradación del código digital autentificador debida a las contingencias físicas que afectan a la imagen durante la etapa de formación de una imagen.

Por ejemplo, la información es representativa de una tasa de errores debido a la etapa de formación de una imagen, de una relación de la señal con respecto al ruido debida a la etapa de formación de una imagen o de una tasa de correlación con un código digital autentificador de origen. Esta información puede representar un nivel de degradación esperado o un nivel de degradación límite más allá del cual el código se considerará como una copia. Así, la autentificación de la imagen se puede realizar de manera autónoma, por medio de un lector adaptado para captar una imagen del código digital autentificador introducido en el código con zonas geométricas variables ya que el mismo indica, por medio de la información de la cual es portador, el nivel de degradación normal y, consecuentemente, a partir de qué nivel de degradación una imagen captada representa una copia del código digital autentificador.

Según características particulares, el procedimiento objeto de la presente invención consta, además, de una etapa de medición de degradación del código digital autentificador generado en el transcurso de la etapa de formación de una imagen.

Según características particulares, en el transcurso de la etapa de medición de degradación, se implementan códigos de detección de errores integrados en dicho código digital autentificador.

Dicha medición, o “puntuación” es, por ejemplo, el porcentaje de bits determinados correctamente, una tasa de correlación entre el CNA de origen y el CNA captado en una imagen captada por un sensor de imágenes.

Según la reivindicación 10, el procedimiento objeto de la presente invención, tal como se ha expuesto brevemente más arriba en la presente, consta de una etapa de determinación de una huella de la imagen generada, siendo dicha huella función de una degradación del código digital autentificador en el transcurso de la etapa de formación de una imagen.

Así, el código o documento que es portador del código con zonas geométricas variables se puede identificar, es decir, reconocer, incluso si el código con zonas geométricas variables y el código digital autentificador son idénticos para una pluralidad de objetos o documentos.

De acuerdo con un segundo aspecto, la presente invención tiene como objetivo un dispositivo de autentificación de un código con zonas geométricas de formas y/o colores variables en función de un mensaje, según la reivindicación 12.

Según un tercer aspecto (reivindicación 13), la presente invención tiene como objetivo un procedimiento de

autentificación de un código con zonas geométricas de formas y/o colores variables, representado por una imagen captada, caracterizado por que el mismo consta de:

- una etapa de lectura de un mensaje portado por las formas y colores medios de las zonas geométricas,

- una etapa de medición de un nivel de degradación de un código digital autentificador representado en por lo menos una parte de las zonas geométricas de dicho código con zonas geométricas y

- una etapa de determinación de la autenticidad de dicho código con zonas geométricas en función de por lo menos dicho nivel de degradación.

Según un cuarto aspecto (reivindicación 14), la presente invención tiene como objetivo un dispositivo de autentificación de un código con zonas geométricas de formas y/o colores representado por una imagen captada, caracterizado por que el mismo consta de:

- un medio de lectura de un mensaje portado por las formas y colores medios de las zonas geométricas,

- un medio de medición de un nivel de degradación de un código digital autentificador representado en por lo menos una parte de las zonas geométricas de dicho código con zonas geométricas y

- un medio de determinación de la autenticidad de dicho código con zonas geométricas adaptado para determinar la autenticidad de dicho código con zonas geométricas variables en función de por lo menos dicho nivel de degradación.

Según un quinto aspecto (reivindicación 15), la presente invención tiene como objetivo un código con zonas geométricas de formas y/o colores variables en función de un mensaje, que representa:

- un mensaje por medio de las zonas geométricas; caracterizado por que representa:

- un código digital autentificador, en por lo menos una parte de sus zonas geométricas, mediante una característica de marcado variable en función de dicho código digital autentificador, presentando el código digital una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado después de la formación.

Al ser similares las ventajas, finalidades y características particulares de estos dispositivos, de este procedimiento y de este código objetos de la presente invención, a las correspondientes del procedimiento de autentificación objeto del primer aspecto de la presente invención, tal como se ha expuesto brevemente más arriba en la presente, las mismas no se reiteran aquí.

Se pondrán de manifiesto otras ventajas, finalidades y características particulares de la presente invención a partir de la descripción que se ofrece seguidamente, con una finalidad explicativa y en absoluto limitativa, en relación con los dibujos adjuntos, en los cuales:

- la figura 1A representa un Data Matrix conocido en la técnica anterior,

- la figura 1B representa una ampliación del Data Matrix ilustrada en la figura 1A,

- las figuras 2A y 3A representan modos de realización particulares de los códigos objeto de la presente invención, aportándose ampliaciones de partes de estos códigos en las figuras 2B y 3B, respectivamente,

- las figuras 4 a 7 representan, en forma de diagramas de flujo, etapas implementadas en modos de realización particulares de los procedimientos objeto de la presente invención,

- la figura 8 representa, esquemáticamente, un modo de realización particular del dispositivo objeto de la presente invención,

- la figura 9A representa un modo de realización particular de un código objeto de la presente invención, ofreciéndose una ampliación de una parte de este código en la figura 9B y

- la figura 10 representa el rendimiento de detección de copias normalizado con respecto al valor óptimo, en función de la relación de la señal con respecto al ruido.

Durante toda la descripción, se utilizan de manera indiferente los términos de “formación de una imagen” o “de impresión” para designar la formación de una marca detectable, por ejemplo por depósito de tinta, ablación de material, transferencia de polvo sólido o una modificación física o química local, por ejemplo bajo el efecto del calor.

Aunque la descripción que sigue se realiza para el caso de códigos de barras de dos dimensiones, la presente invención no se limita a este tipo de marcado e impresión sobre objetos sino que se extiende, muy al contrario, a todos los tipos de marcados y de impresión de códigos con zonas geométricas de formas y/o colores variables en función de un mensaje, especialmente los códigos de barras de una, dos o tres dimensión(es) formados en la

superficie de los objetos y los marcados bajo la superficie de los objetos.

En el caso de los códigos de barras de una dimensión, las zonas geométricas del código son barras verticales rectangulares alternativamente blancas y negras cuya anchura varía en función del mensaje que lleva el código.

En el caso de los códigos de barras de dos dimensiones, las zonas geométricas del código son cuadrados que forman una cuadrícula regular, cuyo color varía en función del mensaje portado por el código.

En lo sucesivo en la descripción, a estas zonas geométricas se les denomina “celdas”.

A continuación en la presente se describen, en particular, métodos y dispositivos para autentificar directamente códigos de barras 2D (denominados también Data Matrix) y, en especial, para autentificar códigos de barras 2D imprimidos por integración de un código digital autentificador “CNA”, marcados por láser de intensidad modulable y por láser de intensidad fija.

Por lo que respecta a la integración de un CNA en un código de barras 2D, se describe, posteriormente en la presente, con respecto a la figura 4, un método para generar un Data Matrix que consta de un CNA integrado. Cabe señalar que los parámetros de generación recomendados del CNA, en particular la resolución en píxeles por pulgadas y el tipo de celda utilizado (es decir, la forma y/o el tamaño de los elementos que componen el CNA, se han determinado anteriormente para el procedimiento de impresión (papel, tinta, máquina impresora, documento), por ejemplo utilizando un método conocido.

Por lo que respecta al método de determinación de los parámetros óptimos de formación de imágenes de los patrones identificadores, existe una tasa de degradación óptima que permite separar de la manera más sencilla posible las diferentes impresiones de un mismo patrón identificador de origen. Así, si la tasa de degradación en la impresión es muy débil, por ejemplo un 1% ó un 2% (un 1 ó 2% de las celdas o píxeles del patrón identificador son leídas incorrectamente a partir de una captura perfecta), las diferentes impresiones de un mismo patrón identificador están muy próximas entre sí, y resulta difícil identificarlas de manera fiable, a no ser que se disponga de una captura muy precisa de la imagen y/o un algoritmo de análisis muy preciso. De manera similar, cuando la tasa de degradación es muy elevada, por ejemplo, del 45 al 50% (el 45 ó 50% de las celdas de la matriz de información protegida son leídas incorrectamente a partir de una captura perfecta, de modo que un 50% significa que no hay ninguna correlación estadística entre la matriz leída y la matriz de origen), los patrones identificadores imprimidos son casi indistintos unos con respecto a otros. En realidad, la tasa de degradación óptima es próxima al 25%, y si las condiciones de la aplicación lo permiten, es preferible aproximarse a ella. En efecto, para un 25% de degradación, suponiendo que las variaciones de impresión y, por tanto, las degradaciones sean de carácter probabilístico, en cada uno de los puntos del patrón identificador impreso se aumentan al máximo las posibilidades de que el mismo difiera con respecto a otros patrones identificadores impresos.

Posteriormente en la presente se ofrece un segundo análisis de las tasas de errores que deben buscarse en el momento de la formación de una imagen a imprimir en función de los medios de impresión a implementar.

Cabe recordar aquí que los códigos digitales autentificadores (“CNA”) están compuestos por diferentes elementos que adoptan valores discretos. En el caso de valor binarios, los elementos se pueden representar mediante una celda de un color negro (impresa) o blanco (no impresa). Durante la detección, se determina una tasa de errores que se corresponde con la tasa de celdas que contienen un valor incorrecto. Cabe señalar que la tasa de errores está vinculada directamente a la relación de la energía de la señal con respecto a la energía del ruido.

Con el fin de determinar cómo se pueden generar MPCV que permitan optimizar la detección de copias, presentamos a continuación en la presente un modelo basado en la teoría de la decisión. Las características medidas sobre las imágenes (o puntos) se representan mediante señales. Para simplificar el análisis, se plantea la hipótesis de que las señales digitales, antes de la impresión, tienen valores binarios, que se corresponden con características que pueden tener valores binarios (por ejemplo, dos tamaños de puntos, dos posiciones, etcétera). Esta hipótesis se justifica por el hecho de que la mayor parte de los procedimientos de impresión procesan imágenes binarias. Evidentemente, las conclusiones del análisis se pueden ampliar a casos más complejos, en particular con varios valores posibles de características de punto. La impresión del MPCV se modeliza con la adición de ruido Gaussiano. Se supone asimismo que las copias se realizan con el mismo procedimiento de impresión, de manera que la impresión de la copia se modeliza también con la adición de ruido Gaussiano de la misma energía. Además, al falsificador, que capta la señal antes de imprimir una copia de la misma, se le obliga a reconstruir una señal binaria obteniendo una estimación del valor inicial que reduce al mínimo su probabilidad de error.

