(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 399**

(51) Int. CI.:

H04N 1/32 (2006.01)
G07D 7/00 (2006.01)
G07D 7/20 (2006.01)
G07D 7/202 (2006.01)
G07D 7/005 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.02.2013 PCT/IB2013/051260**

(87) Fecha y número de publicación internacional: **22.08.2013 WO13121401**

(96) Fecha de presentación y número de la solicitud europea: **15.02.2013 E 13721389 (8)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 2815567**

(54) Título: **Elemento de seguridad y método para inspeccionar la autenticidad de una impresión**

(30) Prioridad:

15.02.2012 HU P1200097

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2020

(73) Titular/es:

GLENISYS KFT. (100.0%)
Fészek u. 3.
1125 Budapest, HU

(72) Inventor/es:

BIRÓ, ATTILA y
KRISTÓ, GÁBOR

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Elemento de seguridad y método para inspeccionar la autenticidad de una impresión

La presente invención se refiere a un elemento de seguridad, así como a un método para determinar la autenticidad de una impresión dispuesta en un sustrato de impresión. Su campo de aplicación cae en el campo de la protección de los materiales impresos producidos por máquinas de impresión o documentos generados con impresoras de inyección de tinta y/o impresoras láser contra la falsificación.

Por el momento, las tecnologías de fotocopiado e impresión láser han experimentado una enorme mejora. Como resultado, la reproducción de alta calidad de diversos materiales impresos se ha simplificado significativamente mediante el uso de estas técnicas. Al mismo tiempo, desafortunadamente, la falsificación de materiales impresos valiosos o personalizados también se ha vuelto más fácil. Por lo tanto, la protección de dichos documentos contra la falsificación ha pasado al primer plano. Cualquier documento provisto de un soporte de datos, tal como, por ejemplo, una escritura o un dibujo, producido mediante, por ejemplo, una máquina de impresión o una impresora de chorro de tinta y/o láser, puede constituir un material impreso que requiere protección. Tales materiales impresos son, por ejemplo, las diversas etiquetas de embalaje (por ejemplo, para medicamentos, cubiertas de CD), entradas valiosas, certificaciones, billetes de banco, cheques, identificadores personales, varios cupones, etc. solo para mencionar algunos ejemplos. Para evitar (o minimizar) malos usos, dichos materiales impresos generalmente están provistos de elementos de seguridad apropiados. En general, los elementos de seguridad aplicados y/o sus combinaciones son bastante complicados.

Existe una gran cantidad de soluciones en el campo de la protección de impresión. En una clase del mismo, el elemento de seguridad que proporciona protección está oculto en la propia imagen impresa. El Folleto de Solicitud de Patente Internacional n.º W099/35819 y la Solicitud de Patente de Estados Unidos n.º 1996/019310 divulgan soluciones basadas solo en este concepto. Según las soluciones enseñadas, una imagen secundaria no visible a simple vista, pero visible para un dispositivo de decodificación específico está oculta dentro de una imagen primaria que es visible a simple vista. Los parámetros físicos de las técnicas utilizadas para crear dicha imagen secundaria se pueden elegir de tal manera que la imagen secundaria simplemente desaparezca al copiar el sustrato (el documento) impreso con la imagen combinada. Es decir, esta información no se puede reconstruir a partir de una copia de la impresión. Para implementar las soluciones en cuestión, sin embargo, se requiere una máquina de impresión de alta precisión (con una resolución de al menos 8000 dpi), y para inspeccionar la autenticidad de la impresión, también se necesita una lente de decodificación. Debido a estas desventajas, la aplicación de dichas soluciones no se extendió/no pudo extenderse en la práctica diaria, donde, como consecuencia de los avances logrados en la impresión digital, debe protegerse la protección de los materiales impresos con impresiones producidas por máquinas en general con una resolución mucho menor (usualmente de 600 dpi).

El elemento de seguridad descrito en la Patente RU n.º 2.430.836 es un fuerte elemento de seguridad que puede inspeccionarse a simple vista y brinda una experiencia estética extraordinaria. Sin embargo, la aplicación del elemento de seguridad obtenido sobre un sustrato de impresión requiere el uso de una máquina de impresión específica (calcografía). Dichas máquinas de impresión suelen ser propiedad de impresoras de billetes y, por lo tanto, el acceso a dichas máquinas es bastante limitado.

En otra clase de protección de impresión, es la tinta de impresión utilizada para aplicar la impresión y/o el sustrato de impresión lo que se hace específico, y se intenta lograr la naturaleza no copiable de esta manera. Dichas soluciones se describen, por ejemplo, en las Patentes EP n.º 2.004.414; 1.858.605; 1.827.864 y 1.779.335. El mayor inconveniente de las soluciones en cuestión se debe a las tintas específicas y, por tanto, relativamente caras (por ejemplo, tintas de impresión con pigmentos ópticamente variables) o el uso de sustratos de impresión específicos que se pueden producir a costes relativamente altos, también.

En aún una clase adicional de protección de impresión, la impresión comprende uno o más identificadores que pueden asociar la impresión con una base de datos. La patente de Estados Unidos n.º 6.952.485 enseña una llamada marca de agua electrónica como el identificador. En este caso, un ruido incorporado en la imagen y no visible a simple vista lleva la información. La marca de agua electrónica se puede reconstruir a partir de la copia preparada mediante reproducción sin ningún cambio, es decir, la marca de agua electrónica siempre se transfiere copiando. Un campo de aplicación para dichas marcas de agua electrónicas es la protección de billetes de banco contra la copia. En particular, esta marca de agua electrónica se incluye en los billetes de Euro como elemento de seguridad. Esta marca de agua es reconocida por el controlador de cada máquina de impresión que se vende hoy en día, y luego simplemente se niega a imprimir la imagen que comprende la marca de agua electrónica. Un inconveniente de esta técnica radica en el hecho de que se requiere un amplio acuerdo entre los fabricantes de impresoras y escáneres en cuanto a la marca de agua electrónica utilizada para la protección de copias. Esto significa que este tipo de protección de impresión se puede utilizar simplemente en materiales impresos muy excepcionales. Asimismo, la marca de agua prohibida se debe "enseñar" a cada controlador de impresora/escáner. Otro inconveniente de esta técnica se origina justo de esta última: los dispositivos de impresión fabricados antes de que se haya hecho el acuerdo simplemente no reconocen la marca de agua prohibida y, por lo tanto, imprimen el material impreso protegido por dicha marca de agua.

