(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 718 528**

(51) Int. CI.:

G06K 7/14 (2006.01)
G06K 19/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.11.2014 PCT/EP2014/073985**

(87) Fecha y número de publicación internacional: **14.05.2015 WO15067725**

(96) Fecha de presentación y número de la solicitud europea: **06.11.2014 E 14796052 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.01.2019 EP 3066612**

(54) Título: **Código de barras bidimensional y procedimiento de autenticación de dicho código de barras**

(30) Prioridad:

07.11.2013 CH 18662013

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.07.2019

(73) Titular/es:

SCANTRUST SA (100.0%)
EPFL PSE-C
1015 Lausanne, CH

(72) Inventor/es:

PICARD, JUSTIN y
LANDRY, PAUL

(74) Agente/Representante:

LÓPEZ CAMBA, María Emilia

DESCRIPCIÓN

Código de barras bidimensional y procedimiento de autenticación de dicho código de barras

Campo de la invención

La presente invención se refiere a un procedimiento para crear un código de barras 2D, un producto que integra un código de barras 2D, un procedimiento de fabricación de dicho producto y un procedimiento de autenticación de dicho código de barras 2D.

Antecedentes

Los códigos de barras 2D son soportes de datos usados para asignar una identidad única o por lotes a un producto, un documento o cualquier otro artículo. Dichos códigos de barras 2D están formados preferentemente por una retícula bidimensional que define una matriz 2D cuyas celdas están codificadas con información, especialmente información binaria tal como bits de codificación 0 o 1 que en serie puede codificar diferentes tipos de caracteres.

Según la invención están incluidos todos los códigos de barras bidimensionales (códigos de barras 2D), y especialmente los siguientes que son muy comunes: los códigos de barras PDF-417, MaxiCode, Datamatrix, Código QR, Aztec Code y EAN. Estos códigos de barras pueden ser leídos hasta un cierto grado de deterioro, usando por ejemplo corrección de errores de Reed-Solomon para permitir una lectura correcta incluso si alguna parte del código de barras está dañada. Cuando el escáner de código de barras no puede reconocer un símbolo de un código de barras, será tratado como una tachadura. En la actualidad, el código QR (Quick Response, respuesta rápida) y Datamatrix son los códigos de barras 2D usados en cada vez más aplicaciones en diversos sectores como fabricación, almacenes y logística, venta minorista, salud, ciencias biológicas, transporte y ofimática. Estos son además los códigos de barras 2D más usados por los consumidores para acceder a información digital relacionada con un medio físico.

Al ser el código QR el usado con mayor frecuencia para el escaneo con teléfonos inteligentes, con el crecimiento explosivo de los teléfonos inteligentes, los códigos QR se están usando ampliamente además en campañas de marketing y publicidad en móviles como una forma rápida y efectiva de conectarse con los clientes y proporcionar contenido de usuarios finales, incluidos enlaces web, cupones por móvil, tarjetas de embarque aéreas y otras aplicaciones como seguimiento de productos, identificación de artículos, registro del tiempo, gestión de documentos, marketing general, etc.

Además, la invención se refiere a códigos QR que incluyen modificaciones agradables estéticamente, en los que se combina una imagen en el código principalmente para mejorar el impacto visual del código QR.

En comparación con los códigos 1-D, los códigos 2-D pueden contener una cantidad de datos mayor en un espacio más reducido, y en comparación con otros códigos 2-D, el código QR y Datamatrix pueden contener potencialmente más datos todavía. Además, los procedimientos de corrección de errores avanzados y otras características únicas para detectar la presencia del código y su posición permiten leer el código QR de manera más fiable y a mayor velocidad que la mayoría de otros códigos.

Al igual que el lenguaje escrito, los códigos de barras son representaciones visuales de información. Sin embargo, a diferencia del lenguaje, que los seres humanos pueden leer, los códigos de barras están diseñados para ser leídos y entendidos (decodificados) por ordenadores, usando sistemas de visión con máquina consistentes en cámaras o escáneres láser ópticos, más en general por lectores de códigos de barras, y software de interpretación de códigos de barras. El alto grado de legibilidad del código QR y Datamatrix en condiciones de bajo contraste puede permitir la impresión, el grabado por láser o el marcado por puntos (DPM, *dot-pin marking*) de un símbolo directamente en una parte o producto.

El código QR es un código de matriz 2-D que transporta información por medio de la disposición de sus celdas elementales oscuras y claras, también llamadas "módulos", en columnas y filas, es decir, en las direcciones horizontal y vertical. Cada módulo oscuro o claro de un símbolo de código QR, un caso específico de código, representa un 0 o un 1, haciéndolo inteligible para una máquina.

El código QR es detectado por un sensor de imagen digital bidimensional y a continuación es analizado digitalmente por un procesador programado. El procesador localiza los tres cuadrados distintivos en las esquinas de la imagen de código QR, usando un cuadrado menor (o múltiples cuadrados) cerca de la cuarta esquina para normalizar la imagen en tamaño, orientación y ángulo de visualización. Los pequeños puntos distribuidos por el código QR son convertidos seguidamente en números binarios y validados con un código de corrección de errores.

La información contenida en el código QR puede usarse para el trazado de un producto en un canal de distribución, o para detectar fraudes relacionados con un producto, tales como desvío, robo, alteración o falsificación. Sin embargo, aun cuando los códigos de barras 2D se usan cada vez más para aplicaciones contra falsificaciones, no

poseen protección incorporada contra la copia. Por tanto pueden ser duplicados muy fácilmente y aplicados en artículos no legítimos, es decir, en falsificaciones.

Descripción de la técnica relacionada

Para potenciar la seguridad, los códigos de barras usados en la lucha contra falsificaciones se complementan con diversos elementos de seguridad física, en general extrínsecos al código de barras 2D, como hologramas, tintas o marcadores especiales que pueden revelarse por medio de un dispositivo de detección específico (tinta con propiedades espectrales específicas que se revelan cuando se iluminan con un cierto espectro), microimpresiones, etc. Sin embargo, se sabe que todos estos procedimientos son caros o incómodos de integrar en los procesos de producción. Además, son incómodos de verificar, y fáciles de copiar o imitar.

Se han propuesto otros procedimientos numerosos con elementos de seguridad colocados intrínsecamente en el código de barras 2D en sí y que forman la llamada información secundaria con respecto a la información primaria usada para codificar una identidad o mensaje. Esta información primaria y esta información secundaria están formadas preferentemente por imágenes elementales negras y blancas o celdas elementales formadas, por ejemplo, por puntos o cuadrados, tal como píxeles.

Como ilustración no limitativa de estas técnicas es posible hacer referencia a la lista siguiente:

- se ha propuesto insertar marcas de agua digitales, es decir, modificaciones imperceptibles de la imagen que codifican información, en los códigos de barras como en los documentos EP-1.239.413, EP-1.485.863 o US-6.398.117,
- el documento WO-2013/012.794 se refiere a sistemas y procedimientos para proporcionar certificación y autenticación de documentos usando códigos de barras 2D, en los que dicho código de barras tiene una parte legible abiertamente con una información primaria que forma una marca robusta y una parte de código de barras legible de manera oculta con una información secundaria que forma una marca frágil incorporada en espacio redundante con la parte del código de barras legible abiertamente. La marca frágil está integrada sobre toda la superficie de la marca robusta,
- se describe otra técnica también en el documento WO-2008/003.964 en el que la información secundaria está integrada en un código de barras, por ejemplo modificando la periferia de algunas de las barras o píxeles en distintas magnitudes,
- el documento WO-2010/034.897 presenta también información secundaria integrada en un código de barras. De forma notable, un código de autenticación digital (DAC, Digital Authentication Code) que se degrada de manera que la degradación tiene una cierta tasa de errores contenida en límites predeterminados. Por tanto, el código DAC puede usarse para proteger documentos de copias ilegales.

Por ejemplo, todos los valores de píxeles en las celdas negras del código de barras 2D pueden modificarse con el código de autenticación digital. Sin embargo, esto puede afectar a su legibilidad. Además, el DAC en sí puede ser difícil de leer ya que cubre una superficie extensa y la sincronización precisa que es necesaria para la lectura puede verse afectada por aberraciones geométricas en la captura de la imagen.

Además, los códigos de barras 2D pueden asociarse con procedimientos relacionados con huellas digitales en los que los elementos singulares de cada impresión, o grupos de impresiones similares, se extraen y se almacenan en una base de datos. Véanse por ejemplo los documentos US-4.423.415, US-4.785.290, US-6.948.657 o US-8.180.174.

El documento US-2013/0.015.236-A1 describe un sistema de autenticación que usa códigos de barras. Los códigos de barras comprenden información abierta e información oculta codificadas en zonas redundantes de los códigos. El código oculto se codifica de forma secreta en la parte superior de un código de barras estándar.

El documento US-2012/0.256.000-A1 describe un código óptico de multirresolución, en el que los píxeles en un código de barras de baja resolución se sustituyen por códigos de barras de alta resolución.

En muchos de estos documentos, la información secundaria se distribuye por toda la superficie de la información primaria, por ejemplo en forma de una marca de agua. Estas técnicas tienen inconvenientes, principalmente los que se enumeran a continuación:

En muchos casos la información está oculta para hacerla invisible para el falsificador que no le prestará una atención especial. La información secundaria oculta puede ser menos segura que la información secundaria visible, ya que está limitada a una relación señal-ruido baja para asegurar su imperceptibilidad. En consecuencia, la entropía es menor y a un falsificador informado le resulta más fácil reproducir toda la información secundaria cuando hace la copia.

Por otra parte, la integración de información secundaria oculta en la información primaria puede tener un impacto en la legibilidad de la primera información que se distorsiona por la presencia de la información secundaria.

Además, la presencia de información secundaria tal como DAC en un código de barras 2D requiere algoritmos complejos para integrar y decodificar el mensaje contenido en la información secundaria, lo que convierte en incómoda y menos fiable la gestión del sistema de autenticación, mientras que el código de barras 2D que contiene solo información primaria está diseñado de manera que sea extremadamente rápido y sencillo de decodificar.

El verdadero inconveniente en los códigos de barras 2D convencionales es que la información secundaria es más complicada de leer que la información primaria. En la actualidad, la información primaria puede leerse fácilmente con un teléfono móvil equipado con una cámara. Las técnicas de la técnica anterior no permiten autenticar automáticamente el código de barras 2D con la información secundaria sin usar un procedimiento o dispositivo específico.

Cuando puede leerse a través de medios ópticos, la información secundaria se ha leído tradicionalmente con escáneres de mesa, cámaras industriales que usan un cierto nivel de aumento o un microscopio USB (por ejemplo, modelos de Veho™ o Dino-lite™). Más recientemente, se han usado teléfonos móviles pero necesitan un adaptador óptico con el fin de obtener el aumento y la nitidez de la imagen requeridos para leer los detalles del DAC que permitan diferenciar los originales de las copias. Por ejemplo pueden usarse los microscopios móviles Handyscope™, o Dermlite DL1™, compatibles con ciertos teléfonos inteligentes (por ejemplo, algunos modelos de iPhone™ y Samsung™).

Esto representa una mejora importante con respecto al uso de un escáner de mesa o un microscopio o USB, ya que permite a los inspectores u operadores de cadenas de suministros sobre el terreno realizar la autenticación. Sin embargo, la necesidad de un adaptador óptico sigue siendo un obstáculo importante para un uso más extenso de estas técnicas. De hecho, el adaptador óptico suele ser bastante caro y, sin embargo, es fácil de extraviar o de perder, y es así necesario que el inspector siempre lo lleve. Hace que el despliegue de las soluciones del lector sea mucho más complejo, ya que es preciso distribuir y mantener cientos si no miles de adaptadores ópticos. Obviamente, el uso de adaptadores ópticos no es viable para su uso en mercados de mayor escala por parte de los consumidores o los minoristas.

La nueva generación de teléfonos móviles tiene impresionantes capacidades ópticas. Un número creciente de teléfonos móviles tiene la capacidad óptica de capturar pequeños detalles, en particular los pequeños detalles en el DAC que permiten diferenciar los originales de las copias.

Estos nuevos teléfonos móviles tienen en principio el potencial de ser usados para autenticar códigos de barras 2D usando información secundaria en un DAC. Sin embargo, las técnicas de la técnica anterior para usar DAC como información secundaria presentan diversos inconvenientes que dificultan el uso de un teléfono móvil sin un adaptador óptico de forma conveniente:

• La información secundaria debe ser decodificada independientemente de la información primaria, usando un procedimiento separado. Los algoritmos para decodificar la información secundaria son mucho más intensivos computacionalmente, y no pueden implementarse en tiempo real en el dispositivo del teléfono móvil. En varios casos se requiere un lector diferente.

• La imagen completa del escaneo debe ser enviada a un servidor para su autenticación. Esto requiere anchura de banda, es costoso y prolonga el tiempo para obtener un resultado de autenticación.

• La información secundaria adquirida en un escaneo no puede ser validada como utilizable para la autenticación en tiempo real por medio del procesamiento de cada trama. Por ejemplo, el escaneo puede no estar enfocado, puede contener artefactos que impiden la lectura, o la colocación puede ser incorrecta, con lo que no debe ser enviada al servidor ni usada para autenticación. Por tanto existe un riesgo elevado de que el usuario espere un resultado de autenticación, solo para recibir la retroalimentación que necesita para realizar otro escaneo. Peor todavía, la respuesta de autenticación podría ser errónea, por ejemplo, un escaneo no enfocado podría interpretarse como una copia. Esto es muy poco conveniente para los usuarios, que pueden perder la confianza en el sistema de autenticación.

• Los usuarios no obtienen retroalimentación en tiempo real que los oriente sobre cómo realizar el escaneo, indicándoles por ejemplo si la imagen está enfocada o no, o si es preciso acercarse o alejarse del código de barras 2D

• El usuario debe pulsar un botón para obtener una imagen en modo cámara, en lugar de que se realice un escaneo automatizado en modo vídeo. Al pulsar un botón es posible que la imagen se desenfoque.

En cualquier caso, esperar a que el usuario decida cuándo está cámara colocada correctamente y cuándo será aceptable la imagen para autenticación es una carga elevada.

En suma, las técnicas de la técnica anterior no permiten a los usuarios autenticar códigos de barras 2D de forma

cómoda usando su dispositivo móvil.

El objetivo de la presente invención es abordar algunos o todos los inconvenientes de la técnica anterior, y proponer un medio para producir códigos de barras 2D que sean seguros frente a copiado, a la vez que se mantiene una buena legibilidad de la información primaria:

La presente invención pretende además proporcionar un medio para autenticar estos códigos de barras de manera que el procedimiento de autenticación sea tan sencillo como leer un código de barras 2D con un dispositivo móvil.

Resumen de la invención

Según la invención, se consiguen varios objetivos por medio de un procedimiento para crear un código de barras 2D según la reivindicación 1, por medio de un producto que integra un código de barras 2D según la reivindicación 7, por medio de un procedimiento de autenticación de un código de barras 2D según las reivindicaciones 12 ó 16.

En la presente memoria se describe un procedimiento para crear un código de barras 2D que comprende:

- la integración de información primaria que puede ser leída por un lector de código de barras 2D en un patrón de información primaria,
- la integración de información secundaria que es difícil de reproducir sin alteración en un patrón visible,

en el que dicho patrón está integrado en dicho código de barras en al menos un área que no contiene ninguna información primaria, que forma así un código de barras 2D fuente. Salvo que en el presente texto se indique lo contrario, el código de barras 2D y todos los elementos del código de barras 2D tales como el patrón de información primaria y su información primaria, el patrón visible y su información secundaria, el área de datos, las celdas elementales, las subceldas elementales, la signatura, la parte secreta, etc., se refieren a un código de barras 2D fuente y a todos los elementos de dicho código de barras 2D, pero no al código de barras 2D original ni a todos los elementos de dicho código de barras 2D (es decir, por ejemplo, código de barras 2D fuente impreso o visualizado en pantalla) ni a un código de barras 2D no original después de la reproducción del código de barras 2D original (es decir, por ejemplo, código de barras 2D original copiado o escaneado).

En este contexto, "información primaria" se refiere a información sobre un producto o un servicio fácilmente accesible para usuarios dedicados, cuya presencia es fácil de detectar y que se reconoce fácilmente en un código de barras 2D. Además, esta información primaria tiene un contenido que es fácil de verificar, un formato que es acorde con las normas de códigos de barras 2D de manera que pueda ser reconocido fácilmente como un cierto tipo de código de barras 2D, y que puede ser fácil de duplicar.