Este modelo se corresponde directamente con MPCV que pueden tener tamaños de punto de 1x1 píxel ó 1x2 píxeles (imprimido, por ejemplo, a 2.400 dpi), para lo cual el falsificador debe escoger necesariamente uno de los tamaños de punto dentro de la imagen reconstruida a partir de un escaneo, en función de un nivel de gris medido o una superficie estimada del punto. El modelo se corresponde asimismo con MPCV con posiciones que varían en 1 píxel, por ejemplo.

A partir de este modelo, se obtienen el detector óptimo, la distribución estadística de los valores del detector, y los valores de parámetro que aumentan al máximo la detección de copias.

La siguiente tabla resume las diferentes variables.

s	Señal de origen
n,n_c	Ruido, ruido copia
x	Señal recibida

Sin pérdida de generalidad, la señal de origen es equiprobable, es decir $s[i]: \{+a,-a\}$ para $i = 0,1,...N$-1, y $a > 0$. El ruido de impresión se distribuye según una ley Gaussiana $N(0,\sigma^2)$.

Las hipótesis del modelo se resumen así:

$$(H0)x[i]:\{+a,-a\} \quad (1)$$

$$(H1)n[i]:N(0,\sigma^2) \quad (2)$$

$$(H2)n_c[i]:N(0,\sigma^2) \quad (3)$$

Se puede verificar fácilmente que el falsificador minimiza su probabilidad de error restaurando la señal al valor más próximo entre $+a,-a$.

Consecuentemente, el problema de detección consiste en distinguir las dos hipótesis siguientes:

$$H_0 : x[i] = s[i] + n[i] \quad (4)$$

$$H_1 : x[i] = a.sign(s[i] + n[i]) + n_c[i] \quad (5)$$

donde H_0 y H_1 son las hipótesis de que la señal recibida es un original, respectivamente, una copia.

La probabilidad de que el falsificador ha estimado correctamente el valor es:

$$p(sign(s[i]+n[i]) = s[i]) = p(s[i]+n[i] > 0) \quad (6)$$

$$= p(N(a,\sigma^2) > 0) \quad (7)$$

$$= p(N(0,1) > -a/\sigma) \quad (8)$$

$$= Q(-a/\sigma) \quad (9)$$

donde $Q(x) = (2\pi)^{-1/2} \int_{-a/\sigma}^{+\infty} \exp^{-x^2/2} dx.$

Disponemos de las siguientes distribuciones de probabilidad para la señal recibida, donde en la hipótesis H_1 tenemos una mezcla de dos distribuciones Gaussianas.

$$p(x;H_0) = \frac{1}{(2\pi\sigma^2)^{N/2}} \exp[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n]-s[n])^2] \quad (10)$$

$$p(x;H_1) = (1-Q(-a/\sigma))\frac{1}{(2\pi\sigma^2)^{N/2}} \exp[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n]+s[n])^2] + \quad (11)$$

$$Q(-a/\sigma)\frac{1}{(2\pi\sigma^2)^{N/2}} \exp[-\frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n]-s[n])^2] \quad (12)$$

Vamos a verificar que un correlador simple ofrece una función de clasificación óptima. Una prueba de detector de Neyman-Pearson decide H_1 si la razón de verosimilitud supera un umbral t:

$$L(\mathbf{x}) = \frac{p(\mathbf{x};H_1)}{p(\mathbf{x};H_0)} > t \quad (13)$$

La razón de verosimilitud viene dada por:

$$L(\mathbf{x}) = Q(-a/\sigma) + (1 - Q(-a/\sigma)) \exp[-\frac{1}{2\sigma^2}(\sum_{n=0}^{N-1}(x[n]+s[n])^2 + \frac{1}{2\sigma^2}\sum_{n=0}^{N-1}(x[n]-s[n])^2] \quad (14)$$

Sacando el logaritmo, y un umbral nuevo *t'*, se obtiene:

$$T'(x,s) = \sum_{n=0}^{N-1} x[n]s[n] < t' \quad (15)$$

La función de clasificación es, por tanto, un correlador simple T', cuyo valor debe ser inferior a un umbral t' para clasificar la señal como copia.

Determinamos los estadísticos de T' para las dos hipótesis. Podemos suponer que T' sigue una Gaussiana (verdadero para N elevado) de la cual obtenemos las medias y varianzas para las dos hipótesis:

$$E[T'; H_0] = Na^2 \quad (16)$$

$$E[T'; H_1] = Q(-a/\sigma)Na^2 - (1 - Q(-a/\sigma))Na^2 = (2Q(-a/\sigma) - 1)Na^2 \quad (17)$$

$$Var[T'; H_0] = Na^2\sigma^2 \quad (18)$$

$$Var[T'; H_1] = N(a^2\sigma^2 + a^4 Q(-a/\sigma)(1 - Q(-a/\sigma))) \quad (19)$$

El segundo término de la varianza para la hipótesis H_1, $(a^4Q(-a/\sigma)/1-Q(-a/\sigma)))$, se puede eliminar si las copias vienen del mismo original. En la práctica, el falsificador minimiza su trabajo no utilizando más que un original para producir un número elevado de copias, y es razonable eliminar el término.

En caso de que las varianzas sean iguales, el rendimiento de detección se puede caracterizar por el coeficiente de desviación d^2, que se corresponde con la diferencia entre las medias de la función T' para las dos hipótesis, normalizada por la varianza de T':

$$d^2 = \frac{(E[T'; H_0] - E[T'; H_1])^2}{Var[T'; H_0]} \quad (22)$$

$$= \frac{2N^2a^4(1 - Q(-a/\sigma))^2}{Na^2\sigma^2} \quad (23)$$

$$= \frac{2Na^2(1 - Q(-a/\sigma))^2}{\sigma^2} \quad (24)$$

$$= 2N\gamma(1 - Q(-\sqrt{\gamma}))^2 \quad (25)$$

donde $\gamma = a^2/\sigma^2$ es la raíz cuadrada de la relación de la señal con respecto al ruido.

Al aumentar el rendimiento de detección con el coeficiente de desviación, el objetivo consiste en determinar el valor de γ que maximiza la expresión $(\gamma(1-Q(\gamma)))^2$.

La Figura 10 representa el valor de la expresión de la ecuación (25) para un valor de N fijo, normalizado sobre su valor óptimo y obtenido en función de γ. Se puede interpretar de la manera siguiente. Los valores de γ cerca de cero se corresponden con un ruido muy elevado con respecto a la señal: cuando el ruido es muy elevado, la señal se degrada demasiado desde la primera impresión, el falsificador introduce un número de errores de estimación demasiado pequeño. Por el contrario, para valores de γ demasiado elevados, la señal no se degrada suficientemente, y, en una proporción demasiado grande de los casos, el falsificador no introducirá ningún error de estimación. Entre los dos extremos, la expresión pasa por un valor óptimo, cuyo valor se estima numéricamente en $\gamma \approx 0{,}752$.

Es interesante observar que, para este valor, la probabilidad de que el falsificador no haya determinado correctamente el valor, es de aproximadamente el 22,6%.

En la práctica, se trata de obtener, durante la impresión, una relación de la señal con respecto al ruido γ^2 lo más próxima posible a $0{,}752^2$, es decir 0,565.

Tomemos un ejemplo para entender mejor cómo buscar este valor de la relación. Supongamos que generamos un MPCV con dos tamaños de punto (expresados en número de píxeles) posibles, siendo el tamaño de punto del orden de nueve píxeles (por ejemplo, 3x3 píxeles). Cabe observar que el tamaño de punto se puede medir implementando una multitud de algoritmos, por ejemplo, por umbralización adaptativa local del nivel de gris y recuento de los píxeles por debajo del umbral. Se imprimen un número suficiente de veces puntos de nueve píxeles. En una imagen capturada, se miden la media y la desviación estándar del número de píxeles de cada punto. Supongamos que se obtiene una media de doce (se observa una ganancia física media del 33%), y una desviación estándar de cuatro. Esta desviación estándar se corresponde con el valor σ que describe el ruido en las fórmulas de nuestro modelo. Se buscará entonces un valor de nuestra señal a del orden de tres, para obtener una relación γ = 0,75, es decir muy cerca del valor óptimo. Para obtener este valor de señal, se pueden definir, por ejemplo, dos tamaños de puntos de quince y de seis píxeles.

Preferentemente, la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador en una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado. Por ejemplo, el primer valor predeterminado es igual al 10% y el segundo valor predeterminado es igual al 35%.

Preferentemente, la etapa de formación de una imagen afecta, debido a las contingencias física de la formación de imágenes, entre dos formaciones del mismo código o con zonas geométricas variables, a la representación del código digital autentificador con una variación superior a un tercer valor predeterminado e inferior a un cuarto valor predeterminado. Por ejemplo, el tercer valor predeterminado es igual al 2% y el cuarto valor predeterminado es igual al 45%.

Preferentemente, la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador con un ruido de tal manera que la relación de la señal con respecto al ruido de la representación del código digital autentificador es inferior a un quinto valor predeterminado y, preferentemente, superior a un sexto valor predeterminado.

Según un primer ejemplo, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,05 y el sexto valor predeterminado es igual a 2,63, dando como resultado un rendimiento de detección de copias de por lo menos el 25% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

Más preferentemente, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,11 y el sexto valor predeterminado es igual a 1,8, dando como resultado un rendimiento de detección de copias de por lo menos el 75% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

Todavía más preferentemente, el quinto valor predeterminado de la relación de la señal con respecto al ruido es igual a 0,32 y el sexto valor predeterminado es igual a 0,93, dando como resultado un rendimiento de detección de copias de por lo menos el 90% del rendimiento óptimo de detección de copias (obtenido para un valor de 0,56).