De acuerdo con la solución divulgada en la Solicitud de Patente Internacional n.º PCT/EP2009/061073, un identificador primario visible y un elemento de imagen de interferencia aleatorio único (información secundaria) que no es visible a simple vista están dispuestos en un artículo a proteger durante la fabricación. Dicho identificador primario y el elemento de imagen, también conocido como información secundaria, se almacenan en una base de datos a través de Internet en forma digitalizada. Cuando se inspecciona la autenticidad de un artículo, basada en la información primaria, la imagen almacenada en la base de datos se busca y luego se compara con una foto del artículo inspeccionado tomada en el acto. Un inconveniente de la solución radica en que, para realizar la inspección, se requiere un acceso a la base de datos remota en cada caso que requiera la disponibilidad de una conexión de comunicación de datos con un ancho de banda apropiado.

En aún una clase adicional de protección de impresión, para inspeccionar la autenticidad de una impresión, se aprovecha la interferencia del dispositivo de impresión y el soporte de impresión durante la impresión. La Solicitud de Patente de EE. UU. n.º 2002/0037093 se refiere a una solución en la que una fotocopiadora o una impresora láser "ensucia" el sustrato de impresión (papel) que lo atraviesa al azar con tóner o micropuntos de tinta que no son visibles a simple vista cuando se prepara la copia. Es decir, analizando una imagen digital de alta definición de un documento, si se buscan tóner o micropuntos de tinta, particularmente en partes de dicho documento sin impresión, uno puede decidir inequívocamente si el documento se genera copiando o no. Un inconveniente de esta técnica radica en que, para realizar el estudio, se requiere un medio de digitalización de alta resolución.

La Solicitud de Patente Japonesa. n.º 2009/034921 A divulga un material impreso provisto de un medio antifalsificación que comprende una figura latente con diseño de líneas, que es una información secundaria. En al menos un borde lateral de cada línea que constituye dicha figura latente, se forma una pluralidad de regiones de proyección extendida cubiertas de tinta que sobresalen a lo largo de la dirección del ancho de la línea, bastante cerca entre sí. Cuando se copia dicho documento, los espacios entre las respectivas regiones de proyección extendida se entierran con tinta en armonía con las características de reproducción de la copiadora. En consecuencia, el ancho de línea de cada línea que constituye dicho patrón de línea se expande y prácticamente resulta en el "desarrollo"/apariencia de la imagen latente, así como de la información secundaria.

La patente FR n.º 2.962.828 A1 divulga un método de marcado de producto que comprende una etapa de formación, sobre o en dicho producto, de una marca robusta a copiar, con una primera resolución; una etapa de formación, sobre o en dicho producto, de una marca sensible a la copia, con una segunda resolución más alta que la primera resolución; una etapa para capturar una imagen de la marca robusta, la marca sensible y otra parte del producto; y una etapa de memorizar una pieza de información representativa de la imagen de la marca robusta, la marca sensible y la otra parte de la imagen. En este caso, la marca robusta para copiar es un código de barras bidimensional y la marca sensible a la copia es un código de autentificación digital. Además, para determinar dicha pieza de información, se aplica una transformada discreta de coseno.

La Patente de EE.UU. 5.189.292 divulga una etiqueta que lleva información codificada ópticamente con un conjunto bidimensional de celdas de datos que incluye un patrón de buscador que comprende una pluralidad de puntos dispuestos en un patrón geométrico predeterminado sustancialmente análogo al patrón geométrico predeterminado de dicho conjunto bidimensional de celdas de datos. El patrón del buscador se detecta escaneando primero el área de la imagen para detectar puntos. Las ubicaciones de los puntos detectados se comparan con la geometría conocida del patrón del buscador para proporcionar una búsqueda rápida y fiable del patrón del buscador y la etiqueta con información. Adicionalmente, los puntos de patrón del buscador detectados proporcionan información para decodificar la matriz de datos bidimensionales con el fin de compensar el aumento de la etiqueta, la inclinación y otras distorsiones.

La Solicitud de Patente de EE.UU. n.º 2009/059304 A1 describe cómo hacer imágenes de medios tonos en impresión de calcografía. El método comprende la generación de microestructura(s) estocástica(s) que se utiliza(n) para aumentar la representación de medios tonos. Como consecuencia de la aplicación de dicha(s) microestructura(s), la apariencia general de la imagen se modifica, es decir, un observador puede reconocer las modificaciones aplicadas por medio de, por ejemplo, medios de aumento apropiados.

La Solicitud de Patente de EE.UU. n.º 2009/046931 A1 divulga sistemas y métodos para segmentar una imagen en al menos dos capas, un primer plano y una capa de fondo, basados en escala de grises principalmente con el propósito de escanear.

Por el momento, códigos de barras, códigos de matrices de datos, varios códigos QR, códigos móviles y otros códigos similares (de ahora en adelante, códigos de puntos, en general) se han convertido en medios de transporte de información bien difundidos. Su popularidad se debe principalmente a la rápida propagación de los teléfonos móviles, especialmente de los teléfonos inteligentes. Su desventaja radica en el hecho de que, en general, no contienen protección contra copias y, por lo tanto, su aplicación como elementos de seguridad es muy limitada.

A la vista de lo anterior, es evidente que, aunque hay una pluralidad de tecnologías de protección de impresión disponibles para proteger las impresiones que estén equipadas con protección contra copias e impresión de sustratos/documentos que tengan tales impresiones, las tecnologías son demasiado caras o requieren un conjunto específico de dispositivos para su creación y/o inspección.

Es una demanda natural, sin embargo, que la autenticidad de un documento puede determinarse de manera simple y rápida por cualquier persona y esencialmente en cualquier lugar sin la necesidad de competencia adicional y equipos técnicos.