"Información secundaria" se refiere a información que está dirigida a validar la autenticidad (carácter original) del código de barras 2D y que es más difícil de reproducir que la información primaria sin alteración. Por tanto, la información secundaria no necesita contener necesariamente ningún mensaje sobre el producto o documento en el que se coloca el código de barras 2D, sino concentrarse enteramente en proporcionar medios de detección de falsificaciones. Por tanto, la información secundaria no es información como la información primaria, en el sentido de que, desde la perspectiva del decodificador, no se decodifica un mensaje, sino que se mide una semejanza con un patrón original. Tanto la información primaria como la información secundaria están preferentemente en forma de píxeles o grupos de píxeles. Así, la "información secundaria" puede estar en forma de un patrón de subceldas elementales que forman una denominada "huella digital", con lo que las subceldas elementales son suficientemente pequeñas para impedir la reproducción del patrón sin introducir errores. El copiado (escaneo) de un patrón impreso originalmente de subceldas elementales que representa la información secundaria, seguido por la reproducción visual (por ejemplo, impresión o representación en pantalla) lleva así a una alteración de la "huella digital" que puede ser detectada por los diversos medios descritos en la presente memoria (por ejemplo, por comparación de la huella digital con un archivo de generación de información secundaria o por comparación con una imagen correspondiente a un escaneo o escaneos de la impresión original de la información secundaria). Tal como se expone en la presente memoria, la información secundaria puede ser generada aleatoriamente, en particular por medio del uso de una clave generada de forma aleatoria o pseudoaleatoria que se mantiene secreta, de manera que la información secundaria contiene una parte secreta que impide que sea regenerada por un falsificador. Un falsificador solo tiene acceso al original impreso que no puede ser copiado y reproducido sin alguna alteración detectable.

Según un aspecto de la invención, la información secundaria no se mezcla con la información primaria sino que se mantiene físicamente separada de la información primaria. Por tanto, según la invención dado que la información secundaria está formada por un patrón separado visible, situado en uno o varios lugares identificados en el código de barras 2D, no existe el riesgo de que la lectura de la primera información esté alterada debido a la modificación de la imagen cuando está presente además la información secundaria. Además la información secundaria separada y la concentración en áreas específicas significan que las etapas de lectura y posterior decodificación son más fiables debido a un riesgo menor de distorsiones geométricas o aberraciones del patrón que contiene información secundaria. Al estar la información secundaria presente en el código de barras 2D, sustituye a la parte o partes de información primaria, aunque no impide la legibilidad de la información primaria, en la medida en que la proporción

de superficie de información primaria sustituida por información secundaria se mantiene en los límites de tolerancia suministrados por el código de corrección de errores.

Además, según otro aspecto de la invención, la información secundaria no está oculta, especialmente al no estar integrada en ni mezclada con la información primaria y/o a través de una marca de agua y/o a través de una forma de ruido aplicada de forma intencionada o cualquier otra modificación no perceptible de la imagen que codifica la información primaria. La información secundaria es visible. La información secundaria visible tiene mayor entropía con respecto a la información secundaria oculta, lo que significa más datos disponibles para codificar la información secundaria para una extensión superficial idéntica usada para representar la información secundaria en comparación con la información secundaria oculta.

Esta situación permite usar una alta densidad de información secundaria y por tanto reduce la fiabilidad de reproducibilidad de la información secundaria con equipos como escáneres y máquinas copiadoras. De hecho, cuanto más alta es la densidad de visible información secundaria, más difícil es que la reproduzca el falsificador sin introducir artefactos que permitirán diferenciar los originales de las copias.

La expresión "difícil de reproducir sin alteración" se refiere a la afectación por el copiado, es decir, que la mayoría de las máquinas copiadoras, escáneres, dispositivos de captura de imágenes o impresoras no pueden copiar, capturar o reproducir el código de barras 2D sin alterar el patrón visible, lo que hace que la información secundaria sea sistemáticamente no legible o no legible correctamente después del escaneo o copiado del patrón visible impreso original. Por ejemplo, el patrón visible impreso original del código de barras 2D original contiene detalles finos que no pueden sobrevivir al copiado: la autenticación se basa en el escaneo y el análisis de los detalles del patrón visible que son más numerosos para los códigos de barras 2D originales que para los códigos de barras 2D no originales. Dicho de otro modo, la expresión "difícil de reproducir sin alteración" significa que la información secundaria se deteriora cuando se copia y se reproduce, de manera que ha perdido cualidades que son características u originales en la información secundaria.

La información secundaria puede estar formada por subceldas elementales negras y blancas que tienen un tamaño inferior al 30 %, o preferentemente incluso inferior al 15 %, o preferentemente incluso inferior al 5 % con respecto a las celdas elementales que forman la información primaria.

La información secundaria está formada por subceldas elementales negras y blancas (especialmente píxeles) que tienen una dimensión máxima menor que 50 μm en el código de barras 2D original.

Ventajosamente, en dicho código de barras 2D fuente y en consecuencia en dicho código de barras 2D original, dicha información secundaria comprende una parte formada por subceldas elementales negras y blancas que tienen una densidad de negro (o nivel de gris) promedio diferente del 50 % ± 5 % de subceldas elementales negras. Esta disposición permite elevar al máximo la densidad de información en impresiones originales y aumentar de este modo la tasa de degradación cuando se reproduce, es decir, elevar al máximo la pérdida de información durante la reproducción del código de barras 2D original y cualquier reproducción posterior (reproducción de primera generación que forma un código de barras 2D no original de primera generación por copiado de un código de barras 2D original, de segunda generación que es una reproducción de dicho código de barras 2D no original de primera generación y forma un código de barras 2D no original de segunda generación, y generaciones posteriores). Según dicha disposición, el porcentaje medio de píxeles negros (referido en lo sucesivo como densidad de negro) en dicho patrón visible que codifica información secundaria está predeterminado y es diferente de la densidad de negro (nivel de gris) promedio igual o cercano al 50 % usado comúnmente en los códigos de barras 2D de la técnica anterior y otros gráficos seguros como los DAC. Esta característica es eficaz para elevar al máximo la densidad de información en el código de barras 2D original y aumentar de este modo el nivel de degradación durante la reproducción del código de barras 2D con respecto a un código de barras 2D que tienen un porcentaje medio de píxeles negros igual o cercano al 50 %, es decir, esta disposición puede mejorar significativamente la dificultad para copiar el patrón visible. Por ejemplo, dicha información secundaria está situada enteramente en al menos dos partes diferentes de dicho patrón visible, teniendo al menos una parte tienen una densidad de negro (o nivel de gris) promedio diferente del 50 % ± 5 % de las subceldas elementales negras. Según otra posible disposición, dicha información secundaria está situada totalmente en al menos dos partes diferentes de dicho patrón visible, teniendo cada parte diferentes densidades de negro medias que son diferentes del 50 % de las subceldas elementales negras y diferentes de la al menos otra parte.

En este contexto "densidad de negro media" o "nivel de gris medio" de un grupo de celdas significa una proporción de celdas elementales negras (información primaria), o subceldas elementales (información secundaria), en particular grupo o grupos de píxeles, entre el grupo de celdas elementales, o grupo de subceldas elementales, que define un área limitada que contiene varias celdas elementales, o subceldas elementales (por ejemplo, nueve, dieciséis o veinticinco celdas elementales, o subceldas elementales). Si las celdas no son negras o blancas, el nivel de gris medio puede ponderar los niveles de intensidad de las celdas. En el presente texto, celdas elementales “negras” o subceldas elementales “negras” significa celdas elementales o subceldas elementales que son negras o más en general oscuras o de cualquier color diferente del blanco; "densidad oscura media" y "nivel de gris medio" significan respectivamente más en general "densidad de color media" y "nivel de color medio", es decir, tono medio

del color cuando el color no es negro.

Ventajosamente, el patrón visible contiene una signatura que puede verificarse localmente por medio de un dispositivo conectado directamente con el lector de código de barras para comprobar la autenticidad del código de barras. Por tanto, en el presente texto, una "signatura" es información secundaria que se controla localmente, formando de este modo información secundaria de primer nivel de seguridad. Dicha signatura constituye una forma sencilla de verificar que el código de barras 2D es original comparando la signatura decodificada del código de barras 2D que se comprobará con una referencia (clave de signatura) que puede estar disponible localmente, por ejemplo, en un teléfono inteligente que se usa como lector de código de barras o cualquier otro dispositivo usado como lector de código de barras o que contiene un lector de código de barras, en particular un dispositivo móvil, conectado directamente con el lector de código de barras, para suministrar una indicación sobre la presencia de la signatura correcta o de una signatura errónea en el código de barras 2D, ofreciendo así una indicación acerca del carácter original o del carácter no original (copia) del código de barras 2D. Por ejemplo, se usa una primera clave K1 generada de forma pseudoaleatoria (o "clave de signatura") para todos los códigos de barras 2D y está presente en o disponible para el dispositivo móvil: la reconstitución de la signatura fuente se realiza preferentemente usando la primera clave K1 y parte de un mensaje de código 2D, es decir, información primaria (por ejemplo, ID único presente como parte del patrón de información primaria) a través de un primer algoritmo presente en el dispositivo móvil: por tanto, la comprobación de autenticación de primer nivel de seguridad se implementa comparando la signatura del código de barras 2D que se comprobará y dicha signatura fuente (siendo dicha "comparación" por ejemplo un cálculo de semejanza de imágenes que produce una puntuación y una comparación de esa puntuación con un umbral). La primera comprobación de autenticación de seguridad puede ser ventajosa cuando el dispositivo de autenticación no está conectado a Internet. Otra ventaja importante de la signatura es la posibilidad de verificar localmente si el escaneo tiene una calidad de imagen apropiada realizando una medida de la signatura. Por ejemplo, si para tramas consecutivas la medida es estable y consistente, puede ser una indicación de que estas tramas pueden usarse para autenticación y pueden enviarse a un servidor remoto para una autenticación completa.

Ventajosamente, para mejorar el nivel de seguridad de autenticación, además o como alternativa a dicha signatura, dicho patrón visible contiene además una parte secreta cuya autenticidad puede verificarse solo por medio de un dispositivo remoto. Por tanto, en el presente texto, una "parte secreta" es información secundaria que se controla solo de forma remota, formando de este modo información secundaria de segundo nivel de seguridad (siendo el segundo nivel de seguridad de nivel superior al primer nivel de seguridad). Dicha parte secreta forma un elemento de seguridad adicional, formado por una parte de imagen del patrón visible, es decir, un patrón único (patrón de ruido único), que en este caso se genera aleatoriamente, que se compara con una referencia (clave secreta) que puede estar disponible solo en un equipo remoto (por ejemplo, la clave secreta es parte de una base de datos presente en un servidor remoto). Al requerir esta situación un intercambio de información entre el lector de código de barras 2D y el servidor remoto, solo las personas que tienen acceso al servidor remoto pueden usar este procedimiento de autenticación remota. Además, el hecho de haber registrado la clave secreta en un servidor remoto permite usar información oculta y difícilmente accesible en la parte secreta. Por ejemplo, la clave secreta forma parte de una lista de partes secretas originales almacenadas de forma remota. Por ejemplo, las segundas claves (o "claves secretas") K2, K2'..., diferentes para cada código de barras o para cada serie de códigos de barras 2D, están presentes solo en el servidor remoto (base de datos segura), son generadas preferentemente de forma auténticamente aleatoria (pero además pueden ser generadas de forma pseudoaleatoria o generadas parcialmente de forma verdaderamente aleatoria/parcialmente de forma pseudoaleatoria). La reconstitución de la parte secreta fuente se realiza a partir de la segunda clave K2 solo presente en el servidor remoto a través de un segundo algoritmo (opcionalmente, dicha reconstitución de parte secreta fuente usa también una parte de mensaje de código 2D, es decir, información primaria (por ejemplo, ID único)). Dicho segundo algoritmo puede estar presente en cualquier lugar lo que incluye dicho dispositivo móvil o dicho servidor remoto. Por tanto, la comprobación de autenticación de segundo nivel de seguridad se implementa por comparación entre la parte secreta del código de barras 2D que se comprobará y dicha parte secreta fuente. Como alternativa al uso de dicha segunda clave K2, la parte secreta fuente, es decir, el patrón, está almacenado en el servidor remoto, de manera que se realiza directamente una comparación entre dicha parte secreta fuente y dicha parte secreta 426 del código de barras 2D que se comprobará. Dicha "comparación" puede ser por ejemplo un cálculo de semejanza de imágenes que produce una puntuación y una comparación de esa puntuación con un umbral. Puede observarse que la signatura puede someterse a comprobación en detalles adicionales y con mayor precisión en el dispositivo remoto, por comparación con más información de referencia, como escaneos de referencia de impresiones originales y umbrales basados en los mismos que están almacenados en el dispositivo remoto.

Ventajosamente, dicha parte secreta puede reconstituirse usando una clave secreta (K2) presente solo en dicho dispositivo remoto. Dicha parte secreta es una segunda parte de datos que forma una parte adicional de la huella digital (patrón visible), y que mejora el nivel de seguridad de autenticación de código de barras 2D: datos generados de forma pseudoaleatoria de la segunda parte de datos forman datos que solo pueden recuperarse con una rutina (operaciones de programa) compleja. Si por ejemplo dicha segunda parte de datos puede recuperarse de al menos información primaria, solo es posible acceder correctamente a la información secundaria cuando la información primaria ha sido decodificada correctamente de antemano. Además, según otra alternativa más segura, cuando la segunda parte de datos solo puede recuperarse conjuntamente de la información primaria y la primera parte de datos generada aleatoriamente de dicha signatura, la información secundaria solo es accesible correctamente

cuando de antemano se ha decodificado o comparado con una fuente tanto la información primaria como la primera parte de datos, es decir, la signatura.

Además, dicho patrón visible puede contener solo una signatura, solo una parte secreta o tanto una signatura como una parte secreta. Las zonas en las que se codifican la signatura y la parte secreta pueden estar separadas físicamente o no. La parte de este patrón visible (información secundaria) formada por una signatura, una parte secreta o tanto una signatura como una parte secreta puede considerarse técnicamente una huella digital.

Breve descripción de los dibujos

La invención se entenderá mejor con la ayuda de la descripción de realizaciones ofrecidas a modo de ejemplo e ilustradas por las figuras, en las que:

las Fig. 1 a 6 muestran vistas esquemáticas de diferentes realizaciones de códigos de barras QR fuente que forman códigos de barras 2D según la invención, en una escala ampliada usada con fines de claridad;

la Fig. 7 es una ilustración de un procedimiento de autenticación de un código de barras 2D según la invención;

la Fig. 8 es un organigrama que ilustra una realización de ejemplo de un procedimiento de autenticación según la invención.

la Figura 9 es una vista esquemática de un código de barras 2D fuente según una realización de la invención, en una escala ampliada con fines de claridad;

la Figura 10a es una vista esquemática de un código de barras 2D fuente según otra realización de la invención, en una escala ampliada con fines de claridad, y la Fig. 10b es una vista ampliada del patrón visible de información secundaria del código de barras 2D de la figura 10a;

la Fig. 11a es una vista ampliada del patrón visible de la realización de la figura 10b después de la impresión (primera impresión original) y la figura 11b es una copia (escaneo y reimpresión) de la impresión original de la figura 10b.

Descripción detallada de realizaciones de la invención

La Figura 1 muestra un primer ejemplo de un código QR que forma una primera realización para un código de barras 2D 100 según la invención. Este código de barras 2D 100 está formado por un símbolo que tiene una forma general cuadrada y que comprende patrones habituales de un código QR, en concreto un patrón de detección de tres posiciones 130 situado en tres de las cuatro esquinas del código QR, y un área de datos 132. Esta área de datos 132 incluye un primer patrón de información primaria 110 formado por una disposición elegida de celdas elementales 102, que en este caso es de 10 × 10 píxeles, y mostrada de forma no limitativa en forma de cuadrados. Estas celdas elementales 102 son información primaria de codificación y tienen un tamaño que permite que la mayor parte de las máquinas copiadoras copien el patrón de información primaria 110 sin alterarlo o con una alteración tan pequeña que este patrón puede ser decodificado correctamente y no existe alteración en la información almacenada en las celdas. El tamaño típico pero no limitativo de las celdas elementales 102 que codifican información primaria en el patrón de información primaria 110 del código de barras 2D original 100 está comprendido entre 5 × 5 píxeles y 90 × 90 píxeles, por ejemplo entre 8 × 8 píxeles y 12 × 12 píxeles. Dependiendo de la resolución de impresión (que puede ser de 600 puntos por pulgada, 2.400 puntos por pulgada, o cualquier otro valor dependiendo del dispositivo de impresión) esto puede corresponder a un tamaño típico pero no limitativo (dimensión máxima) de las celdas elementales 102 del código de barras 2D original 100 comprendido entre 0,05 mm y 3 mm, especialmente entre 0,1 y 2 mm, preferentemente entre 0,2 y 1 mm, y preferentemente entre 0,3 y 0,5 mm.

