

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 727 101**

51 Int. Cl.:

**G06K 19/08** (2006.01)

**B41M 3/14** (2006.01)

**B42D 15/00** (2006.01)

**G07D 7/04** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **11.04.2013** **E 13163309 (1)**

97 Fecha y número de publicación de la concesión europea: **20.02.2019** **EP 2790133**

54 Título: **Rasgo de seguridad y objeto con rasgo de seguridad**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**14.10.2019**

73 Titular/es:

**EUROPEAN CENTRAL BANK (100.0%)  
Kaiserstrasse 29  
60311 Frankfurt am Main, DE**

72 Inventor/es:

**SCHULTE-WIEKING, KAY;  
NOEHTE, STEFFEN y  
BORGSMÜLLER, STEFAN**

74 Agente/Representante:

**PONS ARIÑO, Ángel**

ES 2 727 101 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Rasgo de seguridad y objeto con rasgo de seguridad

### 5 **Campo de la invención**

La invención se refiere a un rasgo de seguridad y un objeto que comprende el rasgo de seguridad.

### **Antecedentes**

10 Es conocida en la técnica una gran diversidad de rasgos de seguridad para toda clase de objetos valiosos o de seguridad. La mayoría de los rasgos de seguridad hacen uso de efectos ópticos específicos de pequeñas estructuras o efectos físicos/ópticos de sustancias raras.

15 A partir del documento US 2006/0279767, frente al cual se delimita la reivindicación 1, es conocida la denominada "Constelación de Eurión" comúnmente usada como un rasgo de seguridad para billetes. Este rasgo consiste en marcas adicionales en forma de pequeños círculos en una disposición geométrica específica. Estos círculos tienen una apariencia similar como el resto del contenido del documento.

20 El documento WO 2009/150622 A2 desvela marcados visibles formados por pequeños elementos que tienen definidas diferentes formas geométricas y que forman información encriptada por una disposición específica y formas variables de pequeños elementos que parecen anticipados.

25 El documento US 7 353 994 B2 describe partículas distribuidas aleatoriamente, es decir las imágenes derivadas de las partículas son aleatorias.

El documento WO 2011/098803 y US 2013 0043311 describen aperturas que no están ocultas en el documento.

30 El documento DE 10 304 805 A1 desvela un marcado de seguridad que comprende un patrón aleatorio que se aplica a un producto o etiqueta. Una huella digital en forma de un conjunto de datos se extrae a partir del patrón de entrada aleatorio. La huella digital contiene las características individuales del patrón y se almacena individualmente para cada marcado de seguridad. La huella digital se extrae durante la autenticación y se comprueba para observar si coincide con la huella digital almacenada. El marcado de seguridad puede usarse en general para protegerse contra falsificación por ejemplo para dinero, documentos, marcas de agua, placas de número de vehículo, etc.

35 El documento US 2003 0115470 A1 desvela aparatos, métodos, y artículos de fabricación que tienen un esquema de validación de comprobación en el que se digitaliza, encripta y embebe una firma del pagador en la parte delantera del cheque usando glifos. Cuando el pagador busca convertir un cheque en blanco en un instrumento negociable, el usuario rellena el cheque y lo firma. Cuando se presenta el cheque a un banco para su pago, un cajero automático que usa un dispositivo de decodificación, decodifica y desencripta la firma digitalizada de manera que puede observarse una imagen legible por humanos de la firma digitalizada en una pantalla para su comparación con la firma escrita del pagador. Si las dos firmas son idénticas, el cheque se paga

45 El documento US 2013 0043311 A1 desvela un elemento de seguridad para un documento de valor. El elemento de seguridad incluye una serie de aperturas a través de al menos una porción del documento de valor, formando la disposición de las aperturas con relación entre sí formando un elemento de datos observable. La serie de aperturas incluye aperturas de al menos dos formas u orientaciones diferentes, representando la aparición de las diferentes formas u orientaciones en la serie un elemento de datos codificados.

50 El documento WO 02/095674 desvela un transpondedor de RFID en forma de un elemento de chip con una antena en forma de un código de barras en un sustrato de papel. El chip divide la antena en dos partes.

55 El documento US 5.464.974 desvela un código binario legible por máquina que es dinámicamente variable en tamaño, formato y densidad de información. El código binario está formado como una matriz que tiene un perímetro y datos contenidos en el mismo. El perímetro se proporciona con indicios de densidad para indicar la densidad de datos contenidos en la matriz. El perímetro también se proporciona con indicios de tamaño para indicar el tamaño de la matriz. Utilizando los indicios de densidad e indicios de tamaño, un dispositivo de exploración puede calcular el tamaño y densidad de información del código binario.