A la vista de lo anterior, un objeto principal de la presente invención es proporcionar un elemento de seguridad aplicado a un sustrato de impresión mediante impresión que, por una parte, contenga datos de identificación asociados con el propio material impreso como información primaria y, por otra parte, también proporcione una protección de copia fiable para el material impreso a través de información secundaria latente.

Un objeto adicional de la presente invención es proporcionar una técnica de protección de impresión, especialmente un método para inspeccionar/determinar la autenticidad de impresión que permita la verificación de autenticidad de un material impreso con un elemento de seguridad de acuerdo con la invención para cualquier persona y sin calificación en seguridad de la información de forma inmediata y en el acto por medio de dispositivos de al menos resolución media (es decir, de 300 a 1200 dpi) que están disponibles en el uso diario, tales como, por ejemplo, teléfonos móviles, tabletas, teléfonos inteligentes, cámaras web, etc.

Nuestros estudios nos llevaron a la conclusión de que un elemento de seguridad que logre el objeto de la invención puede lograrse combinando un código elegido adecuadamente que lleve información primaria con una pieza de información secundaria, en donde la información secundaria no se puede reconstruir a partir de la propia impresión (o sus copias), pero proporciona una característica inherente que se puede analizar mediante métodos estadísticos. Una estructura que transporta dicha información secundaria puede generarse en forma de áreas incorporadas (preferentemente por el fabricante) en el código que lleva información primaria de acuerdo con un concepto/algoritmo de codificación predefinido y no se imprime directamente. Debido a distorsiones/incertidumbres de impresión, tales como, por ejemplo, la deformación del sustrato de impresión y/o de la placa de impresión al ponerse en contacto entre sí o la inevitable humectación de la tinta de impresión aplicada sobre el sustrato de impresión, que surge cuando se ejecuta la impresión, las áreas que quedan fuera de la impresión directa se cubren más o menos con tinta. Según nuestros estudios, una condición para que dicha(s) área(s) excluida(s) sea(n) indetectable(s) a simple vista en la impresión del elemento de seguridad es que la dimensión más grande de dicha(s) área(s) excluida(s) dentro de la impresión en al menos una dirección sea de 2 a 40 micrómetros, dependiendo de la tecnología de impresión aplicada y de la calidad del sustrato de impresión. A pesar de que, debido a incertidumbres de impresión, la información secundaria en cuestión no será detectable a simple vista en la impresión del elemento de seguridad, ni su naturaleza ordenada es reconocible mediante una lupa (con un aumento de 2-20x), se descubrió que la incorporación de dicha información secundaria altera el valor en escala de grises de esa porción de la representación digital de la impresión en la que realmente se había incorporado. Al alterar el valor de la escala de grises, dicha información secundaria atribuye el elemento de seguridad inventivo con una característica inherente que puede analizarse mediante métodos estadísticos, en donde el resultado del análisis es característico del propio elemento de seguridad y, por lo tanto, puede usarse como un elemento de protección de copia para el elemento de seguridad, así como para el sustrato de impresión que tiene dicho elemento de seguridad.

El objetivo de proporcionar un método para inspeccionar la autenticidad de una impresión se logra mediante el método de acuerdo con la reivindicación 1. Otras variantes preferidas del método de la invención se exponen en las reivindicaciones 1 a 9.

El objeto destinado a la provisión de un aparato que implementa el método de la reivindicación 1 se consigue mediante el aparato de acuerdo con la reivindicación 10.

Las realizaciones o ejemplos de la siguiente descripción que no están cubiertos por las reivindicaciones adjuntas se proporcionan simplemente con fines ilustrativos.

A continuación, la invención se explica con más detalle con referencia a los dibujos adjuntos, en donde

- La figura 1A muestra el diagrama de bloques de un método para generar un elemento de seguridad de acuerdo con la invención y aplicarlo sobre un sustrato de impresión;
- La figura 1B ilustra el diagrama de bloques de un método de inspección de autenticidad basado en la aplicación de un elemento de seguridad de acuerdo con la invención;
- La figura 2 muestra esquemáticamente la forma de generar un código combinado, que constituye el elemento de seguridad, a partir de códigos que llevan información primaria y secundaria;
- La figura 3 muestra una parte del código combinado de la figura 2 en una vista ampliada;
- La figura 4 ilustra la descomposición de la porción de código combinado que se muestra en la figura 3 en clases en términos de la información secundaria, realizada junto con un concepto de codificación establecido por el fabricante;
- La figura 5 muestra una celda de código generalizada aplicable cuando la información secundaria se introduce en un código de punto;
- La figura 6 ilustra un par de posibles realizaciones preferidas del área(s) excluida(s) (píxeles) que representan información secundaria que es aplicable en un elemento de seguridad de acuerdo con la invención;

- La figura 7 muestra varios códigos de puntos ejemplares (visibles a simple vista) que llevan información primaria que tiene la dimensión más grande mayor de 50 micrómetros;
- La figura 8 ilustra la apariencia teórica (como se forma en una placa de impresión) y la apariencia real (como se ve después de haber impreso en un sustrato de impresión) de una porción del elemento de seguridad proporcionado por el código combinado; y
- Las figuras 9A y 9B ilustran un fragmento de información secundaria (latente) que tiene una dimensión de como máximo 50 micrómetros en al menos una dirección, oculto en un diseño a modo de punto y a modo de línea, respectivamente, antes y después de la impresión.