Según la invención, este código de barras 2D 100 contiene además, en el área de datos cuadrada 132 y de forma separada al patrón de información primaria 110, un patrón visible 120 con información secundaria. En esta primera realización mostrada en la Figura 1, este patrón visible 120 es un cuadrado situado en una posición central en el patrón de información primaria 110, formando con ello un bloque separado o una isla integrada en el patrón de información primaria 110. Más en general este patrón visible 120 podría tener una forma rectangular, u otra forma geométrica para reconocerlo fácilmente y recogerlo del patrón de información primaria 110, con el fin de que sea decodificado preferentemente por separado de la información primaria del patrón de información primaria 110.

Como puede verse en la figura 1, este patrón visible 120 está formado por subceldas elementales negras y blancas 122 que también se han representado como una disposición escogida de píxeles (mostrados de forma no limitativa como cuadrados) que son menores que las celdas elementales 102 que forman el patrón de información primaria 110 y que codifican la información secundaria. El tamaño de las subceldas elementales 122 permite que la mayoría de las máquinas copiadoras copien el patrón de información secundaria 110 con una alteración suficientemente significativa para impedir una decodificación correcta posterior de este patrón visible 120. Una característica importante de la presente invención no es cuánta información existe en la huella digital y más en general en el

patrón visible 120 original antes de la impresión o el copiado, sino cuánta información existe después de la impresión o copiado en el patrón visible 120. Para el mismo patrón visible 120, los efectos de impresión o copiado y la densidad de información en el patrón visible 120 impreso o copiado dependerán de las propiedades de impresión o copiado (tipo de impresora o máquina copiadora, tipo de tinta de papel y requisitos de densidad de color específica para el trabajo de impresión o copiado). El tamaño típico pero limitativo de las subceldas elementales 122 que codifican información secundaria en el patrón visible 120 está comprendido entre 1 × 1 píxeles y 5 × 5 píxeles, especialmente entre 1 × 1 píxeles y 3 × 3 píxeles, y preferentemente es de 1 × 1 píxeles o 2 × 2 píxeles. Esto puede corresponder a un tamaño típico pero no limitativo (dimensión máxima) de subceldas elementales 122 de código de barras 2D original 100 comprendido entre 5 μm (micrómetros) y 50 μm. Por ejemplo, para una resolución de la impresora de 600 ppi (píxeles por pulgada), un tamaño típico para el código de barras 2D original 100 es de aproximadamente 1,11 cm de longitud de lado del cuadrado, con 33 × 33 celdas elementales 102 que tienen cada una un tamaño de aproximadamente 0,34 mm, y con un patrón visible de 8 × 8 subceldas elementales 122 estando cada una formada por un píxel que tiene un tamaño de aproximadamente 40 μm (micrómetros).

En las realizaciones el patrón visible 120 de información secundaria puede comprender ventajosamente (véanse las figuras 1, 9, 10a) un borde 121 que mejora la recuperación y la selección de la información secundaria. En una realización ventajosa (véanse las figuras 9, 10a), el borde 121 puede comprender un borde negro 121 y alrededor un borde blanco o espacio que separa el patrón visible 120 de información secundaria del código de barras 110 primario para facilitar una identificación rápida y sencilla del patrón visible y reducir los errores de lectura.

Como primera variante preferida, este patrón visible 120 no está situado exactamente en una posición central, sino que cubre el centro de dicho símbolo que expresa materialmente este código de barras 2D 100: en dicha configuración no mostrada, este patrón visible 120 se desplaza ligeramente hacia abajo, hacia arriba, a la izquierda o a la derecha con respecto a la posición centrada exacta mostrada en la figura 1. La colocación del patrón visible 120 que cubre el centro de dicho símbolo que expresa materialmente este código de barras 2D 100 puede ser ventajosa ya que cuando el código de barras 2D se captura con un lector de código de barras o un dispositivo de escaneo tal como un teléfono móvil, el centro del código de barras 2D está cerca a menudo del centro de la imagen capturada, que tiende a estar más enfocada. Por tanto el patrón visible 120 tenderá a estar cerca del centro de la imagen escaneada, que normalmente tiene menos aberración geométrica y está más enfocada.

Como otra variante este patrón visible 120 no está situado en ni cubre una posición central sino que está situado en cualquier otro lugar en el límite de dicha área de datos cuadrada 132, o más en general en el límite de dicho símbolo que forma dicho código de barras 2D 100.

Además, este patrón visible 120 se muestra en la figura 1 como una única parte formada por dos partes adyacentes 120a y 120b, cada una de las cuales tiene una densidad de negro media o un nivel de gris medio diferentes. Estas dos partes 120a y 120b de la figura 1 se representan como un rectángulo con igual tamaño y forma pero podrían tener tamaños y/o formas diferentes. En la figura 1, la parte izquierda 120a está representada con una densidad de negro media o nivel de gris medio bajos de aproximadamente el 20 % de subceldas elementales negras 122 mientras que la parte derecha 120b está representada con una densidad de negro media o nivel de gris medio altos de aproximadamente el 80 % de subceldas elementales negras 122, con lo cual el nivel de gris medio global de este patrón visible 120 es de aproximadamente el 50 % de subceldas elementales negras 122. En la figura 1 se han usado densidades de negro del 20 % y el 80 % por motivos de visibilidad en los dibujos, aunque pueden usarse otros valores de densidad de negro diferentes del 50 % ± 5 % para una o varias partes del patrón visible: Como valores de densidad de negro muy probables puede usarse una densidad de negro media baja de aproximadamente el 40 % de subceldas elementales negras 122 y una densidad de negro media alta de aproximadamente el 60 % de subceldas elementales negras 122. Más en general, una densidad de negro media baja diferente del 0 %, desde el 1 % al 45 % de subceldas elementales negras 122 se asocia con una densidad de negro media alta diferente del 100 %, desde el 55 al 99 % de subceldas elementales negras 122. Usando esta disposición o incluso una disposición similar con más de dos partes, y preferentemente un número par de partes, la formación de dicho patrón visible 120 constituye una disposición preferida. Una densidad de negro media y preferentemente dos o más de dos densidades de negro medias diferentes del 50 % ± 5 % de subceldas elementales negras que forman la información secundaria elevan al máximo la densidad de información en el código de barras 2D original dado que cubre paneles grandes de propiedades de impresión óptima (como la ganancia de puntos) que por sí mismas pueden variar durante una sucesión de impresiones. Una densidad de información más elevada hace más difícil la copia ya que existe más información para replicar.

Existen situaciones en las que no es posible saber con antelación cuál será la densidad de negro media óptima, por ejemplo si no fuera posible probar la impresora por adelantado. Existen también situaciones en que la densidad óptima de la huella digital puede variar durante la impresión. Esto puede suceder por ejemplo si la densidad de la tinta, o la viscosidad, varía durante la impresión. Para ciertos tipos de impresión, por ejemplo rotograbado, puede usarse la misma huella digital (patrón visible) durante un periodo de tiempo prolongado, siempre que se use el cilindro en la aplicación, es decir, varios meses. Claramente, es probable que las propiedades de impresión evolucionen a medida que se desgasta el cilindro. Para afrontar estos efectos, el patrón visible está compuesto preferentemente por diferentes áreas con diferentes densidades de negro. A continuación, puede realizarse la determinación de autenticidad usando las áreas en las que se imprimió de una forma que es la más favorable para

su capacidad de detectar copias. Como una realización preferida, dicho patrón visible 120 está formado por una primera parte que tiene una primera densidad de negro media o primer nivel de gris medio y una segunda parte que tienen una segunda densidad de negro media o segundo nivel de gris medio que es diferente de la primera densidad de negro media, siendo la primera y la segunda densidad de negro media diferentes del 50 % ± 5 % de subceldas elementales negras. Como una posibilidad, el promedio entre dicha primera densidad de negro media y dicha segunda densidad de negro media es de aproximadamente el 50 % de subceldas elementales negras 122. Como una alternativa no mostrada, este patrón visible 120 está formado por dos o más partes separadas distribuidas en una posición relativa no adyacente, esto es, en diferentes posiciones de dicho símbolo que expresa materialmente este código de barras 2D 100, estando una de estas partes colocada preferentemente cubriendo la posición central en el patrón de información primaria 110. Estas dos o más partes separadas podrían tener niveles de gris medios iguales o diferentes entre sí, preferentemente con una densidad de negro o nivel de gris claramente diferente del 50 % de subceldas elementales negras/píxeles, en concreto menor que el 45 % de celdas elementales negras o mayor que el 55 % de subceldas elementales negras, de manera que se eleve al máximo la densidad de información en el código de barras 2D original y por tanto aumente la tasa de degradación cuando este código de barras 2D 100 sea reproducido por una máquina copiadora.

El patrón visible 120 mostrado en la figura 1 se define también por medio de una tercera parte 120c que forma la frontera del patrón visible 120 y que se muestra en la figura 1 como una línea continua de subceldas elementales negras 122 alineadas en una fila doble que forma un bucle cuadrado cerrado. Dicha tercera parte es útil para ayudar al reconocimiento del patrón visible 120 por el lector de código de barras aunque puede omitirse.

Este código de barras 2D 100 modificado mostrado en la Figura 1 es una forma preferida de un tipo modificado de código QR con un símbolo codificado con 29 × 29 celdas elementales 102, con un patrón visible 120 que codifica información secundaria con una zona formada por 9 × 9 celdas elementales 102. Como una alternativa no mostrada, el patrón visible 120 codifica información secundaria con la zona formada por 10 × 10 celdas elementales 102 o por 8 × 8 celdas elementales 102. Dicha situación es un buen compromiso entre buena legibilidad del código QR, teniendo en cuenta el nivel de corrección de errores aceptable para posible daño cuando se lee la información secundaria, y el límite de decodificación del área usada para información secundaria.

Como representación puramente ilustrativa, en la Figura 1 el patrón visible 120 que codifica información secundaria contiene 27 × 27 subceldas elementales 122. Por tanto cada celda elemental 102 de la información primaria es sustituida por 3 × 3, es decir, 9 subceldas elementales 122, teniendo cada subcelda elemental 122 un píxel.

La Figura 2 muestra un segundo ejemplo de un código QR modificado que forma una segunda realización para un código de barras 2D 200 según la invención. Los números de referencia usados para describir este código de barras 2D 200 son los mismos que para las partes idénticas ya mostradas en la figura 1 y aumentan en 100 para partes similares con respecto a las de la figura 1.

En este caso el símbolo que forma el código de barras 2D 200 modificado está formado por un área de datos cuadrada 232 que contiene tres patrones de detección de posición 130a, un patrón de información primaria 210 y un patrón visible 220. En esta segunda realización, la información secundaria está integrada por un patrón visible 220 que no está situado en el área central del área de datos cuadrada 232 sino que está situado en la esquina del área de datos cuadrada 232 que no contiene un patrón de detección de posición 130 (en este caso en la esquina inferior derecha). Esta situación no perturba la función de detección de posición de los tres patrones de detección de posición 130 ya que permanecen en el mismo lugar y no se han modificado. Sin embargo, debe observarse que los códigos QR de la versión 2 y anteriores contienen un cuarto patrón de detección de posición menor en la parte inferior derecha del código, que puede verse afectado por la información secundaria. Además, en esta segunda realización, el patrón visible 220 contiene información secundaria codificada con densidad de negro media intermedia o nivel de gris medio intermedio, es decir, una única parte que tiene una densidad de negro media o un nivel de gris medio de aproximadamente el 50 % de subceldas elementales negras 122, es decir, preferentemente que tiene una densidad de negro media o nivel de gris medio comprendido entre el 45 y el 55 % de subceldas elementales negras 122. Como variante no mostrada de esta segunda realización, el código de barras 2D 200 está formado por un área de datos cuadrada 232 que contiene tres patrones de detección de posición 130 y, aparte de estos patrones de detección de posición 130, el área de datos cuadrada 232 contiene solo el patrón de información primaria 210. Esto corresponde a la situación en que la información secundaria está integrada por un patrón visible 220 situado en uno del patrón de detección de posición 130 para formar con ello un patrón de detección de posición modificado que contiene el patrón visible 220. Esta situación no perturba la función de detección de posición del patrón de detección de posición 230 modificado ya que permanece en el mismo lugar y tiene la misma forma cuadrada, el mismo tamaño y además está delimitado por una misma línea cuadrada negra continua que los patrones de detección de posición 130 no modificados. En esta variante no mostrada de esta segunda realización los otros dos patrones de detección de posición 130 no están modificados pero también pueden modificarse para contener un patrón visible 220 adicional.

La Figura 3 muestra un tercer ejemplo de un código QR modificado que forma una tercera realización para un código de barras 2D 300 según la invención. Los números de referencia usados para describir este código de barras 2D 300 son los mismos que para las partes idénticas ya mostradas en la figura 1 y se incrementan en 200 para partes

similares con respecto a las de la figura 1.

Al igual que el código de barras 2D 100 de la figura 1, el código de barras 2D 300 de la Figura 3 contiene un patrón visible 320 con información secundaria que está centrada en el patrón de información primaria 310, que significa una correspondencia entre el centro geométrico del patrón visible 320 y el centro geométrico del patrón de información primaria 310. En esta tercera realización, el patrón visible 320 está formado por una primera parte cuadrada 320a que tiene una primera densidad de negro media baja o un primer nivel de gris medio bajo y que está situado en posición central dentro del patrón visible 320, y una segunda parte 320b con una segunda densidad de negro media alta o un segundo nivel de gris medio alto y que rodea a dicha primera parte cuadrada 320a. Esta segunda parte 320b se divide en cuatro subpartes cuadradas $320b_1$, $320b_2$, $320b_3$ y $320b_4$ dispuestas en cruz, cada de las cuales tiene un lado lateral que bordea a un lado lateral diferente de la primera parte cuadrada 320a. Al igual que en otras realizaciones, el área de datos 332 contiene tres patrones de detección de posición 130, el patrón de información primaria 310 y el patrón visible 320 que contiene la información secundaria de forma separada de la información primaria. El patrón visible 320 se ilustra con un tamaño que cubre una superficie de más del 10, el 15 o incluso el 20 % de la superficie total del área de datos cuadrada 232 aunque según la invención se prefiere un tamaño más limitado con respecto a la superficie total del área de datos 232 para el patrón visible 320, en concreto un patrón visible 320 que cubre menos del 20 % y preferentemente menos del 13 % de la superficie total del área de datos cuadrada 232. Dicha disposición permite que la inserción de la información secundaria no afecte a la legibilidad de la información primaria del código QR. La información secundaria puede estar en cualquier forma deseada que represente por ejemplo un logotipo, una marca comercial u otras formas de fantasía deseadas por el productor.

La Figura 4 muestra un cuarto ejemplo de un código QR modificado que forma una cuarta realización para un código de barras 2D 400 según la invención. Los números de referencia usados para describir este código de barras 2D 400 son los mismos que para las partes idénticas ya mostradas en la figura 1 y se incrementan en 300 para partes similares con respecto a las de la figura 1.

También en este caso el código de barras 2D 400 de la figura 4 contiene un patrón visible 420 con información secundaria que recubre el centro del patrón de información primaria 410 y del área de datos 432, a la vez que está separado de la información primaria. El patrón visible 420 de la cuarta realización es un rectángulo dividido en zonas separadas que codifican diferentes tipos de información. Más en concreto, el patrón visible 420 se divide en una zona 424 que contiene una signatura (parte derecha del patrón visible 420) y una zona 426 que contiene una parte secreta (parte izquierda del patrón visible 420). Además, en esta realización, la parte secreta está contenida en una zona 426 que se divide en una primera parte de datos 426a (parte izquierda de las zonas de parte secreta 426) y una segunda parte de datos 426b (parte derecha de las zonas de parte secreta 426) que tienen dos densidades diferentes, tales como el 40 % y el 60 % de densidades de negro para las sub-celdas 122 para estas dos partes secretas 426 diferentes.

Tal como se describe de acuerdo con estos ejemplos primero a cuarto de un código QR que forma de la realización primera a la cuarta para un código de barras 2D según la invención, es ventajoso sustituir completamente un área de la información primaria del código de barras 2D con la información secundaria representada por el patrón visible, ya que la información secundaria limitada a una zona homogénea en información primaria se procesará de manera más fácil y fiable.