60 El documento WO 02/095674 trata con un elemento de chip de transpondedor de RFID con una antena en forma de un código de barras.

### **Sumario**

65 Es un objeto de la invención proporcionar un rasgo de seguridad que está disimulado independientemente de si es o no visible para el ojo desnudo. Es también un objeto de la invención proporcionar un objeto que comprende el rasgo

de seguridad.

El objeto se resuelve mediante la materia objeto de la reivindicación 1.

5 La característica del objeto (o elemento del objeto) puede ser debido ventajosamente a un proceso de fabricación del objeto. La característica inherente puede ser un efecto secundario o consecuencia inevitable del proceso de fabricación. La característica inherente puede ser también un efecto deseado o apariencia física deseada del objeto. Sin embargo, la característica inherente ventajosamente no se crea intencionadamente para ocultar el rasgo de seguridad. Este aspecto de la invención generalmente proporciona que el rasgo de seguridad no sea inmediatamente visible cuando se inspecciona el objeto por el ojo desnudo (o incluso por el uso de instrumentos de detección o inspección). El rasgo de seguridad de acuerdo con aspectos de la invención puede mezclarse de esta manera en su entorno.

15 De acuerdo con un aspecto de la invención, pueden añadirse marcas al objeto. El rasgo puede a continuación ocultarse al ojo desnudo (disimulado) debido a diversas diferentes razones. El rasgo de seguridad puede adaptarse ventajosamente a la característica inherente del objeto en términos de uno o más de lo siguiente: tamaño, forma, distribución, número y/o color etc. Más específicamente, el color, tamaño, forma, distribución y/o número de marcas (puntos, orificios, partículas) añadidas (adicionales) puede adaptarse a la característica del objeto (aparición visual). Las marcas añadidas pueden ser muy pequeñas (por ejemplo tener un diámetro menor que 20 µm). Las marcas adicionales pueden tener el mismo color o similar que el objeto (al menos en la localización de la superficie del objeto donde se añaden las marcas). Las marcas adicionales pueden distribuirse aleatoriamente. Las marcas adicionales pueden tener únicamente un número pequeño por área de la superficie del objeto predefinida. Las marcas añadidas o adicionales pueden ser también luminiscentes bajo luz UV (ultravioleta) o luz IR (infrarroja). Bajo condiciones ambientales normales (luz diurna normal) las marcas adicionales pueden ser sustancialmente invisibles al ojo desnudo. Las marcas añadidas ventajosamente no pueden percibirse o ser distinguibles por el ojo desnudo bajo luz ambiente. Estos aspectos soportan adicionalmente la capacidad de disimulo del rasgo de seguridad.

30 El proceso de configuración de cualesquiera datos predeterminados de manera que la apariencia física del rasgo de seguridad sea similar a una característica inherente física específica del objeto forma parte de una codificación de canal. En otras palabras, la invención también proporciona un rasgo de seguridad que comprende marcas adicionales que están dispuestas de acuerdo con la codificación de canal de acuerdo con los aspectos de la invención descritos en este punto a continuación.

35 En una realización de la invención, el objeto puede comprender marcas originales como una característica del objeto. Las marcas originales pueden ser una consecuencia del proceso de fabricación del objeto. Las marcas originales pueden distribuirse aleatoriamente. El rasgo de seguridad puede a continuación estar configurado para tener una apariencia similar como se proporciona por las marcas originales en el objeto. Esto significa que la característica preexistente del objeto puede imitarse sin cambiar sustancialmente la apariencia física original del objeto. Las marcas originales pueden ser defectos, impurezas, partículas, orificios, fibras, pigmentos, etc., el rasgo de seguridad puede comprender entonces marcas adicionales que tienen una apariencia similar que las marcas originalmente existentes. Las marcas adicionales pueden ser similares a las marcas originales en términos de una o más de las siguientes características: tamaño, forma, número, distribución, color, etc. Cada uno de estos aspectos de la invención mejora adicionalmente el disimulo del rasgo de seguridad.

45 La característica preexistente o las marcas originales del objeto pueden también ser sustancialmente invisibles al ojo desnudo. Esto significa que también las marcas originales pueden no ser evidentes cuando se inspeccionan por el ojo desnudo sin usar una lupa, un microscopio u otros medios de inspección o luz especial como luz UV o IR. Las marcas adicionales pueden entonces tener la misma apariencia y también ser sustancialmente invisibles al ojo desnudo.