En la figura 1A se muestra un método general para generar un elemento de seguridad de acuerdo con la invención formado por un código combinado. De acuerdo con esto, se elige un código que lleva información (etapa 100) que está formado por un signo de código conocido (por ejemplo, un código de barras, un código QR, un código de matrices de datos, un código móvil) o un código de línea o punto codificado de forma única. Según todavía una posibilidad más, el código que lleva información primaria también puede estar formado por un código de línea o de punto oculto dentro de una ilustración gráfica ornamental de la impresión. Asimismo, el código que lleva información primaria puede ser la propia información primaria, impreso simplemente sobre el sustrato de impresión en una forma sin codificar. El sustrato de impresión puede ser cualquier documento o la superficie de un objeto a proteger; en particular, por ejemplo, billetes de banco, valores, facturas, embalajes de productos, tarjetas/etiquetas de identidad, cubiertas, entradas, certificados, documentos personales, cupones o cualquier otro documento similar. La información primaria significa una pieza de información que se relaciona con el documento a proteger, generalmente, los datos que identifican el propio documento. Es importante que el código que lleva información primaria se pueda segmentar, es decir, podría estar cubierto por una malla de celdas de tamaño determinado y típicamente de forma regular (en particular, una forma rectangular), opcionalmente girada con un ángulo dado en relación con el código que lleva información primaria. Debido al diseño constructivo, este último requisito se cumple automáticamente para los signos de código conocidos mencionados anteriormente.

Después de seleccionar el código que lleva información primaria, se genera un código que lleva información secundaria (etapa 110). Esta etapa se realiza en armonía con un concepto/algoritmo de codificación preestablecido de una manera discutida para un ejemplo específico a continuación con referencia a las figuras 2 a 4 con más detalle. En particular, la información secundaria es llevada por las áreas que quedan fuera de la impresión del código que lleva información primaria. Debido a su tamaño, el código que lleva información secundaria es una pieza de información latente, es decir, no es visible cuando se inspecciona a simple vista. Esta información secundaria ejemplar definida por las áreas excluidas se ilustra en las figuras 3 y 6. La información secundaria preferiblemente resulta de la información primaria, por ejemplo, de un elemento/datos de la misma.

Después de generar el código que lleva información secundaria, los códigos que llevan información primaria y secundaria se combinan juntos (etapa 120), como resultado de lo cual se obtiene un código combinado que corresponde al elemento de seguridad inventivo.

Finalmente, el material impreso con el elemento de seguridad se produce aplicando el elemento de seguridad así obtenido sobre el sustrato de impresión a través de la tecnología de impresión seleccionada (etapa 130).

El elemento de seguridad del material impreso producido por el método que se muestra en la figura 1A, por una parte, contiene datos que pueden usarse para identificar dicho material impreso (información primaria) y, por otra parte, es adecuado para proteger dicho material de impresión contra copias, dado que la información secundaria es una información latente que no es visible a simple vista y desaparece o se distorsiona de manera detectable cuando se imprime/copia.

Las figuras 2 a 4 ilustran las etapas de combinar juntos los códigos que llevan la primera y segunda información en un caso específico, en donde el código que lleva información primaria es proporcionado por un código de puntos (ver la figura 2) formado por puntos de tinta 20 y que representa una figura "0" impresa a la resolución de 600 dpi, en donde la segmentación se realiza por medio de una malla 30 de celdas de forma cuadrada 34 (véase la figura 3). En este caso, el tamaño de cada celda 34 es de al menos 300 micrómetros a lo largo de las direcciones X e Y. Se descubrió que el tamaño de 300 micrómetros es suficiente para garantizar que cada punto de tinta individual 20 caiga en una celda separada 34 y lejos de los bordes de dicha celda 34 (es decir, prácticamente a la mitad de la celda 34). Además, cada celda 34 se divide en siete por siete píxeles 40 (en este caso específico); los píxeles 40 que forman unidades de dicha división son los "bloques de construcción" para las áreas excluidas 32, 42 que codifican información secundaria. Para una persona experta en la materia, es evidente que la segmentación se puede realizar con diferentes tamaños de celda y/o con diferentes números de píxeles a lo largo de las direcciones X, Y por celdas para un tipo diferente de signo de código. En la figura 5 se muestra una malla rectangular común 50 y su celda (i, j)-ésima 52 aplicable para segmentar. También se señala aquí que, si se usa una resolución más alta, el número de píxeles a lo largo de cada una de las direcciones debe aumentarse proporcionalmente.

Habiendo segmentado el código que transporta información primaria, se realiza la introducción del código que lleva información secundaria. Con este fin, las celdas 34 del código que llevan información primaria obtenida por la segmentación y contienen un punto de tinta, se clasifican en varias clases. En este caso, el número de varias clases

se elige entre cuatro y seis, sin embargo, cualquier otro número de clases puede ser igualmente utilizado. Dado que después de imprimir el elemento de seguridad inventivo, la información secundaria conduce a una característica que puede analizarse mediante técnicas estadísticas, preferiblemente hay al menos diez celdas 34 en cada clase. Dicha clasificación puede tener lugar de manera regular o aleatoria, sin embargo, siempre resulta del código que lleva información primaria. En el presente ejemplo, la clasificación se realiza en términos del número de píxeles que forman el área excluida dentro de cada celda. En este caso, el número inscrito en una celda dada corresponde al tamaño del área excluida dentro de la celda, expresado en píxeles. El tamaño del área excluida cambia de una clase a otra de una manera estrictamente creciente. En consecuencia, por ejemplo, la primera clase permanece inalterada (es decir, no hay área excluida), la segunda clase tendrá un área excluida de un píxel, la tercera clase tendrá un área excluida de al menos dos píxeles, la cuarta clase tendrá un área excluida de al menos tres píxeles, y así sucesivamente.

El tamaño del área excluida en cada celda 34 depende de la tecnología de impresión que se aplicará: el tamaño/dimensión del área excluida siempre se elige de tal manera que la tecnología de impresión aplicada sea inadecuada para imprimir dicha área excluida rápidamente. En consecuencia, debido a la incertidumbre de impresión de las áreas excluidas, dichas áreas no serán visibles en absoluto en el elemento de seguridad impreso cuando se inspeccionen a simple vista. Además, la naturaleza ordenada de la información secundaria tampoco es reconocible mediante una lupa (con un aumento de 2-20x).