A continuación en la presente se describe un algoritmo posible de optimización de los parámetros de impresión:

- en el transcurso de una etapa 720, se recibe la superficie disponible para el patrón identificador, por ejemplo un cuadrado cuyo lado mide 1/6 de pulgada,

- en el transcurso de una etapa 721, se generan varias imágenes digitales de patrones identificadores de dimensiones numéricas diferentes, que se corresponden con las diferentes resoluciones de impresión posibles, por ejemplo un patrón identificador de 66 x 66 píxeles a 400 puntos por pulgada, uno de 100 x 100 píxeles a 600 puntos por pulgada, uno de 133 x 133 píxeles a 800 puntos por pulgada, uno de 200 x 200 píxeles a 1.200 puntos por pulgada,

- en el transcurso de una etapa 722, se imprime varias veces cada uno de los patrones identificadores de dimensiones numéricas diferentes, por ejemplo 100 veces, con la resolución adecuada de manera que las dimensiones de la impresión se corresponden con la superficie disponible,

- en el transcurso de una etapa 723, para cada tipo, se captura varias veces cada uno de los patrones identificadores impresos, por ejemplo, 3 veces,

- en el transcurso de una etapa 724, se calcula la huella de cada patrón identificador, siendo función dicha huella de una degradación del código digital autentificador en el transcurso de la etapa de formación de una imagen, siendo dicha huella en general única para cada imagen formada debido al aspecto aleatorio de cada error individual,

- en el transcurso de una etapa 725, se calculan las puntuaciones de similitud para todos los pares de patrón identificador capturados con la misma resolución de impresión y

- en el transcurso de una etapa 726, se sigue el método descrito en la experimentación del método de extracción de huella genérico expuesto más arriba para medir el “grado de separación de las huellas”, para cada una de las resoluciones de impresión, y escoger la resolución de impresión que ofrece el valor máximo de este grado.

En una variante, se imprimen varias matrices de información protegidas con diferentes resoluciones de impresión, y se determina la resolución de impresión que da como resultado una tasa de errores del 25%, según se calcula con uno de los algoritmos descritos por otro lado.

En una variante, se selecciona la resolución de impresión cuya diferencia es la más elevada entre el valor más bajo de puntuación calculado sobre la comparación entre las huellas correspondientes a impresiones idénticas, y el valor más alto de puntuación calculado sobre la comparación entre las huellas correspondientes a impresiones diferentes.

Tal como se ilustra en la figura 4, en el transcurso de una etapa 105, se reciben uno o varios mensajes, una o varias claves, un tamaño físico de Data Matrix y una resolución de impresión.

En el transcurso de una etapa opcional 110, se determinan, a partir de las claves y los mensajes, el mensaje o mensajes codificados que se introducirán en el CNA. En particular, los mensajes del CNA se pueden poner en correlación con el mensaje representado por el Data Matrix, siendo uno (en parte) función del otro, con el fin de reforzar la autentificación.

En el transcurso de una etapa 115, se genera un Data Matrix a partir de por lo menos uno de los mensajes recibidos en el transcurso de la etapa 105.

En el transcurso de una etapa 120, se determina el número de celdas negras del Data Matrix, pudiendo estar incluidos o no los patrones de alineación (conocidos con la denominación de “finder pattern”) en el Data Matrix. En el transcurso de una etapa 125, en función del número de celdas negras, de la resolución de impresión y del tamaño físico, se determina el número de elementos del CNA.

En el transcurso de una etapa 130, en función del número de elementos, de las claves y de los mensajes, se determinan, utilizando un algoritmo de generación de CNA, los valores adoptados por cada uno de los elementos del CNA. Cabe observar aquí que los algoritmos de generación de CNA constan normalmente de etapas de cifrado, de codificación, de repetición y de aleatorización (“scrambling”) (por ejemplo con permutación y/o sustitución).

En el transcurso de una etapa 135, se crea la imagen digital del Data Matrix, inscribiendo los valores del CNA según un orden predeterminado (por ejemplo, de izquierda a derecha y a continuación de arriba a abajo) en los píxeles correspondientes al número de celdas negras.

En el transcurso de una etapa 140, se imprime o se marca un objeto para formar en el mismo la imagen digital del Data Matrix que incorpora el CNA.

A continuación en la presente se ofrece un ejemplo en el cual se ha generado el Data Matrix 150 ilustrado en la figura 1 según un algoritmo convencional, a partir de un mensaje. El Data Matrix 150 tiene el tamaño de 26x26 celdas incluyendo los patrones de alineación, y contiene 344 celdas negras, siempre incluyendo los patrones de alineación.

Deseamos imprimirlo con un medio de impresión que permite una resolución de 600 píxeles por pulgada (“ppi”), y que ocupe una superficie de 1 cm x 1 cm aproximadamente. El tamaño en píxeles de la imagen equivalente a 1 cm es de 236 x 236 píxeles, es decir 236 píxeles para 26 celdas y 9.07 píxeles/celda (en cada dimensión). Redondeando a nueve píxeles por celda en cada dimensión, se obtiene un tamaño del Data Matrix en píxeles de 234 x 234 (ya que 26 x 9 = 234), y se dispone de 9 x 9 = 81 píxeles por celda.

Como tenemos 344 celdas negras, un CNA generado sobre el conjunto de las celdas negras puede contener 81 x 344 = 27.864 píxeles. Se puede generar, por tanto, un CNA que contiene un bit por píxel, con lo que el CNA contendrá 27.864 bits. Se genera el CNA a partir de las claves y mensajes según algoritmos conocidos, y se introducen los valores del CNA en las celdas negras.

La figura 2 muestra un Data Matrix 160 objeto de la presente invención generado a partir del Data Matrix 150, en el cual un CNA está distribuido sobre el conjunto de las celdas negras. Según el medio de impresión, la tinta o el papel u otro soporte, puede ser que el Data Matrix no tenga la calidad requerida para la descodificación, por ejemplo por que el mismo conste de “agujeros” en el nivel de las celdas. Para remediar esto, en una variante, se selecciona un subconjunto de los píxeles entre las celdas negras para que lleven los valores del CNA. Por ejemplo, se toma uno de cada dos píxeles, manteniéndose negros los píxeles no seleccionados, para tener una tasa media del 75% de píxeles negros por celda. Así, se tiene un CNA de 27.864 / 2 =13.932 bits. La figura 3 muestra un Data Matrix 170 de este tipo. Igualmente, se puede seleccionar un subconjunto de los píxeles de las celdas negras a partir de una clave criptográfica.

Es preferible que la inteligibilidad del Data Matrix no se vea afectada significativamente por las modificaciones efectuadas. A título de ejemplo, los inventores han imprimido con una impresora láser de oficina los Data Matrix 150, 160 y 170 a la resolución de 600 ppi (tamaño de 1 cm.), y han utilizado el dispositivo de verificación de códigos de barras “TruCheck USB verifier” (marca registrada), que permite determinar el grado del Data Matrix. El Data Matrix 150, que sirve como referencia, obtiene un grado de “A”, mientras que los Data Matrix 160 y 170 obtienen, respectivamente, “B” y “A”. Haciendo notar que el Data Matrix 160 contiene más información que puede servir para

la autentificación (y/o para transportar un mensaje) que el Data Matrix 170, se observa que puede existir una relación inversa entre la calidad del Data Matrix, y la cantidad de información contenida en el nivel del CNA. En la práctica, el espacio disponible para la modulación del CNA depende del grado aceptable para la aplicación. En nuestro caso, si es aceptable un grado de "B" (en principio los grados por encima de "C" son aceptables), se toma preferentemente el Data Matrix 160 que consta de más información. Si solamente es aceptable el grado "A", se toma el Data Matrix 170. De lo contrario, se ajusta la tasa de aprovechamiento de la celda utilizada para buscar el grado mínimo requerido.

Para aumentar el número de elementos del CNA, se pueden aprovechar asimismo las zonas blancas (o no marcadas). Se trata entonces de conservar una densidad reducida de color para la zona blanca, de manera que la descodificación no se vea alterada. Por ejemplo, se puede aprovechar el 20% de los píxeles de las zonas blancas, excluyendo preferentemente el cerco de la zona que puede estar en contacto con una zona negra. Se observa que si el CNA posee valores binarios equiprobables, se tiene un 10% de los píxeles en valores medios que son negros, lo cual altera débilmente el índice de coloración de la celda. En nuestro ejemplo anterior, se utilizarían los 7x7 píxeles internos de la zona blanca, y se escogerían 10, de manera seudoaleatoria, conteniendo estos diez píxeles un elemento de CNA. Los elementos se pueden colocar únicamente sobre las columnas y filas pares, por ejemplo, para evitar que los mismos no se toquen. Estos elementos se pueden integrar en el CNA de las celdas negras, o considerarlo como otro CNA, lo cual ofrecer otro medio de autentificación. Las figuras 9A y 9B aportan un ejemplo 180 de Data Matrix del tipo mencionado para el cual las celdas blancas contienen también elementos autentificadores.

Se observa que los elementos de este CNA pueden tener también un tamaño variable, por ejemplo elementos de 1x2 píxeles y de 1x1 píxeles, para hacer que resulte más difícil la identificación de los elementos por parte de un falsificador que buscase reconstruir de manera perfecta el CNA de origen.

A continuación en la presente, se ofrece con respecto a la figura 5, un ejemplo de algoritmo para autentificar un Data Matrix impreso dotado de un CNA.

En el transcurso de una etapa 205, se recibe una imagen proveniente de una captura de imagen, por ejemplo con un escáner, conteniendo esta imagen el Data Matrix y, por tanto, el CNA. En paralelo, se reciben claves de descifrado, y los parámetros de lectura del CNA (por ejemplo, el tamaño en píxeles de cada celda), así como un umbral de decisión.

En el transcurso de una etapa 210, se descodifica el mensaje del Data Matrix portado por las formas y colores medios de las celdas cuadradas.