50 De acuerdo con un aspecto de la invención, una o más de las siguientes características pueden usarse para representar la información legible por máquina predeterminada: la localización absoluta o relativa de las marcas adicionales, el tamaño, la forma, y/o el color de las marcas adicionales individuales.

55 De acuerdo con un aspecto adicional de la invención, las marcas adicionales pueden estar dispuestas en grupos. La información o datos pueden entonces representarse por una disposición específica en un grupo de marcas adicionales. Un grupo de marcas adicionales también se denomina como un símbolo. Un símbolo puede comprender también únicamente una marca adicional. Este aspecto tiene varias ventajas. El grupo o símbolo puede identificarse fácilmente. Un grupo o símbolo puede estar basado en información redundante. Cuanto más redundante sea la información de un símbolo o grupo de marcas adicionales, mejor será la tasa de error durante la lectura de la información.

60 En una realización de la invención, la localización relativa y/o absoluta de las marcas en un área específica, región o porción del objeto puede representar la información (datos). Esto también simplifica la detección de las marcas y puede usarse para aumentar la redundancia de la información. Todos los parámetros y propiedades detectables de las marcas, sean individuales, sean con respecto entre sí o con respecto al objeto pueden usarse ventajosamente para representar información (datos).

65

Cada uno de los grupos puede comprender entonces un número predeterminado de marcas. El número de marcas por grupo puede ser, por ejemplo, n. En realizaciones ventajosas n puede ser igual a 1, 2, 3, 4, 5, 6 o mayor.

5 De acuerdo con un aspecto de la invención, cada grupo de marcas puede representar una palabra de múltiples bits de datos (datos predeterminados) que se representa por (almacena en) el rasgo de seguridad. Esto simplifica el proceso de codificación de canal en el que las marcas, grupo de marcas o símbolos están asignados a los datos (información predeterminada).

10 De acuerdo con un aspecto de la invención, el número de bits de la palabra de múltiples bits puede ser j. En realizaciones ventajosas j puede ser igual a 2, 3, 4, 5, 6, 7, 8, 9, 10 o mayor.

El número de marcas por grupo puede ser diferente del número de bits de la palabra de múltiples bits que se representa por el grupo de marcas. En otras palabras, una marca no representa necesariamente un único bit.

15 De acuerdo con un aspecto de la invención, pueden usarse dos o más símbolos diferentes para los mismos datos (palabra de múltiples bits). Esto es ventajoso ya que la redundancia en el rasgo de seguridad puede aumentarse adicionalmente mientras que la apariencia puede aún ser aleatoria, si uno de los múltiples posibles símbolos se selecciona aleatoriamente.

20 De acuerdo con un aspecto de la invención, la información predeterminada o los datos que se representan por el rasgo de seguridad pueden ser datos encriptados sin procesar. Cualquier información/datos predeterminados (típicamente datos digitales) puede entonces encriptarse antes de que se codifique por canal. Esto aumenta la seguridad del rasgo.

25 Los datos/información predeterminados pueden encriptarse usando la Norma de Encriptación Avanzada (AES). Este es un algoritmo de clave simétrica en el que únicamente el propietario de la clave puede decodificar la información almacenada. El algoritmo AES genera un valor de función de troceo que se almacena en el campo de datos. La lectura del valor de troceo no es suficiente para la reconstrucción de la información almacenada. Además, es necesaria la clave para desencriptar el valor de troceo y para obtener la información original.

30 Adicionalmente, la información/datos predeterminados que se representan por el rasgo de seguridad pueden procesarse de acuerdo con un algoritmo de corrección de errores para hacer posible detectar y/o corregir errores de detección/lectura. Un algoritmo ventajoso es el algoritmo Reed-Salomon.

35 De acuerdo con un aspecto de la invención, los datos sin procesar encriptados pueden ser un número de serie encriptado del objeto (por ejemplo el número de serie de un billete).

40 También es posible usar el rasgo de seguridad de acuerdo con aspectos de la invención jerárquicamente. Esto significa que un rasgo de seguridad puede tener diferentes niveles de modo que un primer nivel es detectable por detectores bastante sencillos. Algunas marcas proporcionadas en el rasgo de seguridad pueden entonces no ser detectables por los detectores sencillos sino únicamente por detectores más complejos. Por consiguiente, es posible incorporar diferentes niveles de seguridad en un único rasgo de seguridad.

45 El objeto al que se aplica el rasgo de seguridad puede ser un objeto valioso, un objeto de seguridad, un producto de consumidor, un documento de seguridad, un documento valioso, un certificado (por ejemplo de nacimiento, residencia, estado marital, nombre etc.), una copia certificada de un documento, una tarjeta, como por ejemplo una tarjeta inteligente, una tarjeta de acceso, una tarjeta de crédito, una tarjeta de bonificación, una tarjeta de identidad, un pasaporte, etc.