En la figura 6 se muestran varios ejemplos de la posible forma de las áreas excluidas formadas por píxeles. La forma y la dimensión del área excluida no pueden ser arbitrarias, esta última está limitada por la tecnología de impresión que se aplicará, como se discutió anteriormente. En la Tabla 1 a continuación, un par de anchos de línea de capacidad de impresión blanca propuestos para la preparación del elemento de seguridad de la invención, obtenidos empíricamente al realizar experimentos de humectación de tinta en un sustrato de impresión se recogen para diferentes tecnologías de impresión. Las mediciones de humectación de tinta se realizaron con tintas de impresión adaptadas a diversas tecnologías de impresión, es decir, por ejemplo, con una tinta de impresión negra de Hewlett Packard, con una tinta de impresión negra de MEMJET, con la tinta negra KODAK Prosper press y una tinta de impresión negra de EPSON, en donde el papel fibroso usado típicamente para la impresión de seguridad se aplicó como sustrato de impresión a la temperatura de 18-22 °C (temperatura ambiente) y a una presión ambiente de 101 kPa. Aquí se observa que los valores incluidos en la Tabla 1 también son válidos para otros tipos de papel, aunque la resolución requerida generalmente cambia. En particular, si el sustrato de impresión es, por ejemplo, un papel brillante, la impresión debe realizarse con una resolución de al menos 600-1200 dpi en lugar de 300-600 dpi.

En línea con lo anterior, cuando una nueva tecnología de impresión esté disponible, la humectación de tinta se puede determinar en una impresión piloto y luego se puede derivar un ancho de línea de capacidad de impresión de blanco propuesto para el área excluida expresada en número de píxeles para la nueva tecnología. Para este fin también se pueden usar las siguientes ecuaciones empíricas:

Ancho de línea [micrómetros] = 1,2 * humectación de tinta [micrómetros].

Ancho de línea [pix] = el mayor número entero de {(1,2 * humectación de tinta [micrómetros] * resolución [dpi]/25,4)/1000 + 0,5}, pero al menos 1.

Tabla 1. Ancho de línea de las áreas excluidas que llevan información secundaria.

Tecnología	Resolución típica [dpi]	Humectación de tinta [micrómetros] (depende del papel)	Ancho de línea de capacidad de impresión de blanco (de un área que queda fuera de la impresión directa)	
			[micrómetros]	[pix]
Impresión por chorro de tinta	600	10-50	12-60	1-2
Impresión láser	720	30-40	36-48	2-3
Impresión offset	8000	10-20	12-24	4-8

Aunque las áreas que quedan fuera de la impresión directa no son visibles a simple vista en la impresión del elemento de seguridad, debido a incertidumbres de impresión, cambian la escala de grises de la celda definida por la expresión de

valor de escala de grises = (número de píxeles negros en la celda) / (número de píxeles totales en la celda);

en este caso, el cambio es inversamente proporcional al aumento en el número de píxeles del área excluida dentro de la clase considerada. Por tanto, el elemento de seguridad inventivo proporcionado por el código combinado discutido anteriormente exhibe una característica inherente en la forma de los valores de escala de grises definidos anteriormente que pueden asociarse con la información secundaria latente; después de imprimir el elemento de seguridad y generar una representación digital de la impresión obtenida, dicha característica inherente puede analizarse estadísticamente.

Decodificar el elemento de seguridad inventivo aplicado sobre un sustrato de impresión y, como resultado de esto, decidir sobre la autenticidad del material impreso en cuestión se realiza de acuerdo con el esquema que se muestra en la figura 1B. De acuerdo con esto, en una primera etapa, se genera una representación digital del signo de código que lleva información primaria de dicho elemento de seguridad (etapa 160) con luz visible que entra en el rango de longitud de onda de 380 a 750 nm o haciendo uso de una fuente de luz que proporciona iluminación que corresponde espectralmente a la luz natural que cae en dicho rango de longitud de onda por medio de un medio de formación de imágenes digital adecuado, tal como un teléfono móvil, un teléfono inteligente, un escáner (de mano), una cámara web, opcionalmente una cámara, teniendo típicamente una resolución media.

Después de esta etapa, se realiza el preprocesamiento de la imagen del signo de código (etapa 170), en donde al principio se inspecciona la calidad de la imagen: en el caso de una imagen con calidad inadecuada (debido, por ejemplo, a una iluminación insuficiente), la imagen del signo de código no se tiene en cuenta y se graba una nueva imagen de signo de código. Si dicho signo de código está oculto en una ilustración ornamental, la separación de la imagen del signo de código de la ilustración ornamental también se realiza durante el procesamiento previo. La forma de ejecutar la separación depende de la forma de esconder; en este sentido, el Folleto de Publicación Internacional n.º W099/35819, mencionado anteriormente, divulga una posible solución ejemplar en detalle. Los expertos en la técnica conocen otros métodos de separación y, por tanto, no se discuten aquí más detalles. Como etapa final del procesamiento previo, la imagen del signo de código se convierte en una imagen sombreada en gris y la imagen en escala de grises así obtenida se almacena para su posterior análisis.

Después de completar las etapas de procesamiento previo anteriores en buen orden, se lleva a cabo una verificación de la información secundaria introducida en el código que lleva información primaria al momento de generar el elemento de seguridad aplicado al material impreso (etapa 180). Con este fin, la clasificación de puntos basada en el código que lleva información primaria se realiza nuevamente. Después de la terminación de la clasificación, se realiza un análisis estadístico de los valores en escala de grises de las clases obtenidas. Para la imagen tomada de una impresión genuina, los valores en escala de grises de las clases tienen que disminuir continuamente. Se requiere el análisis estadístico debido a la distorsión de la cámara. En este caso, la prueba t de dos muestras es un método adecuado con la hipótesis de media1 = media2 contra la hipótesis alternativa de media1 < media2 con un nivel de significado de p=0,05. Para un experto en la técnica, está claro que, en lugar de la prueba t, otras pruebas estadísticas son igualmente aplicables en este caso.

Al copiar, las islas de píxeles que forman el área excluida pequeña se cierran y, por lo tanto, ya no se mantiene un aumento en los valores medios en escala de grises de las clases. El cierre es causado por las etapas durante la copia. En lo que respecta a este proceso, el número de píxeles que forman el área excluida y la disposición de dichos píxeles son de gran importancia. Dicha área excluida tiene que exhibir un ancho, a lo largo de al menos una de sus dimensiones, que corresponde al ancho de la línea de impresión en blanco que se proporciona en la Tabla 1 para que el escáner o la fotocopiadora usados puedan eliminar los píxeles del área excluida con seguridad. En tal caso, el material impreso inspeccionado se considera una "falsificación". Si, como resultado del análisis estadístico, se puede afirmar que el aumento en los valores medios en escala de grises de las clases se mantiene, el material impreso inspeccionado provisto del elemento de seguridad de la invención se considera "genuino".