La Figura 5 muestra un quinto ejemplo de un código QR modificado que forma una quinta realización para un código de barras 2D 200 según la invención. Los números de referencia usados para describir este código de barras 2D 500 son los mismos que para las partes idénticas ya mostradas en la figura 1 y se incrementan en 400 para partes similares con respecto a las de la figura 1.

La principal diferencia con las realizaciones primera a cuarta ya descritas reside en el hecho de que en la realización quinta (y sexta) el patrón visible 520, que contiene información secundaria codificado con subceldas elementales 122 (píxeles pequeños) no está situado en la frontera del patrón de información primaria 510 sino fuera del límite de dicho patrón de información primaria 510, dentro todavía del símbolo que forma el código QR modificado y delimitado por el área de datos 532. El patrón visible 520 de esta quinta realización está formado por dos rectángulos: una primera parte 520_1 del patrón visible 520 se extiende a lo largo de todo el borde izquierdo del patrón cuadrado de información primaria 510 y una segunda parte 520_2 del patrón visible 520 se extiende a lo largo del borde derecho completo del patrón cuadrado de información primaria 510. El área de datos 532 tiene por tanto en este caso específico una forma rectangular cuya longitud se extiende entre las dos partes 520_1 y 520_2. El contenido y la distribución de datos entre las dos partes 520_1 y 520_2 del patrón visible 520 puede variarse, teniendo una zona de signatura y/o zonas de parte secreta con solo la primera parte de datos 520_1 o solo la segunda parte de datos 520_2 o tanto la primera parte de datos 520_1 como la segunda parte de datos 520_2. En este caso, este patrón visible 520 tiene una densidad de negro media intermedia o un nivel de gris medio intermedio, en concreto una densidad de negro media o un nivel de gris medio de aproximadamente el 50 % de subceldas elementales negras 122, es decir, tiene preferentemente una densidad de negro media o un nivel de gris medio comprendidos entre el 45 y el 55 % de subceldas elementales negras 122. En la figura 5, el patrón visible 520 tiene una densidad de negro media o un nivel de gris en la superficie completa de las dos partes 520_1 y 520_2 aunque es posible una densidad de negro o un nivel de gris promedio diferentes y/o una distribución diferente de la densidad de negro media.

La Figura 6 muestra un sexto ejemplo de un código QR modificado que forma una sexta realización para un código de barras 2D 600 según la invención. Los números de referencia usados para describir este código de barras 2D 600 son los mismos que para las partes idénticas ya mostradas en la figura 1 y se incrementan en 500 para partes similares con respecto a las de la figura 1. En este caso, el patrón visible 620 de esta sexta realización está formado por solo un cuadrado situado en el borde de la parte central del lado (derecho) del patrón cuadrado de información primaria 610. El área de datos 632 tiene por tanto en este caso específico una forma poligonal hecha a partir de un patrón de información primaria 610 (patrón de información primaria 610) y un cuadrado menor (patrón visible 620) colocado a lo largo de dicho patrón de información primaria 610.

Cuando el patrón visible que contiene información secundaria está situado fuera del área del patrón de información primaria, puede ser ventajoso imprimirlo en un momento diferente, o con una máquina de impresión diferente. Por ejemplo, la información secundaria se imprime primero con impresión offset, y a continuación la información primaria se imprime con impresión por inyección de tinta. Cuando los dos patrones de información se imprimen en máquinas de impresión diferentes, a menudo sucede, aunque no necesariamente, que el patrón de información secundaria se imprime con un procedimiento de impresión estática (offset, flexografía, rotograbado, etc.) y por tanto no cambia para cada impresión o producto. No obstante, existen diversas situaciones en las que esto resulta ventajoso: por ejemplo si el medio para imprimir el patrón de información primaria tiene una calidad o resolución insuficiente para imprimir el patrón de información secundaria, o si existen restricciones técnicas en la transferencia de datos, la seguridad, la aplicación preexistente para marcar la información primaria que no puede modificarse, etc. En estos casos, puede ser ventajoso usar las mismas claves de generación para el patrón de información secundaria, para un lote o conjunto de códigos que tienen el mismo patrón de información secundaria.

En las figuras, los patrones patrón de información primaria 610, 510 y 210 son exactamente iguales en forma, tamaño de píxel y disposición de píxeles aunque esta es solo una ilustración de ejemplo ya que para patrones de información primaria son posibles todas las formas, tamaños de píxel y disposiciones de píxeles.

Un ejemplo para la aplicación de la quinta realización o la sexta realización es la situación en que es suficiente o se prefiere solo un pequeño código de barras 2D (por ejemplo, un código QR de 4 x 4 mm). En este caso, un patrón visible, y en particular una zona de huella digital que usa aproximadamente el 10-12 % de la superficie puede ser demasiado pequeño para asegurar una distinción fiable de las impresiones originales y las copias. El planteamiento consiste en colocar el patrón visible fuera del cuadrado definido por el patrón de información primaria y que forma el formato de código QR estándar: en la Figura 5 el patrón visible 520 está situado a lo largo de dos lados opuestos del patrón de información primaria 510 y en la figura 6 el patrón visible 620 está situado a lo largo de una parte de un lado (derecho) del patrón de información primaria 510. Son posibles otras formas y disposiciones no visibles para el patrón visible como una situación "general" en la que el patrón visible forma un bucle cerrado que rodea al patrón de información primaria (para mantener el tamaño del cuadrado), o en o a lo largo de solo un lado (por ejemplo, como un patrón cuadrado visible que tiene el mismo tamaño que el patrón de información primaria que define un código QR habitual).

A modo de ejemplo, un procedimiento para crear códigos QR seguros asocia un único patrón de ruido, denominado huella digital (información secundaria contenida tanto en la signatura 424 y como en la parte secreta 426 de las zonas de patrón visible 420), con un código QR específico (información primaria contenida en el patrón de información primaria 410) y/o con un ID único (presente como parte del patrón de información primaria 410). En principio, el código QR puede contener un mensaje arbitrario. Por ejemplo, el código QR puede contener un único enlace con una dirección web, que puede consultarse si un usuario escanea el código QR con un lector de código de barras arbitrario. Por ejemplo http://www.example.com/135dgk86f37gks9 en la que http://www.example.com/ es el prefijo y 135dgk86f37gks9 es un ID único (más en general podría ser un ID único e información encriptada). Este mensaje y/o el ID único permiten recuperar información relacionada con este código QR, y en particular información que se refiere a la huella digital, es decir, especialmente la parte de la información secundaria contenida en la zona de signatura 424 de patrón visible 420, y que puede usarse para autenticación del código QR.

El ID único (parte de la información primaria) puede generarse con un generador de números aleatorios verdadero. Además pueden encriptarse importantes parámetros (umbral de puntuación - umbral de signatura predeterminado y/o umbral de parte secreta predeterminado, número de versión de la huella digital (información secundaria contenida en la zona de signatura 424 y/o las zonas de parte secreta 426 del patrón visible 420), posición y tamaño del patrón visible 420 con respecto al código QR (información primaria), segundas claves K2, K2' usadas para generar parte del patrón visible 420) y añadirse al ID único. Esta información puede ser decodificada en un dispositivo remoto sin conexión con el servidor, lo que permite la autenticación local parcial así como la validación de calidad de la imagen antes del envío a un servidor remoto para una autenticación remota completa.

El uso de la información primaria del código 2D (ID único) permite preparar una información secundaria (en particular, una parte secreta) que cambiará para cada mensaje de código 2D incluso si se usa la misma clave K2. La parte secreta puede generarse también con un generador de números aleatorios verdadero. En este caso, la parte secreta completa se almacena en una base de datos segura en asociación con la información primaria del código 2D (o cualquier ID único formado por información derivada del mismo). Como se explicará adicionalmente, un

planteamiento relacionado consiste en almacenar escaneos del código de barras 2D en la base de datos segura.

El generador de números aleatorios verdaderos (GNAV) y los generadores de números seudoaleatorios (GNSA) para generar la información secundaria, y especialmente la parte secreta, tienen ventajas y desventajas. Claramente una ventaja de los GNSA es que la clave secreta puede ser compartida más fácilmente entre el servidor seguro y otros servidores o dispositivos. Por ejemplo, un dispositivo móvil equipado con la segunda clave K2 tendrá la capacidad de generar localmente la parte secreta, y podría usar la parte secreta generada localmente para realizar una comprobación de autenticidad sin conectarse con el servidor seguro. Esto permite una respuesta más rápida incluso en tiempo real al usuario, y permite una comprobación de autenticidad incluso cuando no es posible la conexión con el servidor seguro.

Sin embargo, una desventaja conocida es que toda la información necesaria para generar partes secretas válidas está almacenada en una clave, y si esta información está almacenada en múltiples servidores o dispositivos, existen riesgos mayores de que un falsificador obtenga acceso a la clave poniendo en riesgo los dispositivos.

Un compromiso entre seguridad y capacidad de uso consiste en hacer que parte del patrón visible que forma dicha parte secreta se genere de forma puramente aleatoria, y otra parte se genere de forma pseudoaleatoria. Por tanto, puede realizarse una comprobación de autenticidad con la parte pseudoaleatoria de la parte secreta, y una comprobación de autenticidad con la parte puramente aleatoria. La segunda clave K2 o claves K2, K2' usadas para generar las partes pseudoaleatorias pueden ponerse a disposición de servidores o dispositivos autorizados, que pueden usarlas para realizar una comprobación de autenticidad sin conectarse con la base de datos. E incluso si estas segundas claves K2, K2' se ven comprometidas, la parte puramente aleatoria de la parte secreta sigue siendo segura, y permitiría detectar cualquier fraude cuando se pusiera en riesgo la parte pseudoaleatoria.

Otra forma de implementar este compromiso consiste en usar una segunda clave K2 para generar una parte de datos que se usa solo para este código de barras 2D en particular y la parte secreta asociada, y solo puede recuperarse a partir de una base de datos; mientras que la otra segunda clave K2' usada para generar la otra parte de datos es compartida por una serie de códigos de barras 2D y la parte secreta asociada, y esta otra segunda clave K2' puede almacenarse en dispositivos remotos.

Después de la creación de un código de barras 2D fuente, este código de barras 2D se usa en un producto (tal como un documento, una etiqueta, artículos de consumo o un envase) o un lote de productos después de la impresión, formando de este modo un código de barras 2D original que se integra en un producto tal como se define en la reivindicación 9. Si este código de barras 2D original es reproducido (copiado o escaneado) para un uso no autorizado, este código de barras 2D falso o no original es detectado de acuerdo con el procedimiento de autenticación de un código de barras 2D tal como se define a continuación a través del fallo en un resultado de autenticación. Si dicho resultado de autenticación es acertado, dicho procedimiento de autenticación permite saber que el código de barras 2D integrado en un producto es en realidad un código de barras 2D original.

Según una realización, un procedimiento de autenticación de un código de barras 2D en un producto comprende:

- la lectura con un lector de código de barras 2D de un código de barras 2D (400),
- la identificación de un patrón visible (420) y la identificación en dicha información secundaria de dicha signatura (424) formando de este modo una signatura detectada,
- la comparación de dicha signatura detectada con una clave de signatura y la determinación en consecuencia de la comparación de una puntuación de semejanza de signatura,
- la comparación de dicha puntuación de semejanza de signatura con un umbral de signatura predeterminado, y
- el establecimiento de un resultado de signatura de autenticación como exitoso si dicho resultado es igual o mayor que dicho umbral de signatura predeterminado o como fallido si dicho resultado es menor que dicho umbral de signatura predeterminado.

Según una realización, el lector de código de barras 2D puede formar parte de un dispositivo móvil (20), en particular un teléfono inteligente, y en el que dicha clave de signatura está almacenada en dicho dispositivo móvil (20) que implementa la etapa de comparación entre dicha signatura detectada y dicha clave de signatura.

Según otra realización, un procedimiento de autenticación de un código de barras 2D (400) en un producto puede comprender:

- la lectura con un lector de código de barras 2D de dicho código de barras 2D (400),
- la identificación de dicho patrón visible (420) y la identificación en dicha información secundaria de dicha parte secreta (426) formando de este modo una parte secreta detectada,
- la comparación de dicha parte secreta detectada con una clave secreta de un código de barras 2D fuente y la determinación en consecuencia de la comparación como una puntuación de semejanza de parte secreta,
- la comparación de dicha puntuación de semejanza de parte secreta con un umbral de parte secreta predeterminado, y
- el establecimiento de un resultado de parte secreta de autenticación como exitoso si dicho resultado es igual o

mayor que dicho umbral de parte secreta predeterminado o como fallido si dicho resultado es menor que dicho umbral de parte secreta predeterminado.

El lector de código de barras 2D puede formar parte de un dispositivo móvil (20), en particular un teléfono inteligente, que está conectado con un dispositivo remoto (30), en el que dicha clave secreta de dicho código de barras 2D fuente está almacenada en dicho dispositivo remoto (30) que implementa la etapa de comparación entre dicha parte secreta detectada y dicha clave secreta, y en el que dicho procedimiento comprende además el reenvío de dicho resultado de parte secreta de autenticación a dicho dispositivo móvil (20).

La Figura 7 sirve de ilustración de procedimientos de autenticación de un código de barras 2D según la invención, para el control del carácter original de un código de barras 2D. Se considera un documento 10 (por ejemplo, un documento de garantía para cualquier equipo comprado recientemente), con un código de barras 2D 400 según la presente invención, que es un código de barras 2D original o que es un código de barras 2D no original, un dispositivo móvil 20 con un lector de código de barras 2D integrado (en este caso un teléfono inteligente) y un servidor remoto 30.

Estos procedimientos de autenticación para un código de barras 2D con un patrón visible que comprende una zona de signatura se describen teniendo en cuenta el código de barras 2D 400 de la figura 4 con un patrón visible 420 que tiene dicha zona de signatura 424 y dichas zonas de parte secreta 426 que forman conjuntamente una huella digital.

A continuación se describe un primer procedimiento de autenticación que puede usarse para cualquier código de barras 2D con un patrón visible que comprende al menos dicha signatura y que constituye un procedimiento de autenticación local de un código de barras 2D para una comprobación de baja seguridad. Este primer procedimiento de autenticación de un código de barras 2D se realiza para detectar si un producto tiene un código de barras 2D original o un código de barras 2D no original, y comprende las etapas siguientes:

- lectura (escaneo) con dicho lector de código de barras 2D del dispositivo móvil 20 de dicho código de barras 2D 400, formando de este modo una imagen 400' (código de barras 2D escaneo) de dicho código de barras 2D 400,
- decodificación de la información primaria contenida en el patrón de información primaria 410 (esta información primaria puede contener una indicación sobre la localización geométrica del patrón visible que contiene información secundaria que contiene información relevante para la selección y autenticación),
- localización en dicha imagen 400' de dicho patrón visible 420 (por selección) e identificación, en dicha información secundaria de dicha signatura (en la figura 4, zona 424) con dicho dispositivo móvil 20 formando de este modo una signatura detectada,
- comparación (por ejemplo, por función de correlación de imagen) de dicha signatura detectada con una clave de signatura (o signatura) de un código de barras 2D fuente disponible en dicho dispositivo móvil 20 (preprogramado en el mensaje de código de barras 2D del patrón de información primaria 410 o precargado desde un servidor) y determinación en consecuencia de la comparación de una puntuación de semejanza de signatura,
- comparación de dicha puntuación de semejanza de signatura con un umbral de signatura predeterminado (que puede insertarse por ejemplo en la información primaria que forma el mensaje de código QR, de manera que la autenticación pueda realizarse en el dispositivo móvil 20 sin ninguna conexión con el servidor 30, alternativamente puede haberse descargado previamente una lista de umbrales de signatura para cada signatura),
- establecimiento de un resultado de signatura de autenticación como exitoso (código de barras 2D original) si dicho resultado es igual o mayor que dicho umbral de signatura predeterminado o como fallido (copia y por tanto código de barras 2D no original) si dicho resultado es menor que dicho umbral de signatura predeterminado. Estas etapas pueden implementarse varias veces para el mismo escaneo o para escaneos diferentes de un supuesto mismo código de barras 2D original, con el fin de ayudar a determinar el umbral de signatura predeterminado que depende de la distribución típica de puntuaciones de semejanza de signatura para código de barras 2D original que pueden servir de referencia.

Alternativamente a la opción de comparar dicha signatura detectada con la clave de signatura de dicho código de barras 2D fuente (situación con un primer umbral de signatura predeterminado), otra opción consiste en comparar dicha signatura detectada con la clave de signatura de series de escaneos previos de códigos de barras 2D originales y que se adapta a lo largo del tiempo con nuevos escaneos de otros códigos de barras 2D originales (situación con un segundo umbral de signatura predeterminado diferente de dicho primer umbral de signatura predeterminado).