50 En una realización ventajosa, el objeto puede ser un documento valioso, como por ejemplo un billete.

55 El rasgo de seguridad puede a continuación incorporarse, por ejemplo en una capa o lámina metalizada (por ejemplo una lámina con una capa metálica fina) de un elemento de un objeto, como por ejemplo un documento valioso o un billete. El metal puede ser aluminio o cobre. En una realización el elemento del objeto puede ser una banda metalizada. En otra realización de la invención, el elemento del objeto que lleva el rasgo de seguridad puede ser un parche. El elemento que lleva el rasgo de seguridad puede ser una lámina fina de metal o laca o color al que se aplica el rasgo de seguridad.

60 El rasgo de seguridad de acuerdo con una realización de la invención puede comprender puntos. Un punto puede ser entonces una marca adicional. Las marcas adicionales, es decir los puntos, pueden imprimirse. Los puntos pueden estar adaptados en número y/o tamaño y o distribución y/o color a la superficie de un objeto. El objeto puede ser una hoja de papel o plástico, etc. Por ejemplo, si la superficie del objeto es blanca, las marcas adicionales (puntos) pueden también ser sustancialmente blancas o amarillo claro. El diámetro máximo de los puntos puede ser menor que 20 µm. Las marcas adicionales pueden imprimirse con color luminiscente (fluorescente, etc.) color, como por ejemplo color luminiscente de UV o IR.

65 En otra realización, el rasgo de seguridad puede ser una estructura escrita con láser. Las marcas del rasgo de

seguridad pueden ser desmetalizaciones con tamaño micrométrico locales. Esto es ventajoso ya que la clase de bandas metalizadas o parches usados en billetes (y otros documentos) normalmente muestran algunos defectos en forma de pequeños orificios que parecen distribuirse aleatoriamente a través de la banda. Estos orificios son debido al proceso de fabricación. El rasgo de seguridad puede estar localizado en una parte de la banda de lámina o puede extenderse a través de la totalidad de la banda de lámina añadiendo marcas adicionales en forma de orificios. Estos orificios pueden generarse por un láser y entonces parecer como todos los demás puntos desmetalizados que son debidos al proceso de fabricación.

El rasgo de seguridad puede leerse con un sensor especializado o aparato de detección. La detección puede estar basada en un reconocimiento de patrón. Puede tomarse una imagen del área donde está localizado el rasgo de seguridad. La instantánea puede a continuación procesarse. Las posibles localizaciones de marcas adicionales son conocidas, de modo que el algoritmo de reconocimiento de patrón puede buscar las marcas adicionales específicas. Si se detectan las marcas, puede confirmarse la autenticidad del objeto. Debido a redundancia, la autenticidad puede confirmarse también si únicamente se detectan unas pocas y no todas las marcas adicionales.

Con respecto a la realización anteriormente descrita que usa un elemento u objeto que comprende puntos desmetalizados, el rasgo de seguridad puede detectarse y leerse en la transmisión usando una configuración de microscopio. Una fuente de luz puede estar localizada detrás del documento valioso (en la parte trasera) y el microscopio puede estar localizado en el lado opuesto del documento valioso (parte delantera). Si las marcas adicionales del rasgo de seguridad son un poco más grandes (en diámetro máximo o área en sección transversal) que las marcas/puntos originales, los puntos desmetalizados pueden parecer más brillantes que el fondo. En otras palabras, el mismo rasgo de seguridad comprende un número de puntos escritos por láser que aparecen estadísticamente. El número de puntos por área de la banda puede ser entonces muy bajo. En una realización, el número de puntos puede ser entre 100 y 200. Esto mejora el disimulo del rasgo.

La robustez de la codificación permite lectura muy estable de los datos/información almacenados en el rasgo de seguridad incluso a velocidades de transporte altas del documento valioso, en particular de billetes. Puede usarse un algoritmo de procesamiento de imágenes para decodificar los datos después de que se toma una imagen. La misma estructura básica del elemento de seguridad puede usarse en diferentes documentos valiosos.