La figura 7 ilustra un par de códigos de puntos ejemplares que llevan información primaria (visible a simple vista), en particular, de izquierda a derecha, un código de barras, un código QR, un código de matrices de datos y un llamado código de diseño, en donde cada uno de los mismos exhibe una dimensión mayor que excede los 50 micrómetros. Para generar el elemento de seguridad de acuerdo con la invención, todos ellos pueden ser utilizados.

El cierre de las islas blancas que llevan información secundaria de una impresión producida por una impresora de inyección de tinta se muestra en la figura 8 tomada por un microscopio de campo con un aumento de 50x. Mientras que el área excluida de la plancha de impresión en el lado izquierdo exhibe límites agudos, las áreas excluidas apenas se pueden detectar en la impresión en el lado derecho. Asimismo, al copiar, la máquina fotocopiadora cierra estos puntos inciertos y la fotocopia se vuelve negra al 100 %.

Las figuras 9A y 9B ilustran algunos ejemplos de una información secundaria oculta en los diseños.

Brevemente resumido: para lograr la presente invención en la práctica, un dispositivo de inspección específico no es absolutamente necesario; con este fin, son suficientes una foto tomada, por ejemplo, con un teléfono inteligente común y un software de decodificación y análisis basado en el método que se muestra en la figura 1B instalado en el teléfono. (No obstante, la foto o la representación digital del elemento de seguridad también puede ser tomada por cualquier otra cámara, y el software de análisis puede ser ejecutado por cualquier ordenador con la capacidad informática adecuada). El dispositivo de inspección puede ser un dispositivo personalizado; debe contener una unidad lectora (CCD, CMOS), por ejemplo, una cámara digital, para generar una representación digital del elemento de seguridad, una unidad de procesamiento de datos, por ejemplo, un microcontrolador o un procesador, preferentemente una unidad de memoria, así como el propio software de decodificación. La aplicación del elemento de seguridad de la invención en un sustrato de impresión no requiere una máquina de impresión de alta precisión; para ello, es adecuada una impresora de inyección de tinta con una resolución de incluso 600 dpi. Esto permite una amplia gama de

aplicaciones para la solución de acuerdo con la presente invención.

Como la información secundaria, en general, no está almacenada en una base de datos, para inspeccionar la autenticidad de un material impreso con el elemento de seguridad de acuerdo con la invención, no hay necesidad de un enlace de comunicación de datos. La información latente (secundaria) se puede deducir de la información primaria y, por tanto, es simplemente el dispositivo de inspección el que realmente se necesita para la verificación de la autenticidad.

Para un experto en la técnica, sin embargo, es evidente que el concepto de codificación previamente seleccionado para la información secundaria (o su clave generadora) puede almacenarse en una base de datos remota. En tal caso, dentro del marco del método de inspección de autenticidad, el dispositivo de inspección establece una conexión con la base de datos a través de un canal de comunicación de datos apropiado, interroga la clave generadora necesaria y luego realiza la verificación de autenticidad del material impreso cuestionado. Una ventaja adicional de tal realización es que dicho dispositivo de inspección también puede proporcionar información precisa para la base de datos sobre la ubicación geográfica de la interrogación clave como consecuencia de la comunicación de datos establecida. Si el dispositivo de inspección es un teléfono móvil o un teléfono inteligente, dicha información puede proporcionarse fácilmente en forma de datos de base móvil o coordenadas GPS.

Además, cuando se aplica un elemento de seguridad de acuerdo con la presente invención, no se requiere(n) cara(s) tinta(s) de impresión de composición específica ni sustratos de impresión costosos producidos específicamente. Como también será evidente para un experto en la técnica, el elemento de seguridad de la invención también se puede formar sobre/en una superficie del objeto a proteger por ablación con láser en lugar de imprimir con tinta. En caso de tales aplicaciones, el sustrato a base de papel es reemplazado por cualquier material que pueda ser mecanizado por ablación láser.

También está claro para una persona experta en la técnica que el elemento de seguridad de acuerdo con la presente invención puede usarse solo o en combinación con otros elementos de seguridad como un elemento adicional al mismo.

REIVINDICACIONES

1. Un método para inspeccionar la autenticidad de un material impreso con un elemento de seguridad, comprendiendo dicho elemento de seguridad un código (20) que lleva información primaria y es detectable a simple vista con luz visible que entra dentro del rango de longitud de onda de 380 a 750 nm, y, combinado con el mismo, un código (32, 42) que lleva información secundaria y es indetectable a simple vista, en donde en el elemento de seguridad aplicado como una impresión en un sustrato de impresión, la dimensión más grande en al menos una dirección del plano del código que lleva información secundaria es de 2 a 40 micrómetros, y en donde el código que lleva información secundaria es generado por áreas del código que llevan información primaria no impresa directamente en las mismas, comprendiendo el método las etapas de
grabar una imagen del código (20) que lleva la información primaria del elemento de seguridad al iluminar el material impreso con luz visible que entra dentro del rango de longitud de onda de 380 a 750 nm;
convertir la imagen obtenida en una imagen en escala de grises y almacenar la imagen en escala de grises;
segmentar la imagen en escala de grises almacenada;
clasificar segmentos de la imagen segmentada en escala de grises en un número dado de clases basándose en un algoritmo de codificación preestablecido;
asignar un valor medio de escala de grises, como característica inherente que se puede analizar estadísticamente, a cada clase sometiendo dichas clases una tras otra a análisis estadístico;
generar una tendencia a partir de los valores medios obtenidos en escala de grises que cambian de clase en clase;
adoptar una postura sobre el tema de la autenticidad de dicho material impreso en función de la forma de dicha tendencia.