En el transcurso de una etapa 215, se determina si el mensaje del Data Matrix se ha leído correctamente, por ejemplo en función de los ECC integrados. En caso negativo, se considera que el Data Matrix no es auténtico y se le presenta visualmente al usuario: "Código no auténtico". Si el mensaje es leído correctamente, en el transcurso de una etapa 220, se crea una imagen del Data Matrix de origen.

A continuación, en el transcurso de una etapa 225, se determina el número de celdas negras, y, en función de los parámetros de lectura del CNA, se determina el número de elementos del CNA.

En el transcurso de una etapa 230, en función de la imagen del Data Matrix de origen y del número de elementos del CNA, se determina la posición (en términos de píxeles) en la imagen, de cada uno de los elementos del CNA. En el transcurso de una etapa 235, se extrae de la imagen un valor asociado al valor de cada elemento del CNA, por ejemplo el nivel de gris del píxel. Se obtiene así un vector de datos representativo del CNA impreso, y de las degradaciones que ha experimentado este último.

En el transcurso de una etapa 240, utilizando las claves de desaleatorización (en el caso en el que el CNA se hubiera aleatorizado), se descodifican el mensaje o mensajes del CNA.

En el transcurso de una etapa 245, se determina su puntuación representativa de la tasa de degradación del CNA. La puntuación es, por ejemplo, el porcentaje de bits determinados correctamente, una tasa de correlación entre el CNA de origen y el CNA medido a partir de la imagen captada, etcétera.

Opcionalmente, si, en el transcurso de su creación, los mensajes del CNA y del Data Matrix se sitúan en correlación, se verifica esta correlación en el transcurso de una etapa 250 y se le presenta visualmente al usuario "Data Matrix no autentificado" si es que los mismos no lo han sido.

Finalmente, en el transcurso de una etapa 255, se compara la puntuación medida con un valor límite predeterminado o "umbral de decisión". Si la misma es superior, por ejemplo debido a una tasa de errores reducida o una tasa de correlación elevada, se le presenta visualmente al usuario "Data Matrix autentificado". Si no, se presenta visualmente "Data Matrix no autentificado". Opcionalmente, se presenta visualmente cada mensaje leído.

En variantes, se reservan bits del CNA para la sincronización, según una manera conocida en sí misma.

Cabe señalar que el mismo Data Matrix puede ser imprimido o marcado varias veces en impresión estática (offset, flexografía, etcétera), o puede variar en cada impresión en la impresión digital.

En un segundo modo de realización, se implementa un sistema de marcado por láser y micropercusión para la integración de un CNA. Ciertos sistemas de marcado, especialmente de láser o de micropercusión, de un Data Matrix, no pueden utilizar imágenes de gran tamaño como se ha visto anteriormente. Por ejemplo, el marcado de una imagen de tamaño 236x236 píxeles como en el ejemplo anterior consumiría un tiempo demasiado grande, lo cual ralentizaría demasiado la cadencia de la línea de producción, o generaría códigos Data Matrix de gran tamaño. El modo de realización particular descrito a continuación en la presente pretende evitar estos inconvenientes.

Cabe señalar que, implementando un láser, son posibles varios métodos de realización de un Data Matrix:

- un impacto de láser puede crear cada celda,

- varios impactos de láser yuxtapuestos pueden crear cada celda, o

- una celda o agrupaciones de las celdas se pueden vectorizar y grabar mediante un disparo de láser continuo.

Además, cabe señalar que, en varios sistemas de marcado por láser, es posible hacer variar localmente las características de diferenciación siguientes:

- la intensidad del láser,

- la polarización del láser,

- la focalización del láser sobre la superficie a marcar,

- el microposicionamiento,

- la dirección, o el orden en el cual se marcan puntos por medio del láser y

- la forma del frente de onda.

Asimismo, en la micropercusión son posibles varios métodos de realización de un Data Matrix:

- un impacto de micropunta puede crear cada celda individual o

- varios impactos de micropunta yuxtapuestos pueden crear cada celda.

Asimismo, se puede utilizar la capacidad de varios sistemas de marcado por micropunta para hacer variar localmente las características de diferenciación siguientes:

- la fuerza del impacto,

- el microposicionamiento,

- la orientación de la micropunta y/o

- la forma de la micropunta.

Con el fin de optimizar el tiempo de ejecución de un Data Matrix compuesto por celdas diferenciadas (según los parámetros controlables del láser o del dispositivo de micropunta), las celdas se dividen en subconjuntos, o “clases”. Cada subconjunto de celdas cuyas características de diferenciación son idénticas se realiza preferentemente durante una sola pasada de la herramienta. Esto permite modificar el parámetro que diferencia el efecto de marcado una sola vez para cada subconjunto de las celdas, en lugar de hacerlo para cada celda individualmente. Cada parámetro que puede ser modificado localmente, y cuya variación tiene un impacto medible sobre el Data Matrix generado, se puede utilizar para almacenar información. Por ejemplo, si la intensidad del láser admite dos niveles, se puede almacenar un bit de información modulando la intensidad u otro parámetro de modulación del marcado. En una variante, también se pueden acumular variaciones sobre diferentes parámetros localmente variables.

En una variante, un parámetro puede variar localmente de manera casi continua, y entonces se puede determinar un número arbitrario de niveles para almacenar información. Por ejemplo, se implementan diez niveles para dicho parámetro (color o variaciones de dimensión, por ejemplo) en lugar de los dos descritos en la presente más arriba, e incluso se hace variar el valor de este parámetro de manera continua.

Sin embargo, en los ejemplos de implementación, resulta ventajoso no utilizar más que dos niveles de valores para la señal de origen. En este caso, se puede utilizar una relación óptima de la razón de la señal con respecto al ruido, de 0,56, para maximizar la detección de copias. Para buscar esta razón, se determinan las propiedades de ruido del canal, típicamente el par material-medio de impresión, caracterizando la distribución del valor medio de la señal sobre la captura de imagen. En el caso de dos niveles de energía, se examinará la distribución estática de las

magnitudes de impacto, para determinar dos niveles de energía suficientemente próximos para que se produzca una superposición parcial de las distribuciones, apuntando a la relación ideal de señal con respecto al ruido mencionada anteriormente en la presente. Concretamente, si para una energía de láser que ofrece unas magnitudes de impacto de 0,10 mm^2, se tiene una desviación estándar de 0,01 mm^2, se tomarán niveles de energía que ofrecen magnitudes de impacto medias próximas a 0,1075 mm^2 y 0,0925 mm^2. En efecto, se obtiene entonces una relación de la señal con respecto al ruido de $0,0075^2 / 0,01^2 = 0,5625$, muy cerca del valor óptimo teórico.

Así, en el caso de un Data Matrix de tamaño 26 x 26 celdas, se tienen 344 disparos de láser. Se genera un CNA de la misma manera que la vista anteriormente, y el CNA se modula mediante puntos de tamaño 0,1075 mm^2 y 0,0925 mm^2.

Tal como se ha visto anteriormente, se verifica si las variaciones introducidas no provocan una degradación del Data Matrix incompatible con las condiciones de la aplicación, por ejemplo un grado mínimo de “C” del Data Matrix.

En ciertos casos, no es posible modular una información suplementaria. Por ejemplo, el medio de impresión o de marcado solamente permite marcar o no una celda (marcado unitario binario). Asimismo, hay casos en los que la información suplementaria que se marca no ofrece una alta seguridad contra las copias. Por ejemplo, un medio de marcado que permite niveles predefinidos de marcado que permanecen diferenciados con respecto a los otros y claramente identificables en la imagen marcada permite introducir una información suplementaria, pero en principio la misma sigue pudiéndose copiar en su forma original.

En estos casos, se puede utilizar el ruido residual de impresión o de marcado, y aprovecharlo como CNA. En efecto, sea cual sea el tipo de impresión, a una cierta escala o resolución, aparecen ciertos “defectos”. Por ejemplo, si un impacto de láser deja, en principio, un punto de impacto de forma circular o elipsoidal, se observa en general, a una resolución suficientemente elevada, que el punto de impacto no tiene una forma perfectamente regular. Ocurre lo mismo si se utiliza un sistema de impresión por chorros de tinta. A una resolución todavía más elevada, se observan irregularidades en la profundidad del punto de impacto, y así sucesivamente.

Las irregularidades del marcado pueden ser captadas, medidas y servir para constituir un CNA. Se puede, entonces, almacenar el CNA en una base de datos, o se puede almacenar el mismo propiamente dicho en forma de código de barras 2D. Sin embargo, este último planteamiento resulta poco ventajoso, ya que el marcado de un segundo código es costoso y consume espacio en el documento, que es lo que se busca evitar en general. Por el contrario, el CNA se puede almacenar asociándolo al mensaje del Data Matrix que, si es único (lo cual preferentemente es así), permite, durante la etapa de autentificación, realizar una simple “verificación” por comparación de la medición de los defectos de marcado con el CNA. Son posibles numerosas mediciones de los defectos, por ejemplo se puede medir el color o el nivel de gris medio de cada celda del Data Matrix, se puede determinar el contorno de una celda, medir la distancia entre el centro de gravedad y el contorno exterior para diferentes ángulos, etcétera. Los puntos de impacto se pueden superponer, en cuyo caso se puede fijar un valor límite de distancia al contorno exterior.

Se puede modelizar, para el canal de impresión en cuestión, el resultado “medio” del marcado de un cierto código de barras 2D, sobre la base del tamaño medio de los puntos de impacto, y, eventualmente, teniendo en cuenta posibles interacciones cuando los puntos de impacto son adyacentes. Se puede restar la imagen estimada por la modelización de la imagen captada, y el resultado consta de menos redundancia, lo cual hace que aumente la relación de la señal con respecto al ruido y, al mismo tiempo, el rendimiento de detección.

A continuación en la presente se ofrece, con respecto a la figura 6, un ejemplo de algoritmo que permite el registro de los defectos de marcado de un código de barras:

En el transcurso de una etapa 305, se recibe una imagen captada que contiene un código de barras.

En el transcurso de una etapa 310, se descodifica el mensaje del código de barras portado por las formas y colores medios de las celdas cuadradas.