En el contexto de esta memoria descriptiva se aplican los siguientes parámetros:

Número de bits de usuario:  $x (= k*j)$

Número de símbolos (datos de usuario)  $k$

Número de bits de número de serie de un billete:  $y$

Número de bits de información adicional (de usuario):  $z$

Número de "marcas" por símbolo:  $n$

Número de bits por símbolo/palabra de múltiples bits:  $j$

Número de "marcas existentes" (marcas originales):  $v$

Número de "marcas añadidas" (marcas adicionales):  $w$

Por ejemplo, un código de error de Reed-Solomon  $RS(m,k)$  transforma  $k$  símbolos de datos en  $j$  bits añadiendo  $2*t$  símbolos de paridad de  $j$  bits. El resultado es  $m$  símbolos de  $j$  bits. En la etapa de decodificación pueden detectarse y corregirse  $t=(m-k)/2$  símbolos incorrectos.

En general, el número de bits a almacenarse en el rasgo depende del algoritmo de corrección de errores usado y el número de errores que han de detectarse y/o corregirse.

De acuerdo con una realización de la invención, pueden incorporarse datos de usuario individuales en el billete. Si por ejemplo, la capacidad de almacenamiento del usuario del rasgo de seguridad es  $x$  bits ( $k$  múltiples palabras de bits de  $j$  bits, es decir  $x=k*j$ ), es posible incorporar por ejemplo un número de serie que puede representarse por  $y$  bits, mientras que  $y$  es igual o inferior a  $x$ . Los datos pueden ser un número de serie del documento valioso. En otra realización, únicamente puede usarse una parte de los datos de usuario (por ejemplo para un número de serie) y los restantes  $z=x-y$  bits pueden usarse para otra información.

De acuerdo con un aspecto de la invención, los datos de usuario individuales a almacenarse en el rasgo de seguridad pueden ser un número de serie, un número de lote, una denominación, un país de producción, un año de producción u otra información.

En una realización de la invención, esta información/datos adicionales (z bits) pueden ser datos estadísticos u otros rasgos del documento valioso. Esto puede a continuación conducir a la posibilidad de correlacionar rasgos de seguridad o datos del documento valioso. Usar correlación puede mejorar el nivel de seguridad contra copiado y falsificación.

5 Una ventaja del rasgo de seguridad de acuerdo con los aspectos de la invención es que el rasgo no se ve afectado necesariamente por un diseño específico del objeto. Adicionalmente, el rasgo de seguridad de acuerdo con aspectos de la invención no afecta al diseño del objeto debido a su carácter disimulado.

10 El rasgo de seguridad de acuerdo con aspectos de la invención puede escribirse un sistema litográfico de láser que permite desmetalización directa de capas metálicas finas. La desmetalización puede tener tamaños de punto muy pequeños (únicamente unos pocos micrómetros, como por ejemplo de 1, 2, 3, 4 hasta 10, 16 o 20  $\mu\text{m}$ ) y una precisión posicional relativa muy alta de las marcas adicionales de por ejemplo de 0,1, 0,2 hasta 0,5  $\mu\text{m}$ .

15 El rasgo de seguridad de acuerdo con aspectos de la invención puede comprender entonces únicamente unos pocos puntos con tamaño de micrómetros que aparecen distribuidos aleatoriamente. Si estos puntos son suficientemente pequeños, no pueden observarse con el ojo desnudo, ni en reflejo ni en transmisión.

20 En una realización de la invención, incluso con una lupa o microscopio, los puntos no pueden detectarse en modo de reflejo por el ojo desnudo. Únicamente en modo de transmisión y por el uso de un microscopio, pueden identificarse los puntos.

25 De acuerdo con un aspecto de la invención, las posiciones de las marcas en cada símbolo están distribuidas aleatoriamente (pseudo-aleatoriamente). Las marcas (o puntos) entonces parecen como un patrón aleatorio similar a defectos en bandas de lámina metalizada de documentos valiosos tales como billetes. En particular, las bandas de lámina metalizada de documentos valiosos o billetes normalmente tienen esta clase de defectos.

30 Debido a la apariencia aleatoria de las marcas adicionales es difícilmente posible notar alguna regularidad comparando los patrones de marca de diferentes objetos.

De acuerdo con un aspecto de la invención, puede almacenarse información estadística individual del objeto en un soporte de datos seguro que se incluye en el objeto.

35 De acuerdo con un aspecto de la invención, los datos/información predeterminados a almacenarse en el rasgo de seguridad pueden estar correlacionados con otra información. Esta información puede estar relacionada, por ejemplo con variaciones de producción del objeto. Estas variaciones de producción pueden comprender propiedades como densidad óptica, alineación, distorsiones geométricas, agudeza de bordes, orificios, etc.

40 En una realización de la invención, los datos/información en el rasgo de seguridad pueden estar correlacionados con el número de serie impreso del objeto.