2. El método de acuerdo con la reivindicación 1, en donde el código (20) que lleva información primaria se elige de un grupo que consiste en códigos de barras, códigos QR, códigos de matrices de datos y códigos de puntos desarrollados de forma única con codificación no pública.

3. El método de acuerdo con la reivindicación 1, en donde el sustrato de impresión está provisto de una ilustración gráfica ornamental y dicho código que lleva información primaria está oculto en dicha ilustración.

4. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde la información secundaria resulta de la información primaria.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, caracterizado por que el sustrato de impresión se elige de un grupo que consiste en billetes, valores, facturas, embalajes de productos, tarjetas/etiquetas de identidad, cubiertas, entradas, certificados, documentos personales, cupones o cualquier otro documento similar o superficie de objeto que esté equipada con protección contra copias.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en donde dicha imagen es generada por un dispositivo de formación de imágenes con una resolución de 300 a 1200 dpi.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, que también comprende la etapa de separar la imagen del código que lleva información primaria de una ilustración ornamental si dicho código está oculto en la ilustración ornamental antes de convertir dicha imagen grabada del código en la imagen en escala de grises.

8. El método de acuerdo con cualquiera de las reivindicaciones 1 a 7, en donde en dicho análisis estadístico de clases también se realiza una prueba t de dos muestras de pares de las clases.

9. El método de acuerdo con cualquiera de las reivindicaciones 1 a 8, en donde adoptar una postura sobre el tema de la autenticidad comprende
confirmar la autenticidad del material impreso cuando dicha tendencia coincide con una tendencia predeterminada de aumentar los valores medios en escala de grises; y
negar la autenticidad del material impreso cuando dicha tendencia no coincide con la tendencia predeterminada de aumentar los valores medios en escala de grises.