En el transcurso de una etapa 315, se calcula un identificador a partir del mensaje.

En el transcurso de una etapa 320, se miden las características de los defectos de marcado del código de barras.

En el transcurso de una etapa opcional 325, se resta la media de las características para un conjunto de Data Matrix, de las características medidas para el Data Matrix considerado.

En el transcurso de una etapa 330, se cuantifican las características, eventualmente se comprimen, y se determina un vector de datos característicos representativo de los defectos.

En el transcurso de una etapa 335, este vector de características se almacena en una base de datos, asociado al identificador del mensaje.

A continuación en la presente se ofrece, con respecto a la figura 7, un algoritmo que permite la autentificación de un código de barras 2D a partir de la medición de los defectos de impresión del marcado:

en el transcurso de una etapa 405, se recibe una imagen captada que contiene un código de barras.

En el transcurso de una etapa 410, se descodifica el mensaje contenido en el código de barras y portado por las formas y colores medios de las celdas cuadradas. Si no se consigue descodificarlo, se le presenta visualmente al usuario “Código de barras ilegible”.

En caso contrario, en el transcurso de una etapa 415, se calcula un identificador a partir del mensaje.

En el transcurso de una etapa 420, se obtiene, de una base de datos, el vector de datos correspondiente a este identificador, así como un umbral de decisión asociado a este vector de características. Si la base de datos no contiene este identificador, se le presenta visualmente al usuario “Código de barras no autentificado”.

En caso contrario, en el transcurso de una etapa 425, se miden las características de los defectos de marcado del código de barras.

En el transcurso de una etapa opcional 430, se resta la media de las características para varios códigos de barras, de las características medidas para el código de barras considerado.

En el transcurso de una etapa 435, se cuantifican las características, eventualmente se comprimen, y se determina un vector de datos representativo de los defectos.

En el transcurso de una etapa 440, se compara el vector de datos extraído con el vector de datos obtenido de la base de datos, y se mide un índice de similitud, denominado “puntuación”.

En el transcurso de una etapa 445, se compara la puntuación medida con el umbral de decisión. Si la misma es superior, se le presenta visualmente al usuario “Data Matrix autentificado”. En caso contrario, se le presenta visualmente al usuario “Data Matrix no autentificado”. Opcionalmente, al usuario se le presenta visualmente cada mensaje leído.

En la figura 8, se observa un terminal local 505 dotado de una impresora 510, de un medio de captura de imágenes 535, de dos sensores 540 y 545 y de un medio de acceso 515 a una red 520 a la cual está conectado un servidor 525. El servidor 525 está dotado de una base de datos 530.

El terminal local 505 es, por ejemplo, de tipo ordenador de uso general. El mismo está instalado en una cadena 550 de fabricación o de transformación de objetos, por ejemplo de embalajes. La cadena 550 consta, por ejemplo, de un desapilador de objetos planos (no representado) y de un transportador (no representado) que pone en movimiento los objetos a procesar, uno detrás de otro.

El sensor 540 está posicionado en la cadena de fabricación 550, aguas arriba del campo óptico del sensor de imágenes 535 y está adaptado para detectar la llegada de un objeto a procesar. Por ejemplo, el sensor 540 es una célula óptica que consta de un emisor y de un receptor de rayos luminosos. El sensor 545 se coloca en la cadena 550 y determina la velocidad de los objetos sobre esta cadena. Por ejemplo, el sensor 545 está conectado a un autómata (no representado) que rige el funcionamiento de la cadena 550 ó está conectado a un soporte de desplazamiento de los objetos, por ejemplo una cinta de transportador. El terminal local 505 ordena la impresión de los objetos por medio de la impresora 510, de una manera conocida en sí misma, por ejemplo por chorros de tintas o por marcado de láser. El medio de acceso 515 a la red 520 es, por ejemplo, un módem de un tipo conocido, para acceso a la red 520, por ejemplo la red Internet.

El medio de captura de imágenes 535 es, por ejemplo, una cámara fotográfica digital, un sensor lineal o una cámara industrial.

El servidor 525 es de tipo conocido. La base de datos 530 mantiene, por lo menos, una lista de identificadores de objetos y de vectores de datos de defectos vinculados a estos objetos, determinados de acuerdo con el procedimiento objeto de la presente invención. Preferentemente, esta base de datos 530 mantiene, en relación con cada identificador de un objeto, un identificador de tipo de objeto y de posición de zona de posicionamiento del código geométrico objeto de la presente invención para este tipo de objeto, y un identificador del proveedor que lleva a cabo la fabricación o la transformación.

El terminal 505 mantiene un *software* que, durante su ejecución, implementa etapas de un procedimiento objeto de la presente invención. El servidor 525 mantiene un software que, durante su ejecución, implementa etapas de un procedimiento de almacenamiento y de recuperación de vectores de datos de defectos.

En una variante, el terminal 505 no mantiene ningún *software* específico sino que implementa un navegador web y un servicio web (en inglés “web service”) alojado por el servidor 525.

REIVINDICACIONES

1. Procedimiento de autenticación de un código con zonas geométricas de formas y/o colores variables en función de un mensaje, que consta de:

- una etapa de generación de dicho código con zonas geométricas variables, en función de un mensaje para suministrar zonas geométricas,

- una etapa de generación de un código digital autentificador para suministrar valores numéricos; caracterizado por

- una etapa de formación de una imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas y/o en por lo menos un espacio entre zonas geométricas, de una parte de dicho código digital autentificador;

afectando la etapa de formación de una imagen, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador en una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado.

2. Procedimiento según la reivindicación 1, en el cual la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, entre dos formaciones del mismo código con zonas geométricas variables, a la representación del código digital autentificador en una variación superior a un tercer valor predeterminado e inferior a un cuarto valor predeterminado.

3. Procedimiento según una de las reivindicaciones 1 ó 2, en el cual la etapa de formación de una imagen afecta, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador con un ruido tal que la relación de la señal con respecto al ruido de la representación del código digital autentificador es inferior a un quinto valor predeterminado.

4. Procedimiento según una de las reivindicaciones 1 a 3, que consta, además, de:

- una etapa de determinación de condiciones de formación de dicha imagen y

- una etapa de determinación de características físicas de celdas de por lo menos una parte del código digital autentificador, en función de las condiciones de formación de la imagen.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el cual, en el transcurso de la etapa de generación de dicho código con zonas geométricas variables, las zonas geométricas variables son barras en general rectangulares paralelas cuya anchura y/o separación varía en función de dicho mensaje.

6. Procedimiento según una de las reivindicaciones 1 a 4, en el cual, en el transcurso de la etapa de generación de dicho código con zonas geométricas variables, las zonas geométricas variables son zonas cuadradas introducidas en una matriz cuyo color y/o por lo menos una de cuyas dimensiones varía en función de dicho mensaje.

7. Procedimiento según una de las reivindicaciones 1 a 6, en el cual, en el transcurso de la etapa de formación de la imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas, de una parte de dicho código digital autentificador, el código digital autentificador adopta la forma de una variación de por lo menos una dimensión de zonas geométricas variables.

8. Procedimiento según una de las reivindicaciones 1 a 7, en el cual, en el transcurso de la etapa de formación de la imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas, de una parte de dicho código digital autentificador, cada parte del código digital autentificador introducida en una zona geométrica del código con zonas geométricas variables, adopta la forma de una distribución de celdas rectangulares de por lo menos un orden de magnitud más pequeño que las dimensiones de dicha zona geométrica, presentando una parte de dichas celdas un color diferente del correspondiente de dicha zona geométrica.

9. Procedimiento según una de las reivindicaciones 1 a 8, en el cual, en cada zona geométrica que consta de una parte del código digital autentificador, la superficie de dichas celdas es inferior a un cuarto de la superficie de dicha zona geométrica.

10. Procedimiento según una de las reivindicaciones 1 a 9, que consta, además, de una etapa de determinación de una huella de la imagen generada, siendo dicha huella función de una degradación del código digital autentificador en el transcurso de la etapa de formación de una imagen.

11. Procedimiento según una de las reivindicaciones 1 a 10, que consta, además, de una etapa de codificación de una información en dicho código digital autentificador, siendo dicha información representativa de una medición de degradación del código digital autentificador debido a contingencias físicas que afectan a la imagen durante la etapa de formación de una imagen.

12. Dispositivo de autentificación de un código con zonas geométricas de formas y/o colores variables en función de un mensaje, que consta de:

- un medio de generación de dicho código con zonas geométricas variables, en función de un mensaje adaptado para suministrar zonas geométricas,

- un medio de generación de un código digital autentificador adaptado para suministrar valores numéricos; caracterizado por

- un medio de formación de una imagen de dicho código con zonas geométricas que consta, en por lo menos una parte de sus zonas geométricas y/o en por lo menos un espacio entre zonas geométricas, de una parte de dicho código digital autentificador;

afectando el medio de formación de una imagen, debido a las contingencias físicas de la formación de imágenes, a la representación del código digital autentificador en una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado.

13. Procedimiento de autentificación de un código con zonas geométricas de formas y/o colores variables, representado por una imagen captada representativa de una imagen formada según el procedimiento de autentificación según una de las reivindicaciones 1 a 11, caracterizado por que el mismo consta de:

- una etapa de lectura de un mensaje portado por las formas y colores medios de las zonas geométricas,

- una etapa de medición de un nivel de degradación de un código digital autentificador representado en por lo menos una parte de las zonas geométricas de dicho código con zonas geométricas y

- una etapa de determinación de la autenticidad de dicho código con zonas geométricas en función de por lo menos dicho nivel de degradación.

14. Dispositivo de autentificación de un código con zonas geométricas de formas y/o colores representado por una imagen captada representativa de una imagen formada según el procedimiento de autentificación según una de las reivindicaciones 1 a 11, caracterizado por que el mismo consta de:

- un medio de lectura de un mensaje portado por las formas y colores medios de las zonas geométricas,

- un medio de medición de un nivel de degradación de un código digital autentificador representado en por lo menos una parte de las zonas geométricas de dicho código con zonas geométricas y

- un medio de determinación de la autenticidad de dicho código con zonas geométricas adaptado para determinar la autenticidad de dicho código con zonas geométricas variables en función de por lo menos dicho nivel de degradación.