45 De acuerdo con un aspecto de la invención, los datos/información en el rasgo de seguridad pueden estar correlacionados con otro rasgo de seguridad del objeto. Este otro rasgo de seguridad puede ser una impresión UV (ultravioleta), magnética o de infrarrojos (IR).

50 De acuerdo con un aspecto de la invención, los datos/información en el rasgo de seguridad pueden estar correlacionados con variaciones de producción del objeto en su totalidad o únicamente del componente del objeto que lleva el rasgo de seguridad. Estas variaciones de producción pueden estar relacionadas con fibras de UV, rugosidad de papel, alineación, propiedades de lote, etc.

De acuerdo con un aspecto de la invención, cada símbolo puede estar localizado en (o delimitado por) un área específica, región o porción del objeto. Usar esta clase de área definida, región o porción puede ser ventajoso para identificar los diferentes símbolos. El área predefinida de un símbolo se denomina como un bloque.

55 De acuerdo con un aspecto de la invención, los varios bloques (áreas, regiones o porciones que contienen los símbolos) pueden estar compuestos para representar campos de datos.

60 De acuerdo con otro aspecto de la invención, pueden proporcionarse múltiples campos de datos que contienen la misma información en el objeto. Este aspecto de la invención mejora la robustez de las características de seguridad, si uno o más de los campos de datos se destruye parcial o completamente.

65 De acuerdo con un aspecto de la invención, dos símbolos de un conjunto de símbolos nunca comparten cualesquiera marcas. Esto significa que las marcas de dos símbolos nunca están en la misma localización. Las marcas de diferentes símbolos pueden también variar en forma y tamaño.

De acuerdo con un aspecto de la invención, el número de marcas por símbolo puede aumentarse. Esto reduce la tasa

de error ya que un símbolo aún puede detectarse correctamente y leerse incluso si no todas las marcas fueran legibles. Cuantas más marcas se usen por símbolo, más robusta es la codificación de canal.

De acuerdo con un aspecto de la invención, las posiciones de las marcas en los símbolos se eligen aleatoriamente.

5 De acuerdo con un aspecto de la invención, cada rasgo de seguridad puede calcularse individualmente. Esto proporciona una estructura individual única para cada rasgo de seguridad y objetos diferentes pueden tener un rasgo de seguridad diferente.

10 De acuerdo con un aspecto de la invención, puede proporcionarse un marcado o estructura adicional en el objeto que lleva el rasgo de seguridad. El marcado adicional puede servir para alinear el objeto con un detector para leer el rasgo de seguridad.

15 En una realización de la invención, el objeto puede comprender un primer marcado adicional para alineación aproximada y un segundo marcado adicional para alineación precisa. Al menos el segundo marcado para alineación precisa puede producirse por las mismas etapas de fabricación y/o dispositivos que se usan para las marcas adicionales del rasgo de seguridad.

20 Si, en una realización, el rasgo de seguridad comprende marcas adicionales fabricadas por un láser, el láser puede usarse también para el segundo marcado. Si, en otra realización, el rasgo de seguridad comprende marcas adicionales fabricadas por impresión, el mismo dispositivo de impresión puede usarse también para el segundo marcado. Esto proporciona que la misma precisión que se usa para las marcas adicionales del rasgo se aplique automáticamente al segundo marcado que sirve para alinear apropiadamente el objeto para la detección de las marcas adicionales del rasgo de seguridad.

25 Adicionalmente, el primer marcado puede ser un tipo diferente de marcado que el segundo marcado. Por ejemplo, puede ser visible al ojo desnudo mientras que el segundo marcado no es visible. La estructura y visibilidad del primer marcado pueden ser mucho mayores que la visibilidad y estructura del segundo marcado.

30 De acuerdo con otro aspecto más de la invención el rasgo de seguridad puede organizarse jerárquicamente. Esto significa que un rasgo de seguridad puede tener diferentes niveles de modo que puede detectarse un primer nivel por un primer tipo de detectores y se detecta el segundo nivel por un segundo tipo de detectores. El primer tipo de detectores puede ser detectores bastante sencillos. Algunas marcas proporcionadas en el rasgo de seguridad pueden entonces no ser detectables por los detectores sencillos sino únicamente por detectores más complejos (segundo tipo). Por consiguiente, es posible incorporar diferentes niveles de seguridad en un único rasgo de seguridad.

35 Los niveles jerárquicos diferentes en el rasgo de seguridad pueden proporcionarse usando diferentes formas y/o tamaños y/o colores y/o números y/o distribuciones y/o patrones para las marcas de diferentes niveles del rasgo de seguridad. Por ejemplo, un tamaño menor (diámetro o área máxima) de las marcas adicionales puede hacer imposible detectar esas marcas con un detector bastante sencillo.