Como opción, cuando se decodifica información primaria, la extracción de un ID único y la encriptación de información que permite verificar si el código de barras 2D contiene una huella digital (signatura y/o parte secreta de información secundaria en un patrón visible), y los parámetros asociados útiles para autenticar la huella digital (signatura y/o parte secreta).

El planteamiento en el que el umbral de signatura predeterminado está almacenado en el código de barras 2D constituye una comprobación de seguridad de primer nivel con baja fiabilidad: si, por ejemplo, la producción fue de menor calidad de lo habitual, entonces puede aumentar la probabilidad de falsa alarma, salvo que el umbral preprogramado se ajuste a un valor intencionadamente bajo para evitar la falsa alarma, lo que al mismo tiempo

facilita potencialmente las copias para sortear el sistema. El umbral de signatura predeterminado puede ajustarse para compensar imperfecciones del escaneo. Estas imperfecciones pueden ser genéricas (calidad relativa del lector de código de barras) o depender de un escaneo en particular: por ejemplo, el código QR puede tener un tamaño esperado en píxeles, o un tamaño relativo para resecar el tamaño de imagen, en el escaneo si se captura con el dispositivo móvil a una distancia aproximada recomendada (por ejemplo, a 8 cm). Si el dispositivo móvil está más lejos (por ejemplo, 12 cm), el código QR será menor, y esta baja resolución de escaneo puede afectar al nivel de puntuación de semejanza de signatura. El umbral de signatura predeterminado puede ajustarse automáticamente para compensar una distancia subóptima con el dispositivo de captura. Un procedimiento alternativo consiste en hacer que el dispositivo móvil advierta al usuario de que el código QR no está a la distancia de lectura óptima y, por ejemplo, sugerirle que se acerque.

En una variante de dicho primer procedimiento de autenticación, cuando la puntuación de semejanza de signatura está por debajo del umbral de signatura predeterminado, se realizan algunas comprobaciones adicionales: por ejemplo, una o más lecturas consecutivas por debajo del umbral de signatura predeterminado pueden aportar una confirmación adicional de que el documento es una copia; además, las medidas de nitidez y otras distorsiones que afectan a la medida (por ejemplo, una alta transformación de perspectiva, una luz ambiental baja) pueden indicar también que debe realizarse otro escaneo antes de adoptar una decisión final. En una variante de dicho primer procedimiento de autenticación, dicho dispositivo móvil reconstituye dicha clave de signatura de dicho código de barras 2D fuente mediante un primer algoritmo presente en el dispositivo móvil usando una primera clave K1 (preferentemente generada de forma pseudoaleatoria) disponible en el dispositivo móvil y a partir de una parte de dicha información primaria (parte del patrón de información primaria 410 que forma un ID único).

Aunque es muy deseable una verificación instantánea, no debe ponerse en riesgo la seguridad. Por tanto, cuando se dispone de conectividad en red, al menos parte de la autenticación debe realizarse en el servidor seguro 30, para detectar un posible fraude y realizar una comprobación más completa.

A continuación se describe un segundo procedimiento de autenticación que puede usarse para cualquier código de barras 2D con un patrón visible que comprende al menos dichas zonas de parte secreta y que constituye una autenticación remota de un código de barras 2D para una comprobación de seguridad superior. Este segundo procedimiento de autenticación comprende

- la lectura (escaneo) con dicho lector de código de barras 2D del dispositivo móvil 20 (teléfono inteligente) de dicho código de barras 2D 400, que forma de este modo una imagen 400' (código de barras 2D escaneo) de dicho código de barras 2D 400,
- la decodificación de información primaria contenida en el patrón de información primaria 410 (esta información primaria puede contener una indicación acerca de la localización geométrica del patrón visible que contiene información secundaria que contiene información relevante para la selección y autenticación),
- la identificación (localización) en dicha imagen 400' de dicho patrón visible 420 (por selección) y la identificación (localización) en dicha información secundaria de dicha parte secreta (en la figura 4, zona 426) formando de este modo una parte secreta detectada,
- la comparación (por ejemplo, por función de correlación de imagen) de dicha parte secreta detectada con una clave secreta (o parte secreta) de un código de barras 2D fuente, que no está disponible en dicho dispositivo móvil 20, y la determinación en consecuencia de la comparación de una puntuación de semejanza de parte secreta,
- la comparación de dicha puntuación de semejanza de parte secreta con un umbral de parte secreta predeterminado,
- el establecimiento de un resultado de parte secreta de autenticación como exitoso (código de barras 2D original) si dicho resultado es igual o mayor que dicho umbral de parte secreta predeterminado o como fallido (copia y por tanto código de barras 2D no original) si dicho resultado es menor que dicho umbral de parte secreta predeterminado.

Alternativamente a la opción de comparar dicha parte secreta detectada con la clave secreta de dicho código de barras 2D fuente (situación con un primer umbral de parte secreta predeterminado), otra opción consiste en comparar dicha parte secreta detectada con la clave secreta de series de escaneos previos de códigos de barras 2D originales y que se adapta a lo largo del tiempo con nuevos escaneos de códigos de barras 2D originales (situación con un segundo umbral de signatura predeterminado diferente de dicho primer umbral de signatura predeterminado).

Dicha clave secreta está almacenada en dicho dispositivo remoto (servidor remoto 30). Por ejemplo, dicha clave secreta de dicho código de barras 2D fuente se obtiene mediante un segundo algoritmo que usa dicha segunda clave K2 que está presente solo en el servidor remoto 30 (base de datos segura), y opcionalmente usando una parte de dicha información primaria (parte del patrón de información primaria 410 que forma un ID único). Para este segundo procedimiento de autenticación, preferentemente dicho dispositivo móvil 20 está conectado con un dispositivo remoto (servidor remoto 30), en el que dicha clave secreta (o escaneos previos) está almacenada en dicho dispositivo remoto (servidor remoto 30) que implementa la etapa de comparación entre dicha parte secreta detectada y dicha clave secreta, y en el que dicho procedimiento comprende además el reenvío de dicho resultado de parte secreta de autenticación a dicho dispositivo móvil 20.

Los procedimientos de autenticación primero y segundo descritos anteriormente pueden combinarse. De esta forma,

se obtiene un compromiso interesante ya que una parte del patrón visible se verifica en el dispositivo móvil (la "autenticación de primer nivel") y una parte del patrón visible se verifica en el servidor seguro (la autenticación de segundo nivel). La comprobación de baja seguridad se realiza en tiempo real cuando el código QR (o patrón de información primaria 410) se decodifica, en una parte del patrón visible que puede generarse en el dispositivo móvil con la primera clave k1 correspondiente (almacenada en el dispositivo móvil) y el umbral de signatura (preprogramado en el mensaje de código QR -o patrón de información primaria- o precargado desde el servidor). Esta comprobación de baja seguridad puede servir como una forma de validación de la calidad de imagen: si la puntuación (resultado de signatura de autenticación) está por encima del umbral de signatura predeterminado, o la puntuación está por debajo del umbral de signatura predeterminado y la validación adicional confirma que el escaneo es adecuado para el análisis, el patrón visible se recopila del escaneo y se envía al servidor, junto con el mensaje de código QR y toda la información relevante de la comprobación de baja seguridad, tal como la geolocalización y el ID del dispositivo móvil. Mientras el dispositivo móvil está esperando la comprobación de alta seguridad del servidor, puede mostrarse ya un mensaje al usuario. En el caso en que la puntuación está por encima del umbral de signatura predeterminado para la comprobación de baja seguridad, este mensaje podría ser "Leído como original, en espera de resultados de la comprobación de alta seguridad del servidor". Si está por debajo del umbral de signatura predeterminado, la detección puede mostrar ya un mensaje que indique que el servidor 30 recibe el patrón visible recopilado y el mensaje de código QR (patrón de información primaria), así como la información adicional formada por la información secundaria. El mensaje de código QR (patrón de información primaria) permite recuperar los datos de huella digital de referencia (información secundaria original contenida en el patrón visible) necesarios para realizar la comprobación de alta seguridad. Esta información puede ser las partes de los datos fuente del patrón visible generados por el GNAV (segunda clave K2) o escaneos de referencia del mismo patrón visible. Se realizan una o más correspondencias de imagen, de manera que se producen una o más puntuaciones (resultado o resultados de parte secreta de autenticación). Una puntuación (resultado de signatura de autenticación o resultado de parte secreta de autenticación) calculada por correspondencia de imágenes con el patrón visible fuente (información secundaria del código de barras 2D fuente) estará generalmente en una escala diferente que la puntuación calculada por comparación con un escaneo de referencia, con lo que pueden usarse diferentes valores umbral dependiendo del patrón visible o de la parte del patrón visible usados para correspondencia de imágenes.

Si existe una puntuación comparación con un umbral de signatura predeterminado en el dispositivo móvil (comprobación de baja seguridad) y una o más comparaciones de puntuación con umbrales de parte secreta predeterminados correspondientes en el servidor seguro 30 (comprobación de alta seguridad), el mensaje de retorno del servidor al dispositivo puede ser cualquiera de los siguientes:

- todas las puntuaciones por encima del umbral: original,
- todas las puntuaciones por debajo del umbral: copia
- puntuación de comprobación de baja seguridad por debajo del umbral y todas las puntuaciones de comprobación de alta seguridad por encima del umbral: solicitar nuevo escaneo (probablemente un original pero no se estableció una correspondencia correcta en el escaneo en el dispositivo móvil),
- puntuación de comprobación de baja seguridad por encima del umbral y todas las puntuaciones de comprobación de alta seguridad por debajo del umbral: sospecha de fraude, ya que podría indicar que el falsificador ha accedido a las claves almacenadas en un dispositivo remoto para replicar correctamente la parte correspondiente de la huella digital, pero no las otras partes de la huella digital,
- resultados no coherentes, por ejemplo algunas puntuaciones están por encima del umbral y otras por debajo del umbral: solicitar al usuario un nuevo escaneo y/o retener el producto para investigación posterior.

Considérese el escenario en el que un dispositivo fuera pirateado y algunas claves de signatura se usaran para la comprobación de baja seguridad sustraída. Entonces un falsificador podría ser capaz de producir códigos QR (patrones de información primaria) con una signatura que es detectada como auténtica en el dispositivo. La comprobación de baja seguridad obtendrá probablemente una puntuación por encima del umbral de signatura. Sin embargo, las comprobaciones de alta seguridad en el servidor seguro 30 probablemente producirían puntuaciones por debajo del umbral de signatura. Por tanto, unos segundos más tarde o incluso menos (con buena conectividad) el mensaje de salida indicaría el fraude al usuario.

Gracias a este procedimiento de realización de una comprobación de alta seguridad en el servidor, la seguridad no se debilita almacenando parte de la información (por ejemplo, la primera clave K1) para generar claves de signatura en el dispositivo móvil. Además, este procedimiento no influye en la experiencia del usuario ya que recibe una respuesta inmediata (al menos en el caso en que el patrón visible es auténtico), y en caso de anomalía esta respuesta puede corregirse rápidamente (con buena conectividad). Si no existe conectividad, el usuario recibirá advertencias, si fuera el caso, en cuanto que el dispositivo móvil 20 vuelva a conectarse al servidor remoto 30.

En un aspecto de la invención, un procedimiento de autenticación un código de barras 2D que usa un dispositivo local comprende las etapas de: escaneo de dicho código de barras 2D usando el dispositivo local para generar al menos una trama de imagen, lectura de la información primaria de la trama de imagen en dicho dispositivo local, extracción de la información secundaria de la trama de imagen en dicho dispositivo local, generación de una parte de información secundaria usando una clave almacenada en el dispositivo local, comprendiendo dicha parte o

formando una signatura de la información secundaria, y comparación de dicha signatura de la información secundaria con la información secundaria extraída para verificar la autenticidad en un primer nivel local del código de barras 2D.

El procedimiento puede comprender además el envío de la información primaria o de una información correlacionada con la misma, y de una imagen de la información secundaria extraída, a un servidor remoto, y autenticación del código de barras 2D en un segundo nivel comparando la imagen de la información secundaria extraída con una imagen de código de barras 2D original almacenada o generada en el servidor remoto.

La comparación de dicha signatura de la información secundaria fuente con la información secundaria extraída puede generar ventajosamente una puntuación.

En una realización del procedimiento de autenticación, el escaneo de dicho código de barras 2D usando el dispositivo local genera una pluralidad de tramas de imágenes, para producir una pluralidad de puntuaciones, de manera que dicha pluralidad de puntuaciones se usa para determinar si debe realizarse una autenticación de segundo nivel por medio de un servidor remoto.

En una realización, el procedimiento de autenticación puede comprender la verificación de calidad de imagen de la al menos una trama de imagen para determinar si dicha imagen es adecuada para la autenticación del código de barras 2D por medio de un servidor remoto.

Una técnica para verificar la calidad de imagen, según una realización, incluye la extracción de la información secundaria de la trama de imagen en dicho dispositivo local, la generación de una parte de información secundaria usando una clave almacenada en el dispositivo local, comprendiendo dicha parte o formando una signatura de la información secundaria, la comparación de dicha signatura de la información secundaria con la información secundaria extraída para generar una puntuación y el uso de un conjunto de puntuaciones como un indicador de calidad de la imagen.

En otra realización, una técnica para verificar la calidad de imagen incluye la medida de la nitidez de transición entre las celdas de información primaria negras y blancas.

En referencia a la figura 8, una realización de ejemplo de un procedimiento de autenticación según la invención puede comprender las etapas siguientes:

Etapa 8-1: Vaciar memoria de dispositivo móvil de huellas digitales almacenadas (información secundaria) y puntuaciones;

Etapa 8-2: Extraer imagen de mapa de bits de la transmisión de vídeo;

Etapa 8-3: Decodificar código 2D en imagen. Si la decodificación no se realiza con éxito se volverá a la etapa 8-1 (mensaje = nulo), en caso contrario se recibirá un mensaje y datos de posicionamiento de código en la imagen (por ejemplo, esquinas de código de barras 2D, o posición de patrones de detección) y se avanzará a la etapa siguiente 8-4;

Etapa 8-4: Verificar (en el teléfono móvil) la signatura del mensaje (la signatura del mensaje puede ser un fragmento de parte del contenido del mensaje que debería corresponderse con otra parte del contenido del mensaje). Si la signatura del mensaje no se verifica, se enviará al usuario el mensaje "No es un código de barras 2D con información secundaria legible" con un botón que propone realizar otro escaneo. Después de que el usuario pulse el botón se retrocederá a la etapa 8-1. Si se verifica el mensaje, se avanzará a la etapa siguiente 8-5;

Etapa 8-5: Extraer parámetros del mensaje, incluido el umbral de calidad de imagen, la clave secreta o el índice de clave secreta almacenados en el dispositivo móvil para verificación local y medida de calidad, tamaño del código 2D, ID único del código y otros parámetros requeridos para verificación;

Etapa 8-6: Si el tamaño del código 2D está disponible en los parámetros (o puede asumirse de otro modo el tamaño esperado por defecto), comparar con el tamaño esperado como un porcentaje del tamaño de la imagen. Si el tamaño de la imagen escaneada es demasiado pequeño se devolverá al usuario el mensaje "Acérquese al código 2D" (alternativamente "Aléjese del código 2D") y vuelva a la etapa 8-1 (véase más adelante, por ejemplo, el algoritmo para medir el tamaño);

Etapa 8-7: Verificar si la imagen aparece suficientemente nítida para poder usarla para autenticación, ejecutando un algoritmo de medida de nitidez de la imagen (véase más adelante, por ejemplo, el algoritmo). Si el valor está por encima del umbral, se avanzará a la etapa siguiente. En caso contrario, como opción se mostrará al usuario el mensaje "Toque la pantalla para autoenfoque", y se pasará a la etapa 8-1;

Etapa 8-8: A partir de la imagen escaneada y los datos de posicionamiento del código 2D, extraer el área de la

imagen de huella digital (información secundaria). La imagen extraída puede ser simplemente una recopilación, o una imagen transformada para corregir la transformada de perspectiva y a un tamaño adecuado para la autenticación;

Etapa 8-9: Con la clave secreta, generar la parte de huella digital fuente (información secundaria);

Etapa 8-10: Medir la semejanza de imágenes entre la parte de huella digital fuente generada y el área de la huella digital extraída, para obtener la puntuación;

Etapa 8-11: Almacenar en memoria la huella digital extraída y la puntuación;

Etapa 8-12: Si se cumple la condición C (véase más adelante) O se cumple la condición D, entonces

Etapa 8-13: Enviar la huella digital con la máxima puntuación al servidor (alternativamente enviar todas las huellas digitales), y la información útil para autenticación incluyendo el mensaje del código de barras 2D, el tamaño estimado del código de barras (que puede tenerse en cuenta para la autenticación). En caso contrario se volverá a la etapa 8-2;

Etapa 8-14: Esperar hasta que se reciba el resultado de autenticación del servidor y mostrar el resultado de autenticación recibido.