15. Código con zonas geométricas de formas y/o colores variables en función de un mensaje, que representa:

- un mensaje por medio de las zonas geométricas; caracterizado por que representa:

- un código digital autentificador, en por lo menos una parte de sus zonas geométricas, mediante una característica de marcado variable en función de dicho código digital autentificador, presentando el código digital autentificador una tasa de errores superior a un primer valor predeterminado e inferior a un segundo valor predeterminado después de la formación.

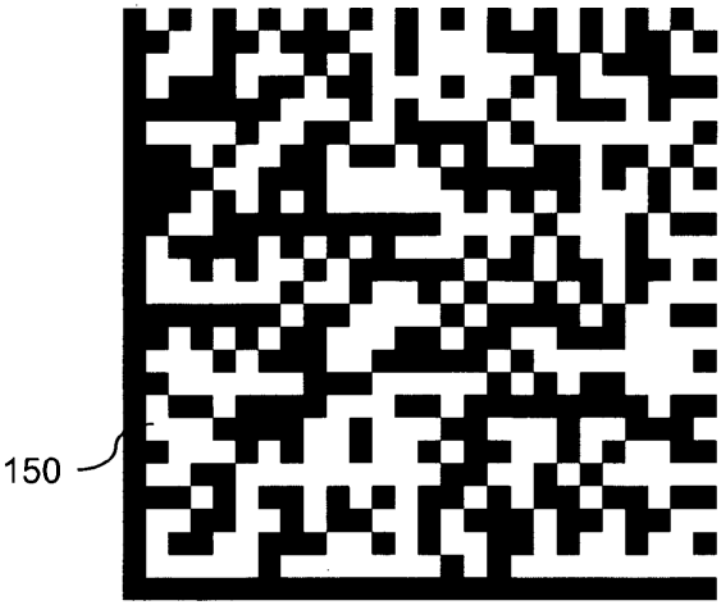

Figura 1A

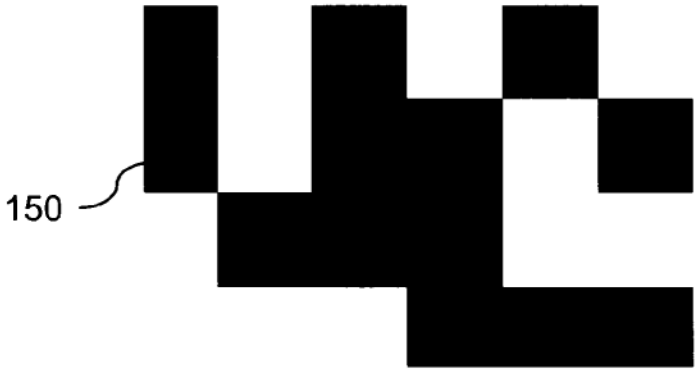

Figura 1B

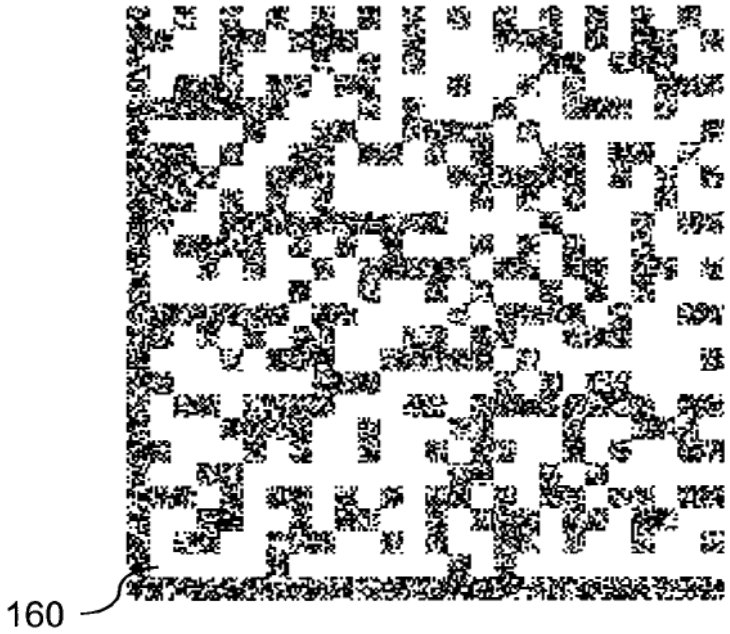

Figura 2A

Figura 2B

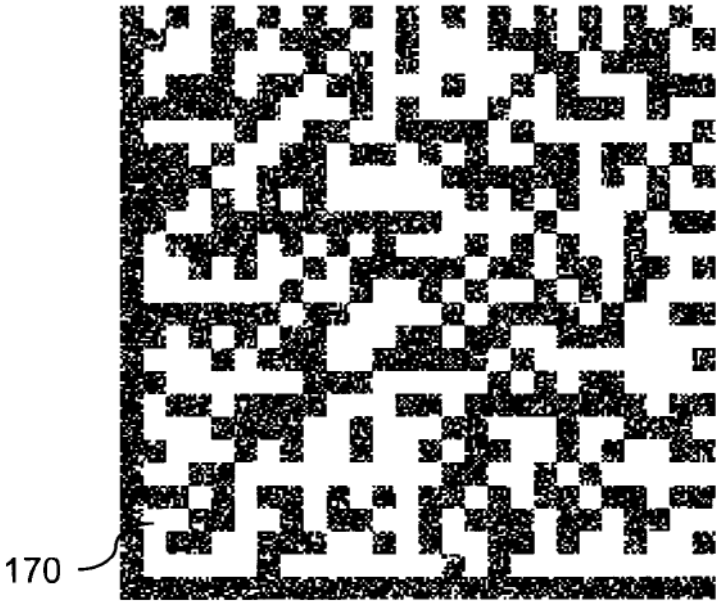

Figura 3A

Figura 3B

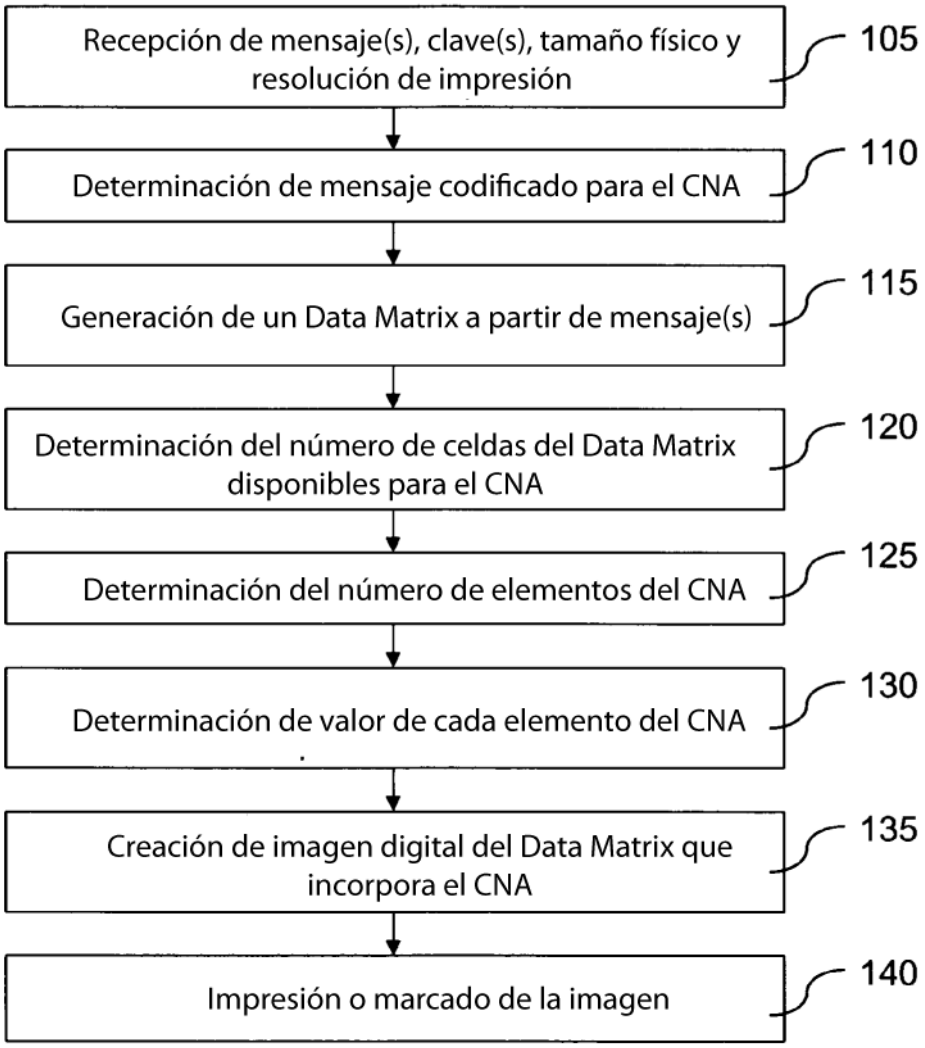
Recepción de mensaje(s), clave(s), tamaño físico y resolución de impresión
105
Determinación de mensaje codificado para el CNA
110
Generación de un Data Matrix a partir de mensaje(s)
115
Determinación del número de celdas del Data Matrix disponibles para el CNA
120
Determinación del número de elementos del CNA
125
Determinación de valor de cada elemento del CNA
130
Creación de imagen digital del Data Matrix que incorpora el CNA
135
Impresión o marcado de la imagen
140