La invención también proporciona un objeto valioso u objeto de seguridad que comprende un rasgo de seguridad de acuerdo con la invención.

45 Ventajosamente, se proporciona un billete que comprende el rasgo de seguridad de acuerdo con aspectos de la invención.

50 La invención también proporciona un método de fabricación de un rasgo de seguridad de acuerdo con el aspecto de la invención. Un objeto o un componente y/o elemento y/o área y/o región y/o porción del objeto puede analizarse a continuación para una característica específica, como por ejemplo una apariencia física del objeto y/o el componente y/o elemento y/o región y/o área, y/o porción del objeto.

55 El objeto y/o el componente y/o elemento y/o región y/o área y/o porción del objeto está fabricado. Un elemento de seguridad puede a continuación aplicarse al objeto y/o al componente y/o elemento y/o región y/o área y/o porción del objeto, ya sea después de la fabricación del objeto o mientras se está fabricando.

El rasgo de seguridad puede estar adaptado por forma y/o tamaño y/o color y/o distribución y/o apariencia a la característica del objeto y/o el componente y/o elemento y/o región y/o área y/o porción del objeto.

60 Si la característica es un cierto patrón o conjunto de patrones, puede crear ventajosamente marcas adicionales para el rasgo de seguridad que tiene aproximadamente el mismo tamaño, forma y/o color (individualmente). Sin embargo, las marcas adicionales son ventajosamente menores en número que las marcas ya existentes (marcas originales). Puede usarse una codificación de canal para proporcionar una representación de información o datos predefinidos que son legibles por máquina y la apariencia física de los cuales es similar a una característica de un objeto (o un elemento de un objeto) al que se aplica el rasgo de seguridad.

La característica del objeto (o elemento del objeto) puede ser debido ventajosamente a un proceso de fabricación del objeto. La característica puede ser un efecto secundario o consecuencia inevitable del proceso de fabricación. La característica puede también ser un efecto deseado o apariencia física deseada del objeto. Este aspecto de la invención proporciona en general que el rasgo de seguridad no sea visible inmediatamente cuando se inspecciona el objeto por el ojo desnudo bajo luz ambiente normal (por ejemplo luz diurna).

**Breve descripción de los dibujos**

Resultarán ventajas y características adicionales de la invención a partir de la siguiente descripción de las realizaciones preferidas de la invención con referencia a los dibujos adjuntos, en los que

- La Figura 1 muestra una representación esquemática simplificada de un objeto que tiene características de producción específicas,
- la Figura 2 muestra el objeto de la Figura 1 que lleva el rasgo de seguridad de acuerdo con una realización de la invención,
- la Figura 3 muestra un diagrama de bloques simplificado de una realización de acuerdo con aspectos de la invención,
- la Figura 4 muestra un diagrama de bloques simplificado de una realización de acuerdo con aspectos de la invención,
- la Figura 5 muestra un diagrama de bloques simplificado de una realización de acuerdo con aspectos de la invención,
- la Figura 6 muestra un diagrama que ilustra aspectos de la invención,
- la Figura 7 muestra un diagrama de flujo que ilustra el procedimiento de creación de un rasgo de seguridad de acuerdo con aspectos de la invención,
- la Figura 8 es un diagrama esquemático simplificado de una realización de la invención,
- la Figura 9 es un diagrama esquemático simplificado de un aparato de detección, y
- la Figura 10 es un diagrama esquemático simplificado de una realización de la invención.

**Descripción detallada de realizaciones preferidas**

La Figura 1 muestra una representación esquemática simplificada de un objeto 1 que tiene una característica inherente. En la presente realización, esta característica es una pluralidad de marcas 2 que se crean durante la fabricación del objeto 1. Sin embargo, en general, estas marcas pueden ser cualquier clase de característica pretendida o no pretendida. En esta realización, las marcas originales 2 pueden ser, por ejemplo, uno cualquiera o varios de los siguientes: defectos y/o impurezas y/o partículas y/o orificios y/o fibras y/o pigmentos. Estas marcas o defectos pueden estar distribuidos aleatoriamente.