En el Servidor, en la etapa 15:

• Se recibe el mensaje del código de barras 2D, o alternativamente el código ID, una o varias huellas digitales escaneadas y sus puntuaciones asociadas

• Se recuperan los datos de autenticación del ID del código (parámetros de comparación, escaneos anteriores, huella digital fuente)

• Se comparan una o más huellas digitales escaneadas con la huella digital fuente y se usan los parámetros de comparación para tomar una decisión sobre la autenticidad

• Se devuelve el resultado de la autenticación

Condiciones C y D:

• Ejemplo de la Condición C: Al menos 3 tramas de imagen consecutivas con puntuación por encima del umbral de calidad; alternativamente 3 tramas de las últimas 5 con puntuación por encima del umbral de calidad; alternativamente todas las tramas en el último segundo con puntuación por encima del umbral de calidad

• Ejemplo de la Condición D: Al menos 6 tramas de imagen consecutivas con puntuación por debajo de umbral; alternativamente todas las tramas en los últimos 2 segundos con puntuación por debajo del umbral pero la diferencia de puntuación entre las puntuaciones mínima y máxima obtenidas en todas las tramas está por debajo de un segundo valor umbral

Ejemplo de medida del tamaño de imagen:

La pantalla tiene una anchura de 1.080 píxeles, y para un factor de zoom de valor 25, definido en el dispositivo móvil, se ha medido que un código de 1 cm de anchura ocuparía aproximadamente hasta el 60 % de la pantalla para ser leído de forma óptima (en el sentido de que tiene la puntuación máxima). Por debajo del 50 % del tamaño de la pantalla, se pierde una información secundaria importante que hace menos fiable la autenticación. Por encima del 70 %, el código de barras 2D está demasiado cerca y el dispositivo no es capaz de enfocarlo.

El tamaño de píxel objeto es por tanto 648 píxeles para un código de 1 cm, y el tamaño debería estar entre 540 y 756 píxeles.

Si el tamaño del código de barras 2D almacenado en los parámetros es diferente de 1 cm, estos valores pueden adaptarse fácilmente.

Ejemplo de algoritmo de medida de la nitidez de la imagen:

El código de barras 2D está compuesto por zonas alternas negras y blancas con una transición nítida. Si la imagen no está enfocada, la transición tenderá a ser menos nítida, y ocupará un número mayor de píxeles en las imágenes. Existen muchas formas de medir la nitidez de transición. Una forma preferida consiste en lo siguiente:

• Para cada celda en la imagen escaneada excluida el área de información secundaria, determinar si la celda era

originalmente negra o blanca (esto puede hacerse a partir del código de barras 2D recodificado o se realiza generalmente durante el proceso de decodificación del código de barras 2D).

• Determinar el valor de referencia que es el mínimo valor en la escala de grises para las celdas negras, alternativamente el máximo valor en la escala de grises para las celdas blancas

• Determinar el umbral de aceptación, que puede ser por ejemplo el valor 30 en la escala de grises desde el valor de referencia

• Determinar las regiones de transición. Existe un máximo de 4 regiones de transición por celda, dependiendo de si las celdas están arriba, a la izquierda, a la derecha, abajo o son del mismo color o no. La región de transición está compuesta normalmente por del 10 al 20 % de píxeles en el lado de la celda que está más cerca de la celda siguiente de diferente color.

• Determinar la proporción de píxeles que están por encima, respectivamente por debajo, del umbral de aceptación (para celdas negras, respectivamente celdas blancas) en la transición; esto se realiza para todas las regiones de transición en el escaneo

• Si la proporción total de píxeles en la región de transición está por encima de un umbral (que puede ajustarse en el dispositivo móvil y/o en las especificidades de impresión del código de barras 2D), entonces se considera que la imagen no está enfocada y por tanto no es adecuada para autenticación.

En referencia a las Figuras 9 y 10a, 10b, que muestran un ejemplo de un código de barras 2D según una realización de la invención, la información secundaria que forma el patrón visible 120 puede ser un conjunto aleatorio de valores de píxeles binarios, en los que cualquier píxel puede tener cierta probabilidad por defecto (el 30, el 40, el 50 %, etc.) de ser negro o blanco. Una parte del patrón se verifica de forma remota, en un servidor en el que es posible almacenar los valores de píxeles, y/o el medio para regenerarlos. Otra parte del patrón puede verificarse localmente por ejemplo en un teléfono móvil, y se genera preferentemente con un conjunto limitado de claves criptográficas usando por ejemplo un algoritmo criptográfico estándar.

Al contrario de los códigos de barras 2D convencionales, los códigos de barras 2D según las realizaciones de la invención tienen información de identificación que puede ser autenticada usando el patrón de autenticación visible de la información secundaria. En códigos de barras convencionales con un segundo código de barras menor integrado en un código de barras primario tal como se describe en el documento US-2012/0.256.000, la decodificación del código de barras menor no proporciona una prueba de autenticidad. Además, si el segundo código de barras menor es ilegible, se obtiene la situación ambigua en la que la información podría ser ilegible de hecho porque ha sido copiada erróneamente o podría ser ilegible debido a otras diversas razones como, por ejemplo, cuestiones de implementación.

En realizaciones ventajosas, la información secundaria no contiene información distinta de la información de autenticación que permite autenticar el patrón visible. Esto permite recuperar la información de autenticación sin tener que recuperar otra información, de manera que la información de autenticación puede decodificarse con probabilidad máxima.

Como puede verse en las figuras 10a, 10b, el patrón visible 120 que comprende la información secundaria parece muy aleatorizado y caótico, lo que mejora la efectividad para discernir los originales de las copias de originales. La Fig. 10b muestra una representación del patrón visible 120 de información secundaria antes de la impresión, estando la anchura del patrón visible 120 por ejemplo en el orden de 2 mm a 4 mm. La Fig. 11a muestra el patrón visible 120a de información secundaria después de la impresión, con lo que la Figura 11a representa por tanto una primera impresión original. Como puede verse en la figura 11a el patrón visible 120a del primer original ya se ha alterado pero conserva parte de su aspecto original. La Figura 11b representa una copia 120b, hecha por ejemplo con un escáner de alta resolución, seguido por procesamiento de la imagen y después la reimpresión en la misma impresora y papel. Sin embargo, la copia 120b en la Figura 11b es significativamente diferente del archivo original y a partir de la primera impresión original, y puede detectarse la alteración.

Números de referencia usados en las figuras

10 Documento
20 Dispositivo móvil
30 Servidor remoto
100 Código de barras 2D
102 Celda elemental
110 Patrón de información primaria
121 Borde de información secundaria
120 Patrón visible con información secundaria
120a Primera parte de patrón visible con primera densidad de negro media baja

120b Segunda parte de patrón visible segunda densidad de negro media alta
120c Tercera parte que forma la frontera de patrón visible
122 Subcelda elemental
130 Patrón de detección de posición
132 Área de datos
200 Código de barras 2D (segunda realización)
210 Patrón de información primaria
220 Patrón visible con información secundaria con densidad de negro media intermedia
232 Área de datos
300 Código de barras 2D (tercera realización)
310 Patrón de información primaria
320 Patrón visible con información secundaria con densidad de negro media intermedia
320a Primera parte cuadrada de patrón visible con primera densidad de negro media baja
320b Segunda parte de patrón visible con segunda densidad de negro media alta
$320b_{1-}$ Subparte cuadrada de la segunda parte
$320b_4$ 332 Área de datos
400 Código de barras 2D (cuarta realización)
400' Código de barras 2D escaneo (imagen)
410 Patrón de información primaria
420 Patrón visible con información secundaria con densidad de negro media alta
424 Zona de signatura
426 Zonas de parte secreta
426a Primera parte de datos de zonas de parte secreta
426b Segunda parte de datos de zonas de parte secreta
432 Área de datos
500 Código de barras 2D (quinta realización)
510 Patrón de información primaria
520 Patrón visible con información secundaria con densidad de negro media intermedia
520_1 Primera parte de patrón visible con densidad de negro media
520_2 Segunda parte de patrón visible con densidad de negro media
532 Área de datos
600 Código de barras 2D (sexta realización)
610 Patrón de información primaria
620 Patrón visible con información secundaria con densidad de negro media intermedia
632 Área de datos

REIVINDICACIONES

1. Un procedimiento para crear un código de barras 2D (100; 200; 300; 400; 500; 600), que comprende:

- la integración de información primaria que puede ser leída por un lector de código de barras 2D en un patrón de información primaria (110; 210; 310; 410; 510; 610),
- la integración de información secundaria en un patrón visible (120; 220; 320; 420; 520; 620) integrado en dicho código de barras en al menos un área que no contenga ninguna información primaria de manera que la información secundaria esté separada de la información primaria, en el que dicha información secundaria en un patrón visible está formada por subceldas elementales claras y oscuras que tienen una dimensión máxima menor que 50 μm configuradas de manera que sean difíciles de reproducir sin alteración, y en el que la información secundaria se genera usando una clave secreta de manera que el patrón visible contiene una parte secreta (426).

2. Procedimiento según la reivindicación 1, en el que dicho patrón visible (120; 220; 320; 420) está integrado en dicho código de barras en una sola área.

3. Procedimiento según una cualquiera de las reivindicaciones 1 o 2, en el que dicha información secundaria está formada por subceldas elementales negras y blancas (122) y tiene una densidad de negro media diferente del 50 % ± 5 % de las subceldas elementales negras (122).

4. Procedimiento según la reivindicación 3, en el que dicha densidad de negro media es menor o igual que el 45 % o mayor o igual que el 55 % de subceldas elementales negras (122), preferentemente menor o igual que el 40 % o mayor o igual que el 60 % de subceldas elementales negras (122), preferentemente menor o igual que el 30 % o mayor o igual que el 70 % de subceldas elementales negras (122).

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que dicho patrón visible (420) contiene una signatura (424) que puede ser verificada localmente por un dispositivo conectado con el lector de código de barras para comprobar la autenticidad del código de barras (400).

6. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que dicha clave secreta (K2) se genera de forma aleatoria o pseudoaleatoria.

7. Producto que integra un código de barras 2D (100; 200; 300; 400; 500; 600) que comprende un patrón de información primaria (110; 210; 310; 410; 510; 610) que representa información primaria que puede ser leída por un lector de código de barras 2D y un patrón visible (120; 220; 320; 420; 520; 620) que representa información secundaria que es difícil de reproducir sin alteración, **caracterizado porque** dicho patrón visible (120; 220; 320; 420; 520; 620) está integrado en dicho código de barras en al menos un área que no contiene ninguna información primaria, teniendo dicho patrón visible formado por subceldas elementales claras y oscuras una dimensión máxima menor que 50 μm generada usando una clave secreta.

8. Producto que integra un código de barras 2D (100; 200; 300; 400; 500; 600) según la reivindicación 7, en el que dicho código de barras 2D incluye un código QR o Datamatrix modificado en forma de un símbolo que forma un área de datos que comprende patrones de detección de posición situados en tres esquinas de dicho símbolo.

9. Producto que integra un código de barras 2D según la reivindicación 7 u 8, en el que dicho patrón visible está totalmente contenido en un rectángulo con solo información secundaria.

10. Producto que integra un código de barras 2D según la reivindicación 7 u 8, en el que dicho patrón visible está situado dentro del límite de dicho patrón de información primaria y recubre el centro de dicho patrón de información primaria, o dicho patrón visible (520; 620) está situado fuera del límite de dicho patrón de información primaria.

11. Producto que integra un código de barras 2D según cualquiera de las reivindicaciones 7 a 10, en el que dicha clave secreta (K2) se genera de forma aleatoria o pseudoaleatoria.

12. Procedimiento de autenticación de un código de barras 2D en un producto según cualquiera de las reivindicaciones 7 a 11, que comprende:

- la lectura con un lector de código de barras 2D de dicho código de barras 2D,
- la identificación de dicho patrón visible y la identificación en dicha información secundaria de dicha signatura formando de este modo una signatura detectada,
- la comparación de dicha signatura detectada con una clave de signatura y la determinación en consecuencia de la comparación de una puntuación de semejanza de signatura
- la comparación de dicha puntuación de semejanza de signatura con un umbral de signatura predeterminado,
- el establecimiento de un resultado de signatura de autenticación como exitoso si dicho resultado es igual o mayor

que dicho umbral de signatura predeterminado o como fallido si dicho resultado es menor que dicho umbral de signatura predeterminado.

13. Procedimiento de autenticación según la reivindicación anterior, en el que dicho lector de código de barras 2D forma parte de un dispositivo móvil (20), en particular un teléfono inteligente, y en el que dicha clave de signatura está almacenada en dicho dispositivo móvil (20) que implementa la etapa de comparación entre dicha signatura detectada y dicha clave de signatura.

14. Procedimiento de autenticación de un código de barras 2D en un producto según cualquiera de las reivindicaciones 7 a 11, que comprende

- la lectura con un lector de código de barras 2D de dicho código de barras 2D,
- la identificación de dicho patrón visible y la identificación en dicha información secundaria de una parte secreta formando de este modo una parte secreta detectada,
- la comparación de dicha parte secreta detectada con una clave secreta de un código de barras 2D fuente y la determinación en consecuencia de la comparación como una puntuación de semejanza de parte secreta,
- la comparación de dicha puntuación de semejanza de parte secreta con un umbral de parte secreta predeterminado,
- el establecimiento de un resultado de parte secreta de autenticación como exitoso si dicho resultado es igual o mayor que dicho umbral de parte secreta predeterminado o como fallido si dicho resultado es menor que dicho umbral de parte secreta predeterminado.

15. Procedimiento de autenticación según una reivindicación anterior, en el que dicho lector de código de barras 2D es parte de un dispositivo móvil (20), en particular un teléfono inteligente, que está conectado con un dispositivo remoto (30), en el que dicha clave secreta de dicho código de barras 2D fuente está almacenada en dicho dispositivo remoto (30) que implementa la etapa de comparación entre dicha parte secreta detectada y dicha clave secreta, y en el que dicho procedimiento comprende además el reenvío de dicho resultado de parte secreta de autenticación a dicho dispositivo móvil (20).

16. Procedimiento de autenticación de un código de barras 2D que comprende las características de un código de barras 2D creado según el procedimiento de la reivindicación 1, que comprende: el escaneo de dicho código de barras 2D usando un dispositivo local para generar al menos una trama de imagen, la lectura a partir de la información primaria de la trama de imagen en dicho dispositivo local, la extracción a partir de la información secundaria de la trama de imagen en dicho dispositivo local, la generación de una parte de información secundaria usando una clave almacenada en el dispositivo local, comprendiendo o formando dicha parte una signatura de la información secundaria, la comparación de dicha signatura de la información secundaria con la información secundaria extraída para verificar la autenticidad en un primer nivel local del código de barras 2D en el que la comparación de dicha signatura de la información secundaria fuente con la información secundaria extraída genera una puntuación.

17. Procedimiento según la reivindicación anterior, que comprende además el envío de la información primaria o de una información correlacionada con ella, y una imagen de la información secundaria extraída, a un servidor remoto, y la autenticación del código de barras 2D comparando la imagen de la información secundaria extraída con una imagen de código de barras 2D original almacenada o generada en el servidor remoto.

18. Procedimiento según una cualquiera de las dos reivindicaciones directamente anteriores, en el que dicho escaneo de dicho código de barras 2D usando el dispositivo local genera una pluralidad de tramas de imágenes, que producen una pluralidad de puntuaciones, usándose dicha pluralidad de puntuaciones para determinar si debe realizarse una autenticación de segundo nivel por medio de un servidor remoto.

19. Procedimiento según una cualquiera de las tres reivindicaciones directamente anteriores que comprende la verificación de la calidad de imagen de la al menos una trama de imagen para determinar si dicha imagen es adecuada para autenticación del código de barras 2D por medio de un servidor remoto.