Figura 4

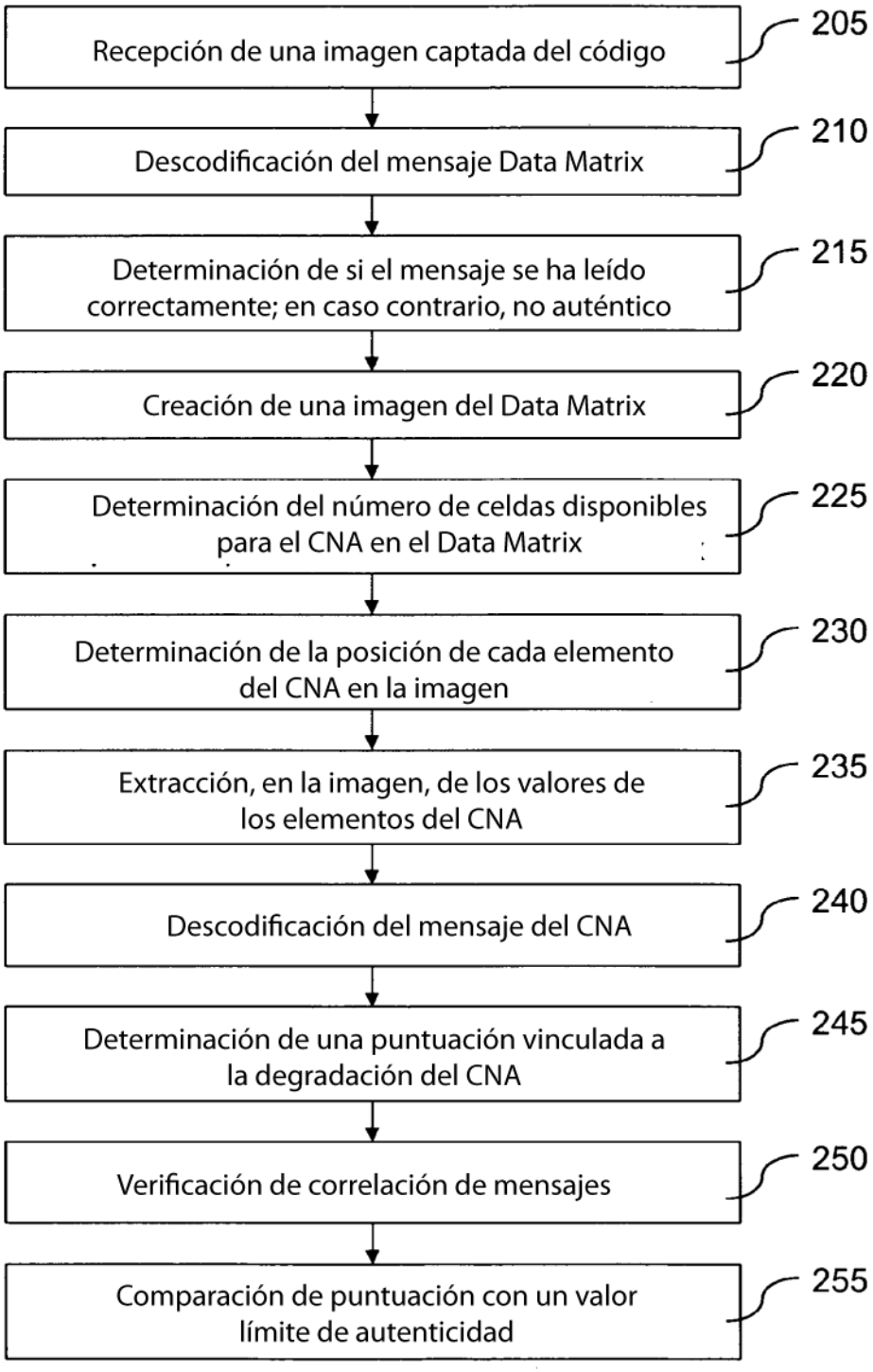
Recepción de una imagen captada del código
205
Descodificación del mensaje Data Matrix
210
Determinación de si el mensaje se ha leído correctamente; en caso contrario, no auténtico
215
Creación de una imagen del Data Matrix
220
Determinación del número de celdas disponibles para el CNA en el Data Matrix
225
Determinación de la posición de cada elemento del CNA en la imagen
230
Extracción, en la imagen, de los valores de los elementos del CNA
235
Descodificación del mensaje del CNA
240
Determinación de una puntuación vinculada a la degradación del CNA
245
Verificación de correlación de mensajes
250
Comparación de puntuación con un valor límite de autenticidad
255

Figura 5

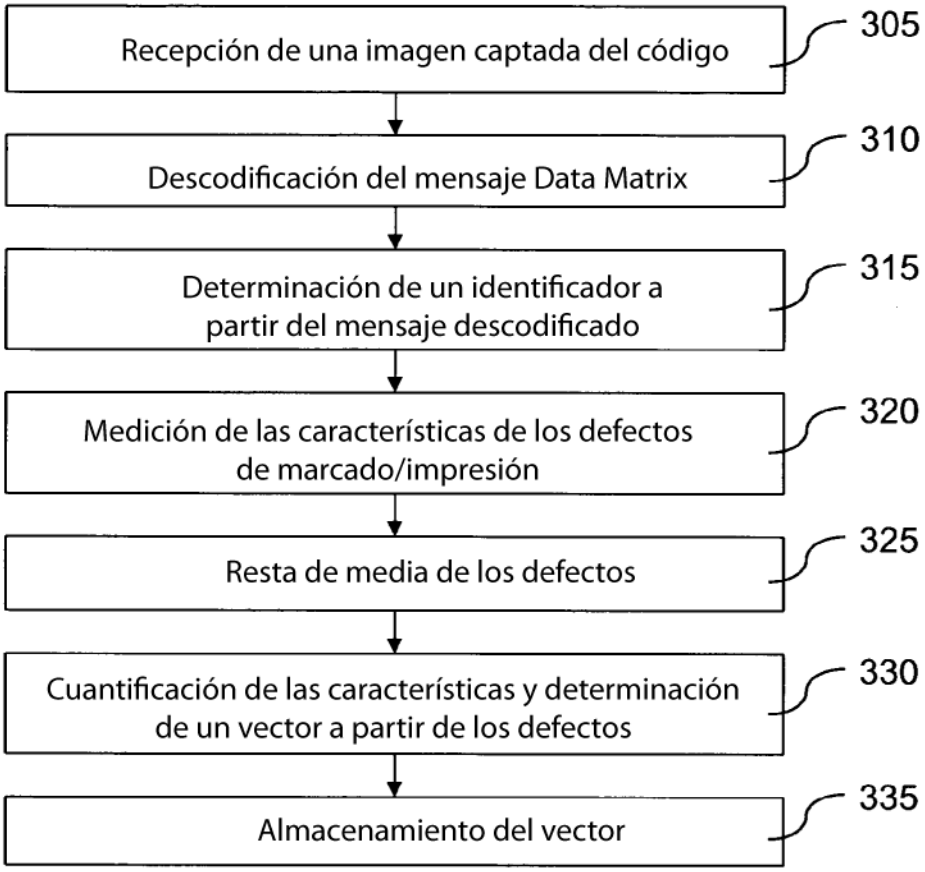
Recepción de una imagen captada del código
305
Descodificación del mensaje Data Matrix
310
Determinación de un identificador a partir del mensaje descodificado
315
Medición de las características de los defectos de marcado/impresión
320
Resta de media de los defectos
325
Cuantificación de las características y determinación de un vector a partir de los defectos
330
Almacenamiento del vector
335

Figura 6

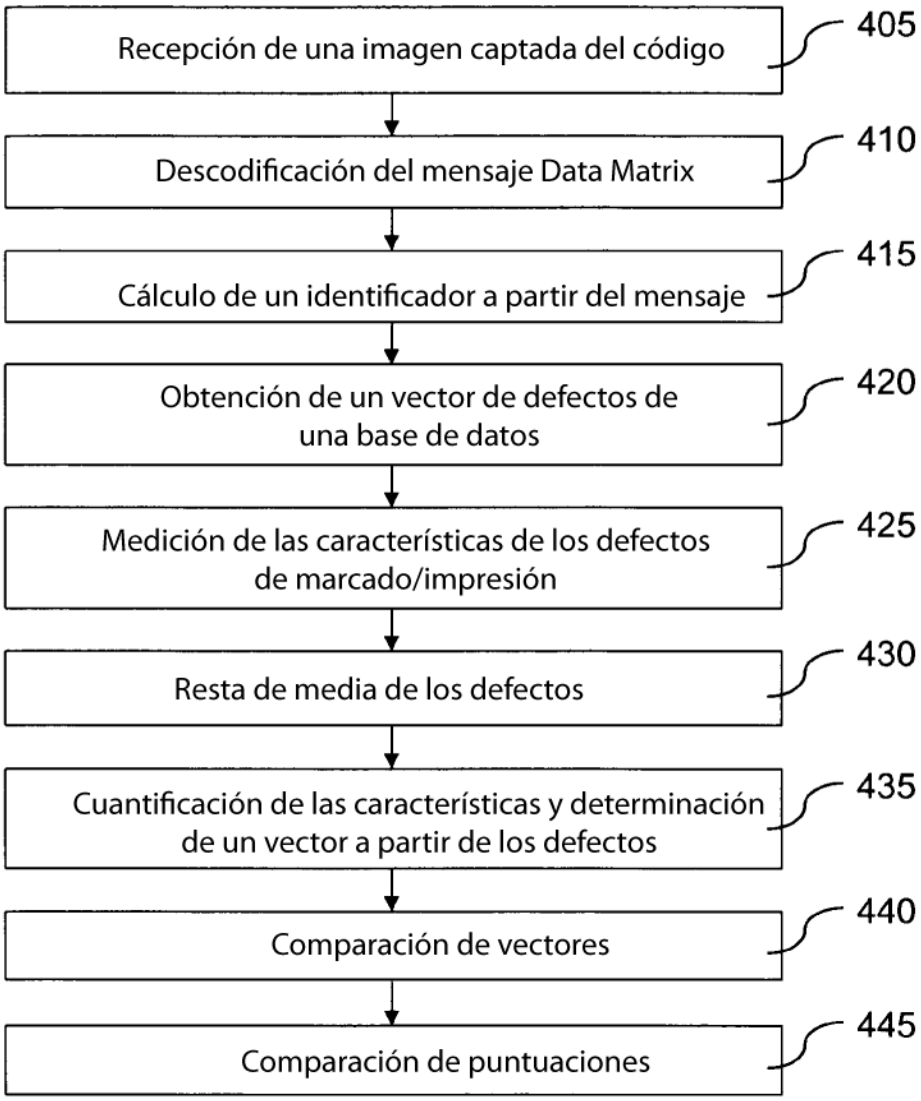
Recepción de una imagen captada del código
405
Descodificación del mensaje Data Matrix
410
Cálculo de un identificador a partir del mensaje
415
Obtención de un vector de defectos de una base de datos
420
Medición de las características de los defectos de marcado/impresión
425
Resta de media de los defectos
430
Cuantificación de las características y determinación de un vector a partir de los defectos
435
Comparación de vectores
440
Comparación de puntuaciones
445