10. Un aparato configurado para implementar el método de acuerdo con cualquiera de las reivindicaciones 1 a 9.

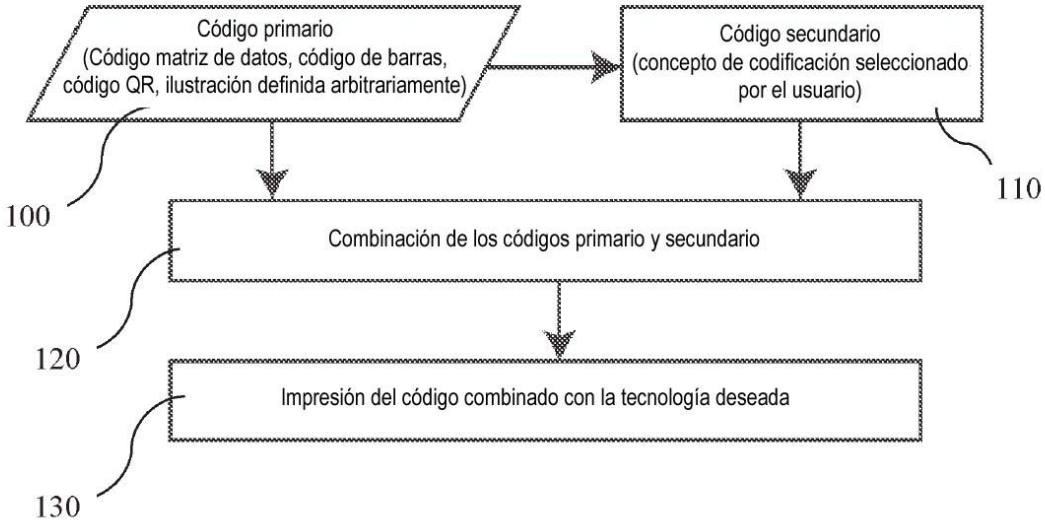

Figura 1A

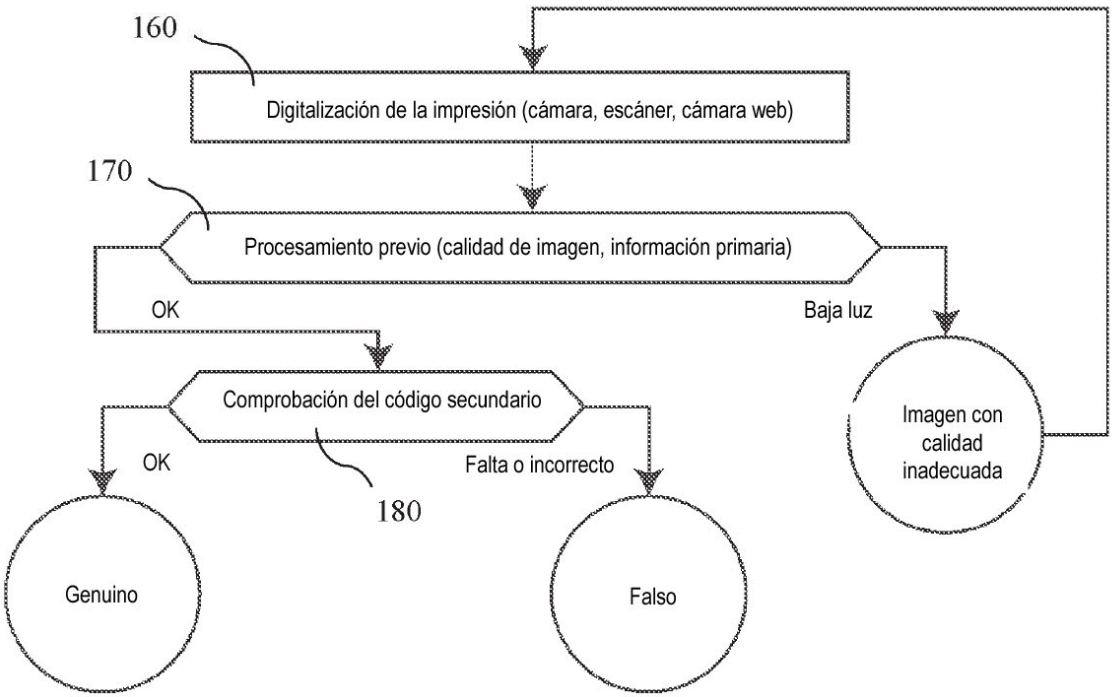

Figura 1B

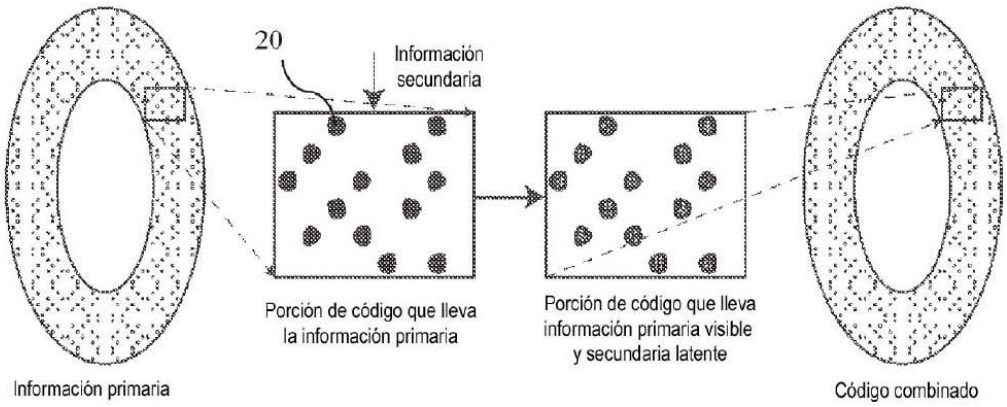

Figura 2

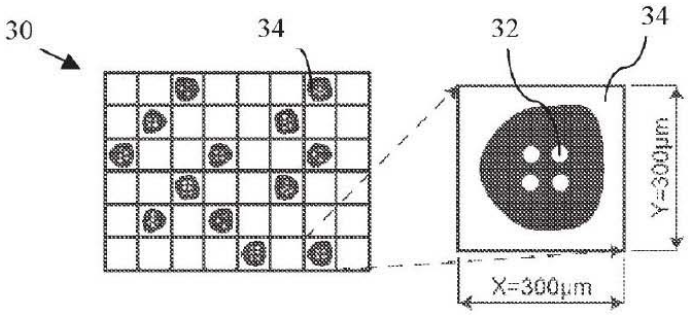

Figura 3

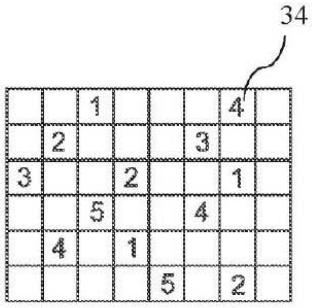

Figura 4

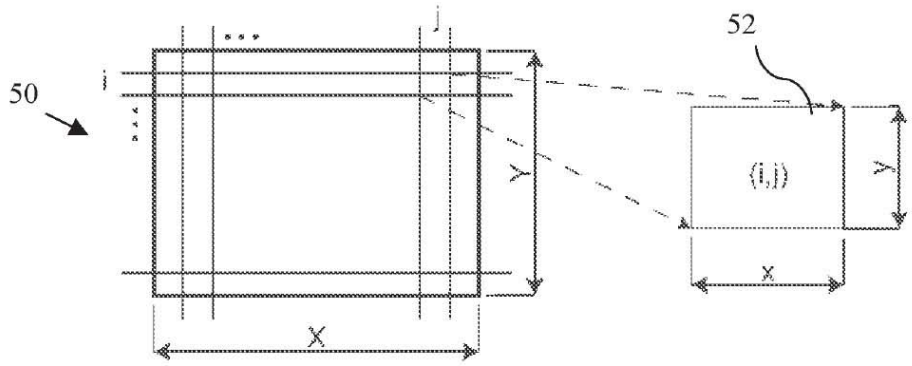

Figura 5

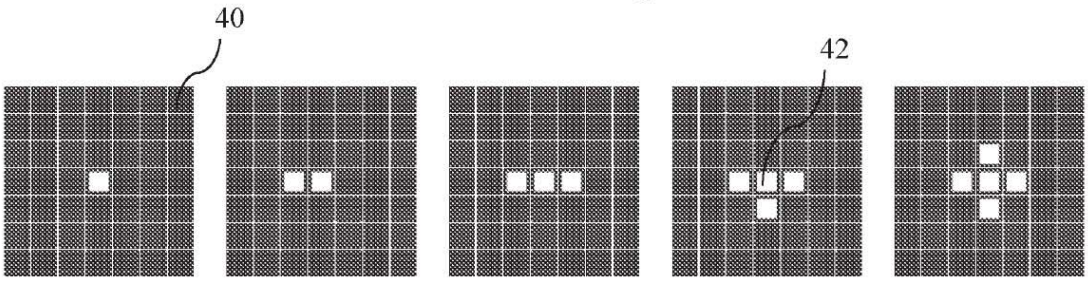

Figura 6

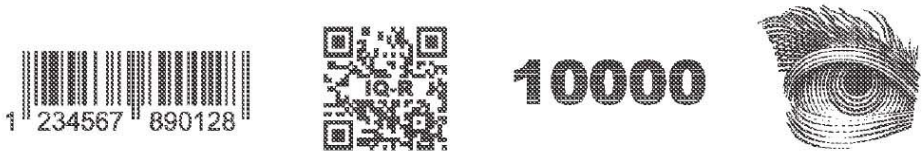

Figura 7

Figura 8

Figura 9A

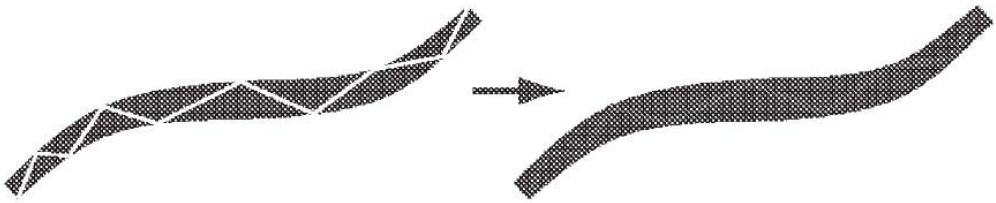

Figura 9B