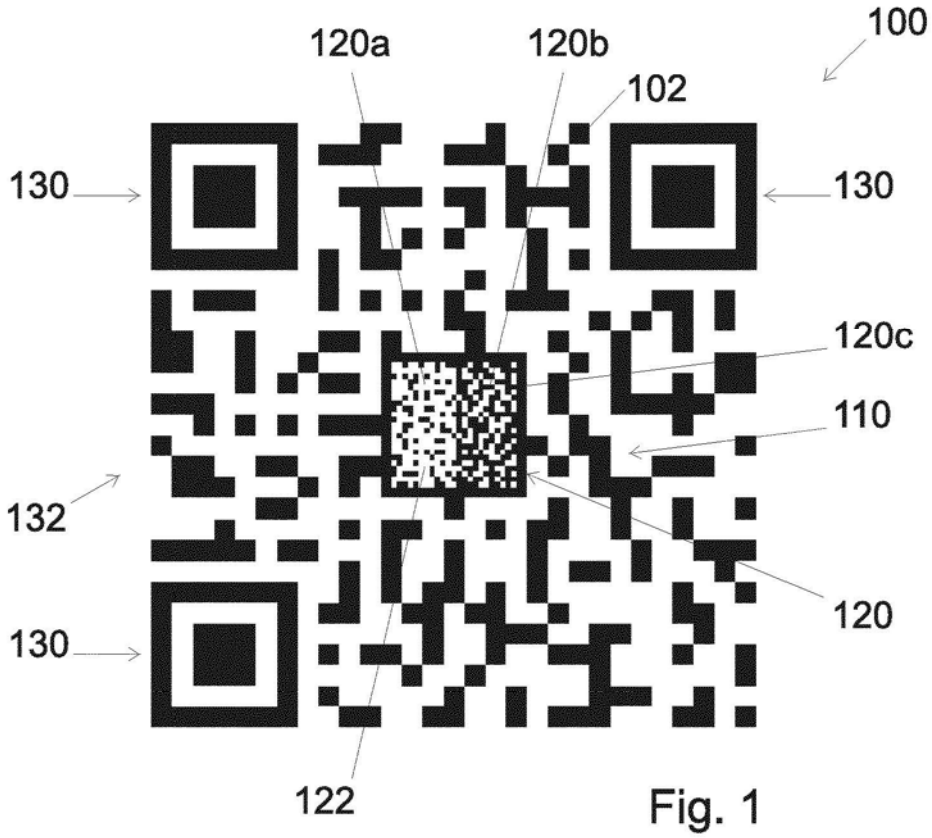

100
120a
120b
102
130
130
120c
110
132
120
130
122

Fig. 1

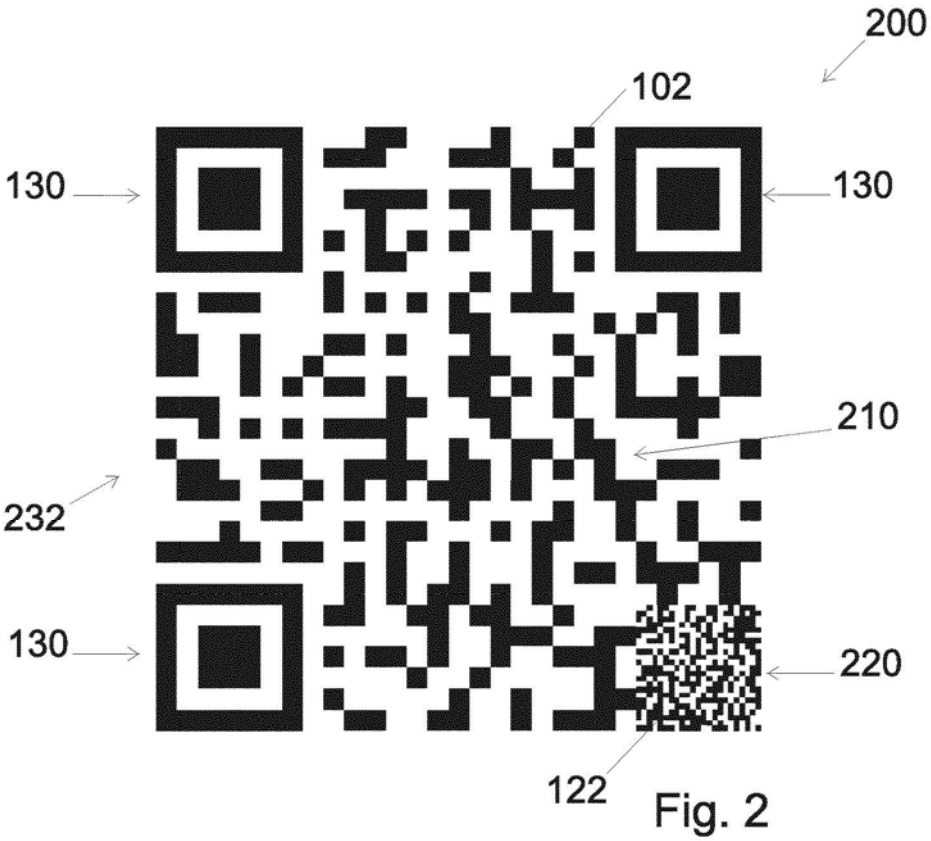

200
102
130
130
210
232
130
220
122

Fig. 2

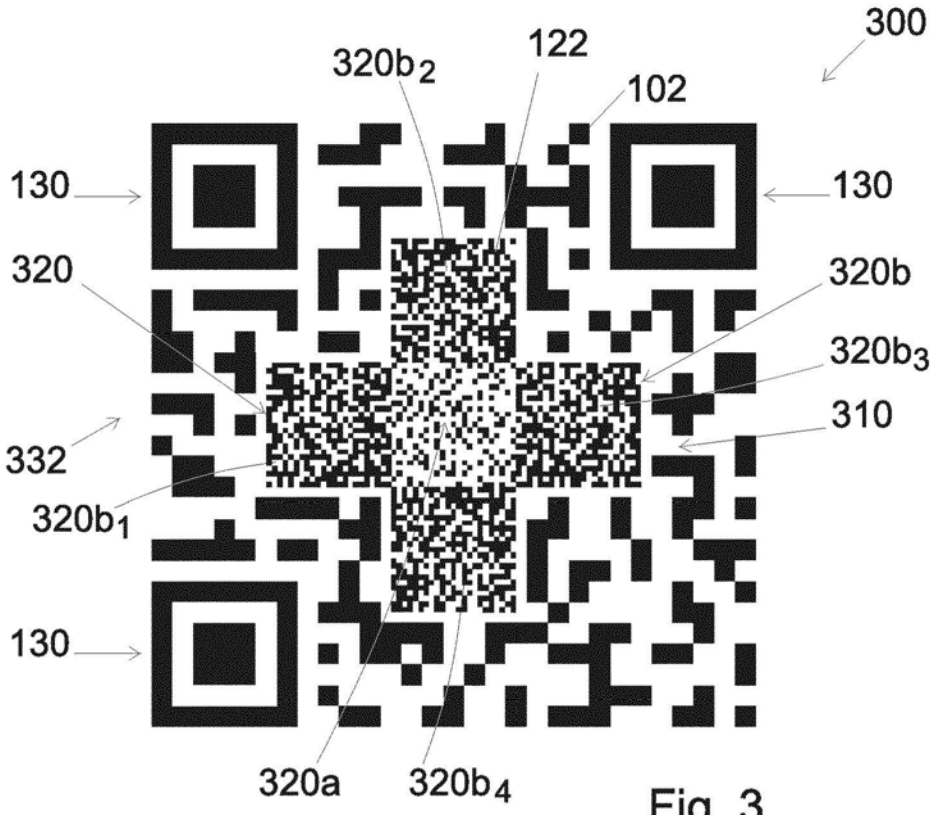

300
320b2
122
102
130
130
320
320b
320b3
310
332
320b1
130
320a
320b4

Fig. 3

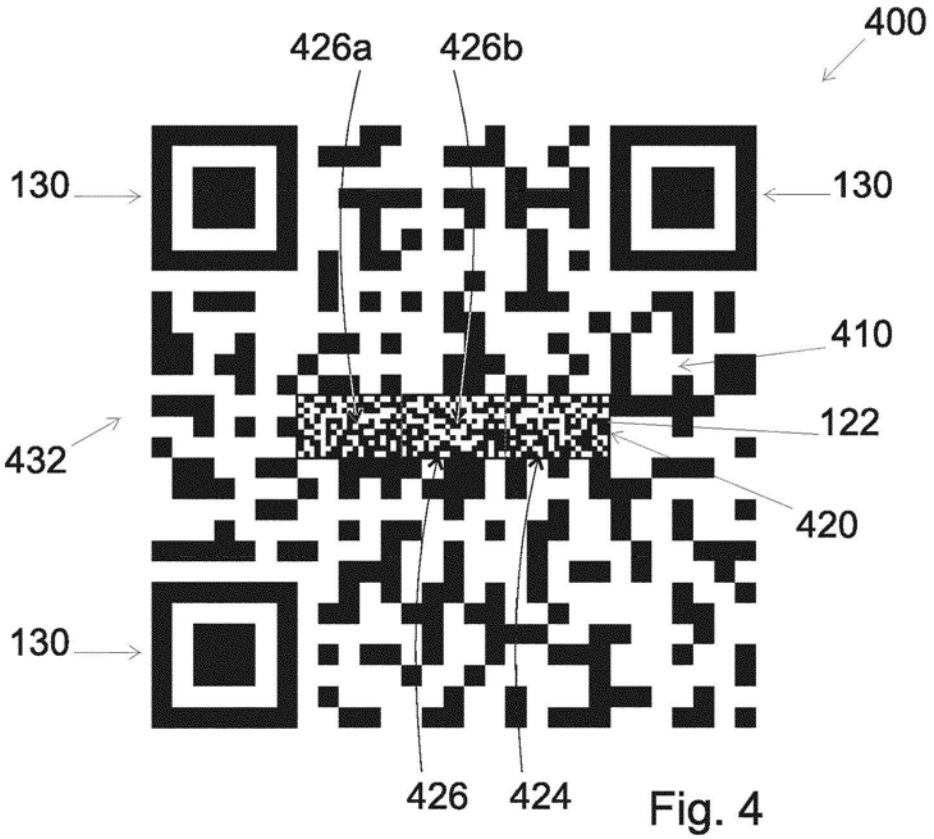

400
426a
426b
130
130
410
122
432
420
130
426
424

Fig. 4

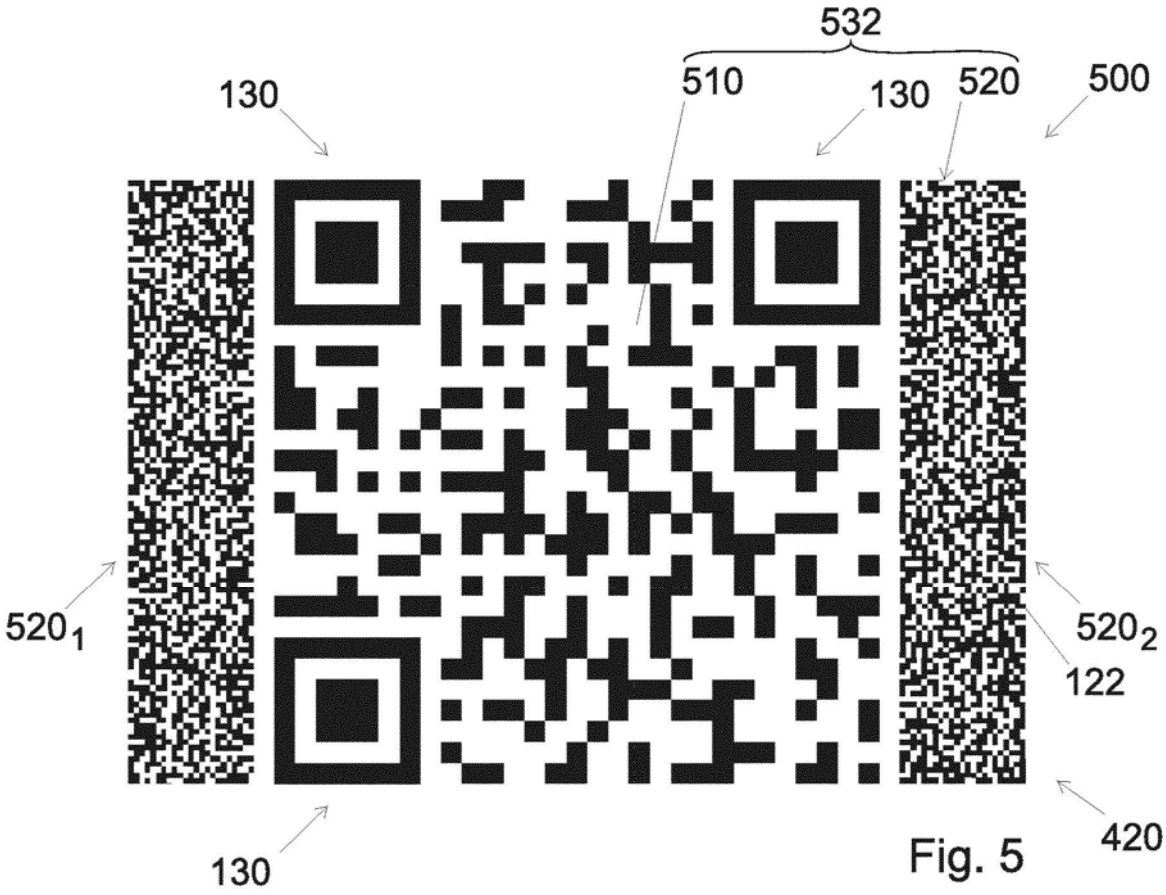

532
510
130
520
500
130
520_1
520_2
122
420
130

Fig. 5

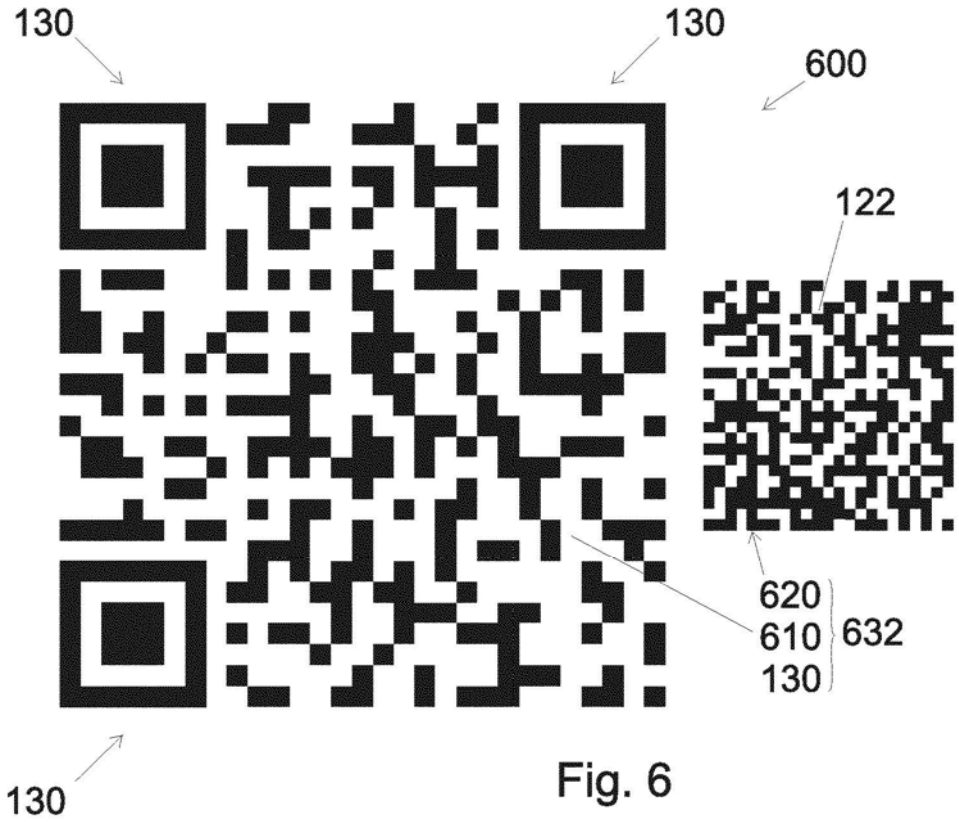

130
130
600
122
620
610
130
632
130

Fig. 6

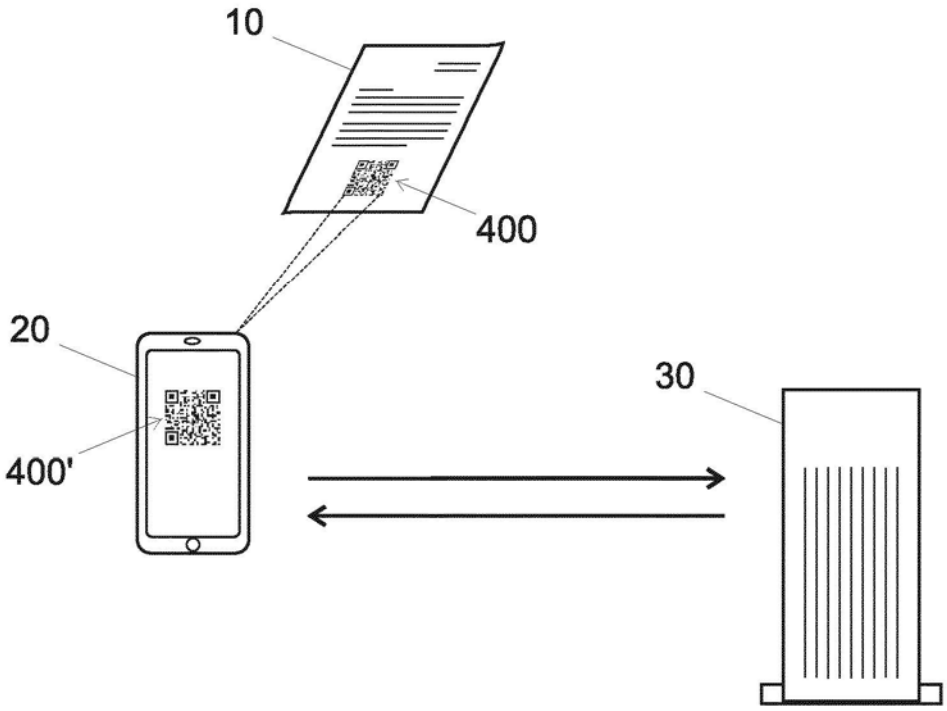
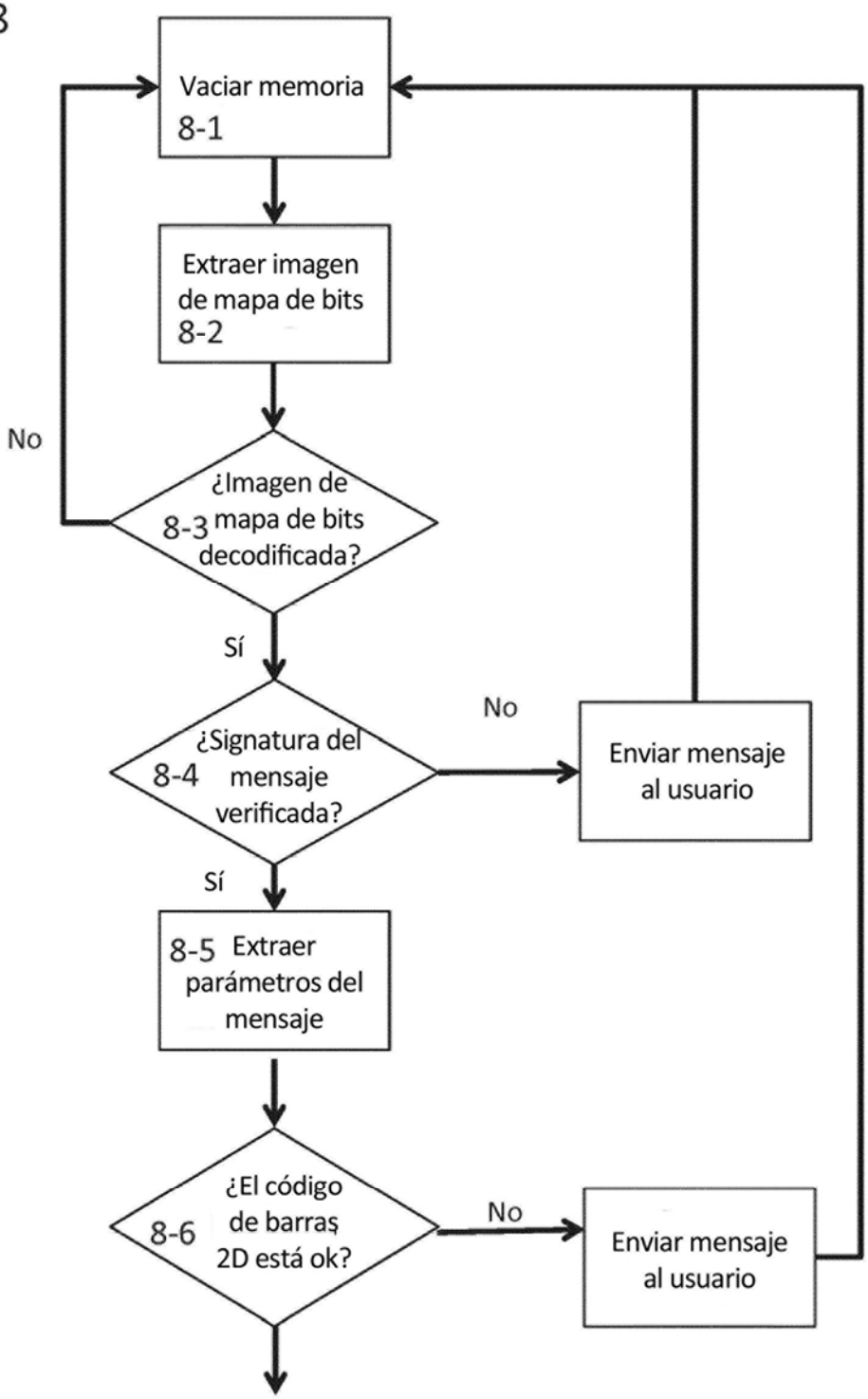


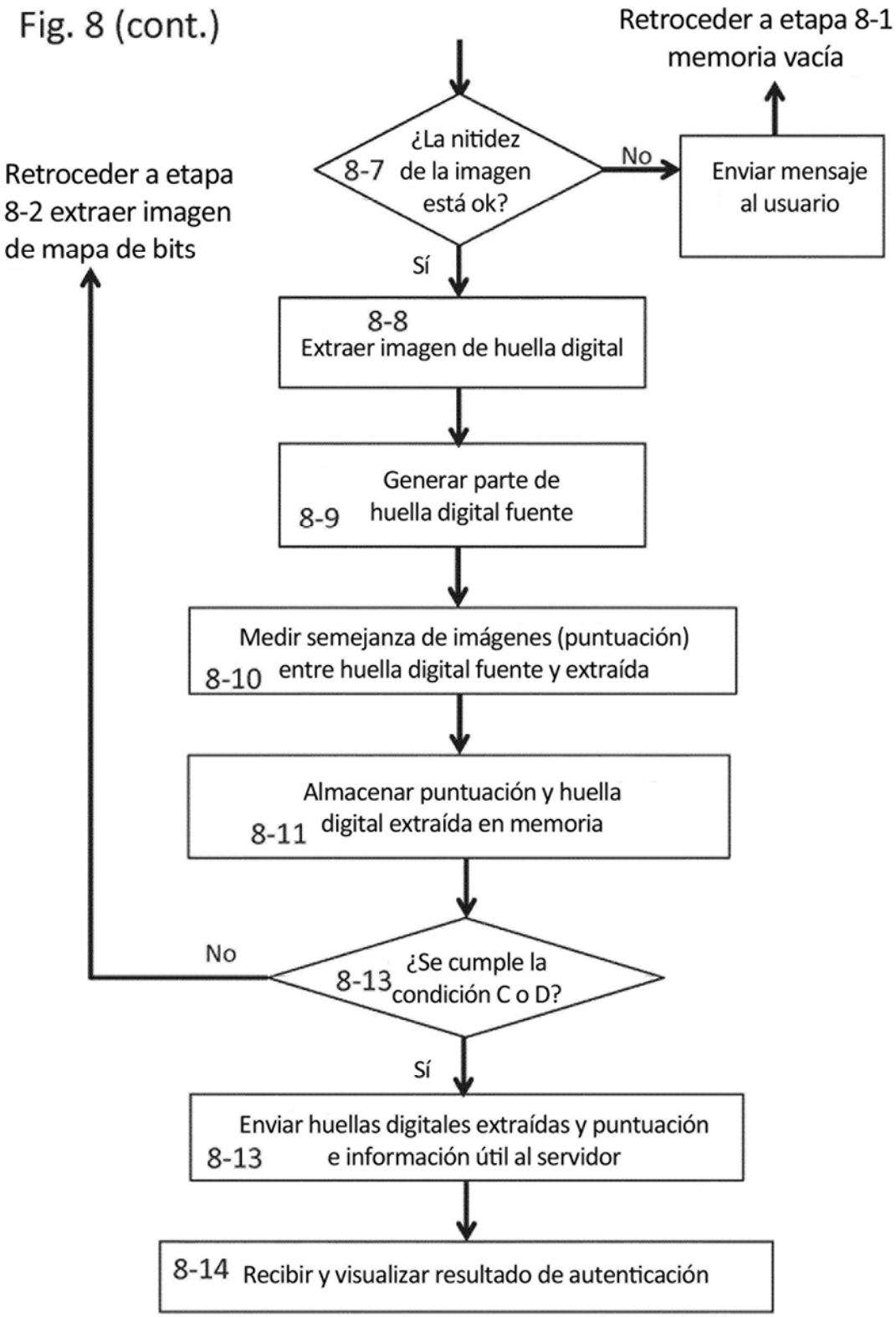
Fig. 7

Fig. 8



Continúa en página siguiente