Figura 7

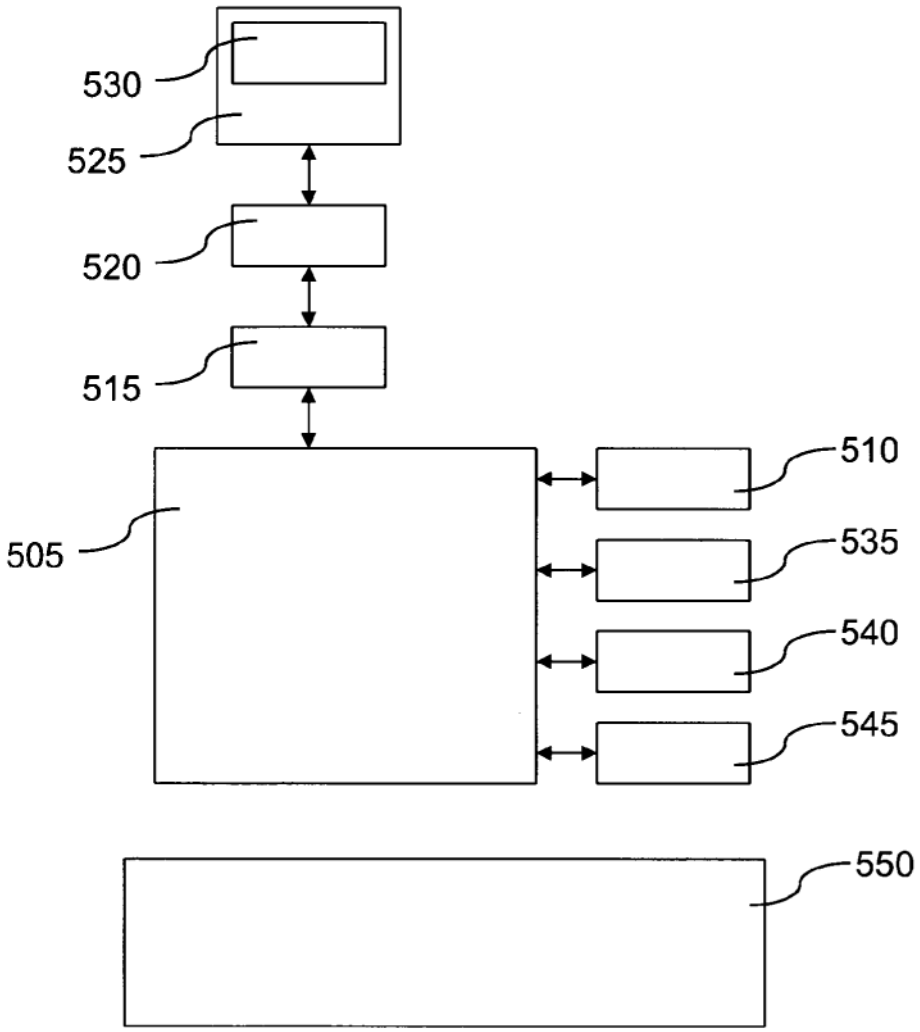

Figura 8

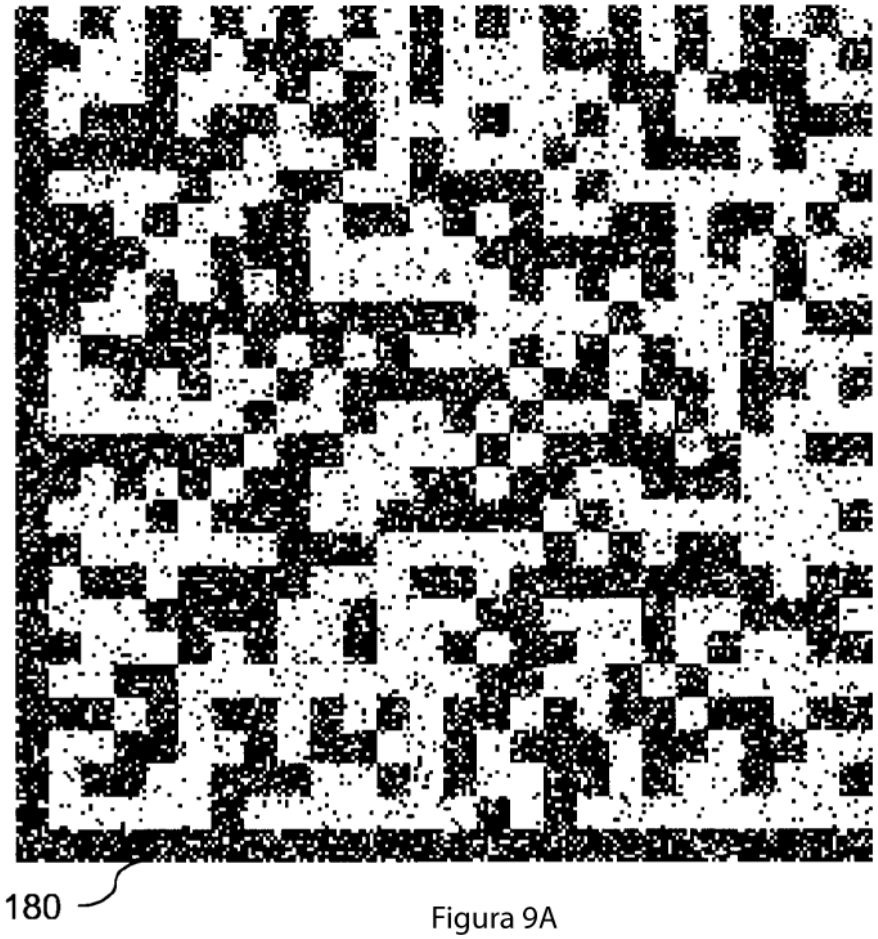

Figura 9A

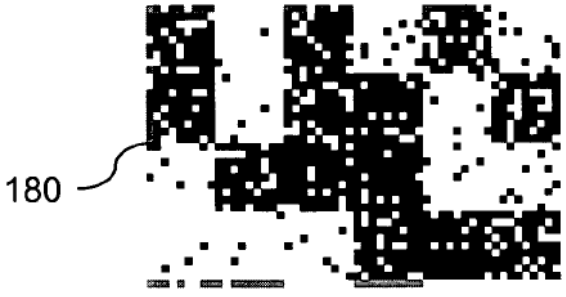

Figura 9B

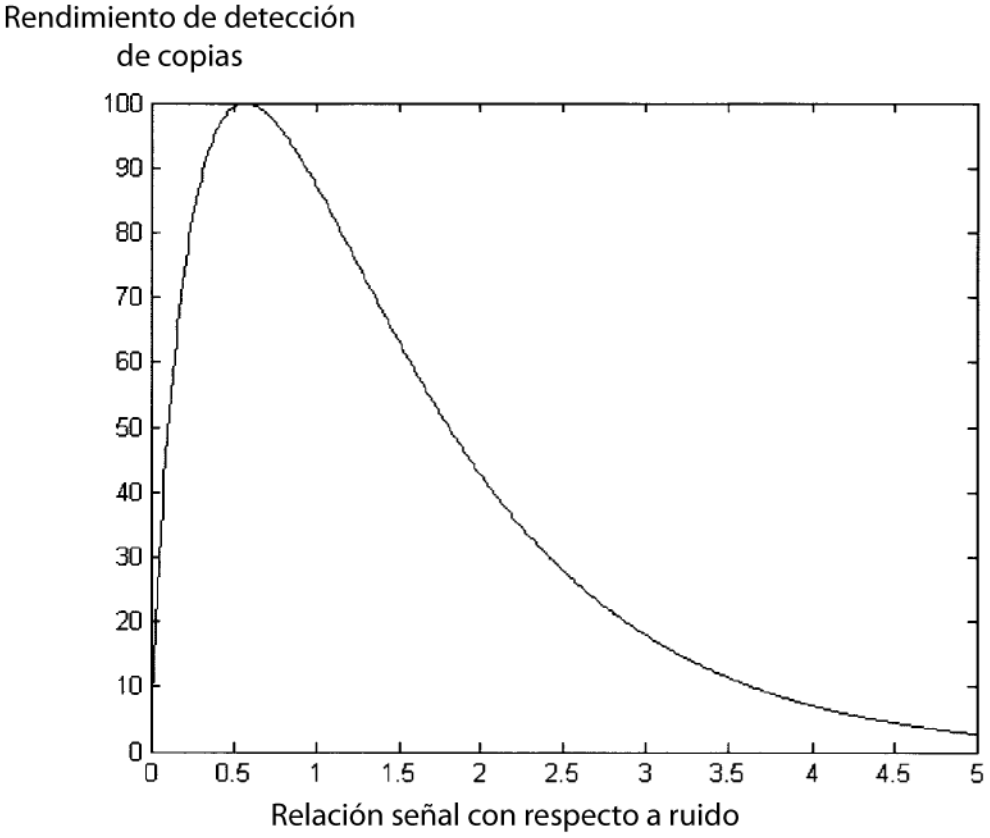
Rendimiento de detección
de copias
100
90
80
70
60
50
40
30
20
10
0
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
Relación señal con respecto a ruido

Figura 10