Fig. 8 (cont.)


Retroceder a etapa 8-1
memoria vacía
¿La nitidez
8-7 de la imagen
está ok?
No
Enviar mensaje
al usuario
Retroceder a etapa
8-2 extraer imagen
de mapa de bits
Sí
8-8
Extraer imagen de huella digital
Generar parte de
8-9 huella digital fuente
Medir semejanza de imágenes (puntuación)
8-10 entre huella digital fuente y extraída
Almacenar puntuación y huella
8-11 digital extraída en memoria
No
¿Se cumple la
8-13 condición C o D?
Sí
Enviar huellas digitales extraídas y puntuación
8-13 e información útil al servidor
8-14 Recibir y visualizar resultado de autenticación

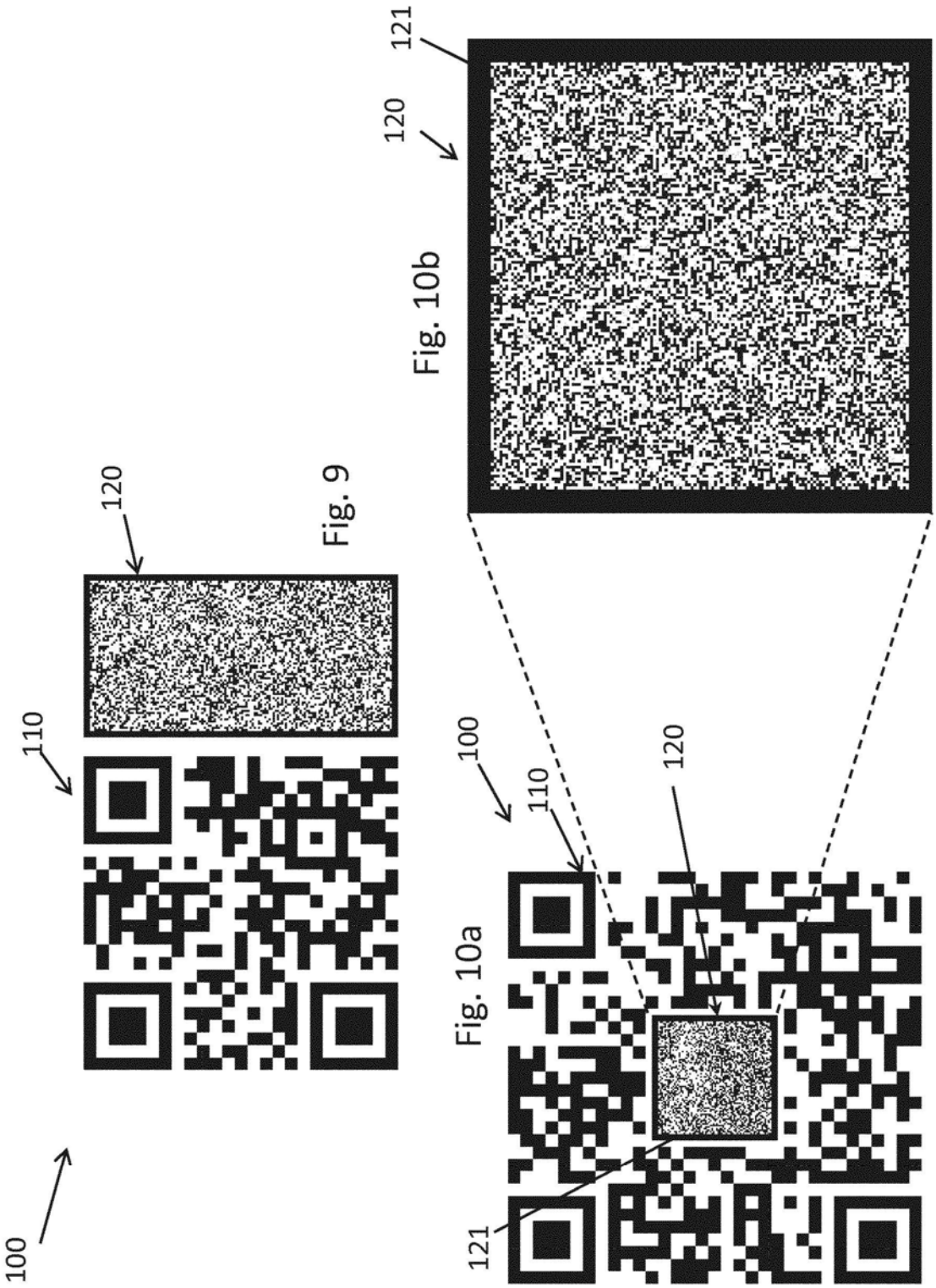
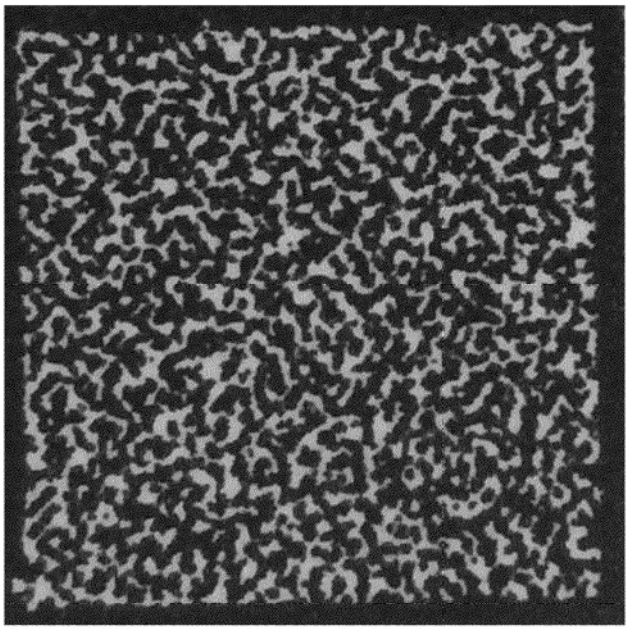


Fig. 10b

Fig. 9

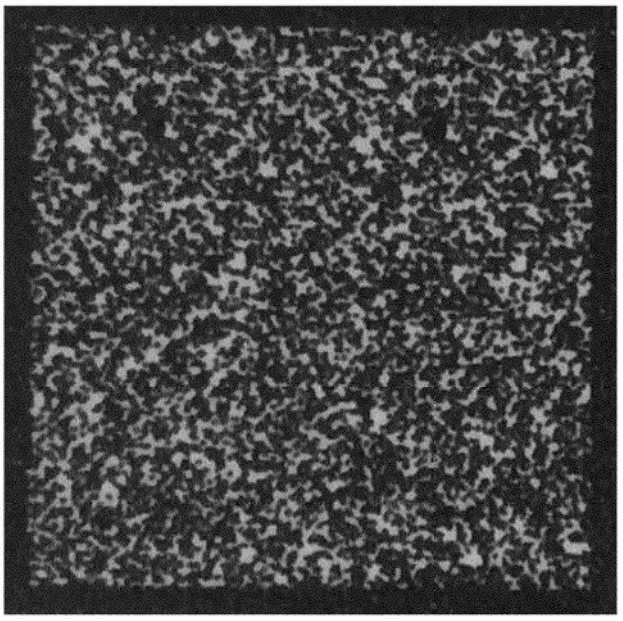
Fig. 10a

Fig. 11b



120b

Fig. 11a



120a