La Figura 2 muestra el objeto 1 de la Figura 1 de nuevo. Sin embargo, el objeto 1 ahora incluye marcas adicionales 3 que son similares a las marcas ya existentes (originales) 2 y también parecen estar distribuidas aleatoriamente. De acuerdo con este aspecto de la invención, el rasgo de seguridad se oculta usando una apariencia para las marcas 3 que es similar a la apariencia de las marcas originales 2. También las marcas 3 mismas pueden tener aproximadamente la misma forma, tamaño, color u otra característica para hacer que las marcas parezcan como las marcas 2. Ventajosamente, únicamente se añaden unas pocas marcas, de modo que la apariencia general de las marcas originales permanece sustancialmente sin variar. Si el número de marcas añadidas 3 es  $w$  y el número de marcas existentes es  $v$ , una relación ventajosa es  $w < v$  ( $w$  es menor que  $v$ ). La relación  $v/w$  puede ser ventajosamente mayor que 1, y en algunas realizaciones mayor que 10 o mayor que 20. En otras palabras, las marcas adicionales del rasgo de seguridad están adaptadas a las marcas existentes del objeto en términos de tamaño, forma, distribución, número y/o color etc. Esto mejora el disimulo del rasgo de seguridad. El rasgo de seguridad (es decir en esta realización, las marcas adicionales del rasgo de seguridad) se mezcla en el área, región y/o porción del objeto en el que se crean las marcas adicionales.

La localización y/o forma y/o color y/o distribución de las marcas adicionales representa o representan información (datos) legible por máquina predeterminada. Están adaptados a la característica (marcas preexistentes debido a fabricación) del objeto (o un elemento de un objeto) al que se aplica el rasgo de seguridad. La característica del objeto (o elemento del objeto) puede ser debido ventajosamente a un proceso de fabricación del objeto. La característica puede ser un efecto secundario o consecuencia inevitable del proceso de fabricación. La característica puede también ser un efecto deseado o apariencia física deseada del objeto. El rasgo de seguridad es, al menos no inmediatamente

visible cuando se inspecciona el objeto por el ojo desnudo.

La Figura 3 muestra un diagrama simplificado de una realización de acuerdo con aspectos de la invención. En esta realización, los datos sin procesar 4 se procesan de acuerdo con un algoritmo de codificación de canal para generar los datos codificados de canal 6. Los datos codificados de canal 6 tienen la apariencia física necesaria para ocultar los datos codificados de canal en el objeto 1. Se describen a continuación realizaciones ventajosas de la codificación de canal.

La Figura 4 muestra un diagrama simplificado de una realización de la invención de acuerdo con aspectos de la invención. En esta realización, los datos sin procesar 4 se procesan en primer lugar de acuerdo con un algoritmo de corrección de errores (por ejemplo corrección de errores de Reed-Solomon) para generar los datos codificados de corrección de errores 8. Estos datos codificados de corrección de errores 8 se procesan a continuación de acuerdo con el algoritmo de codificación de canal 5 para generar los datos codificados de canal 6. El proceso de corrección de errores adicional puede usarse ventajosamente para incorporar datos redundantes en los datos sin procesar. Estos datos redundantes o adicionales pueden servir para detectar y/o corregir errores durante un proceso de lectura de los datos codificados de canal 6. El algoritmo Reed-Solomon es bien conocido en la técnica y la cantidad de datos redundantes puede adaptarse a los requisitos específicos de la aplicación.

La Figura 5 muestra un diagrama simplificado de una realización de acuerdo con aspectos de la invención. Los datos sin procesar 4 se procesan en primer lugar de acuerdo con un algoritmo de encriptación (como por ejemplo AES - norma de encriptación avanzada) en el que se usa por ejemplo una clave. Los datos encriptados 10 se procesan a continuación de acuerdo con el algoritmo de corrección de errores 7 (como se ha descrito anteriormente). Los datos codificados de corrección de errores 8 se procesan a continuación con un algoritmo de codificación de canal 5 para obtener los datos codificados de canal 6 (como se ha descrito anteriormente).

En otras palabras, la información o datos predeterminados que se representan por el rasgo de seguridad pueden ser datos encriptados sin procesar. Cualquier información/datos predeterminados (típicamente datos digitales) puede entonces encriptarse antes de que se codifique por canal. Esto aumenta la seguridad del rasgo. Adicionalmente, puede aplicarse un algoritmo de corrección de errores, como el algoritmo Reed-Solomon a los datos para hacer posible detectar y/o corregir errores de detección/lectura.

La Figura 6 muestra un diagrama simplificado que ilustra el proceso de codificación de canal 5. Simplemente como un ejemplo simplificado, puede haber números binarios 1011 (11) que representan cualquiera de los datos sin procesar 4, los datos codificados de corrección de errores 8 o los datos encriptados 10. Esta palabra de múltiples bits 1011 puede únicamente ser una parte de un flujo de datos largo que incluye una pluralidad de palabras de múltiples bits. Para cada palabra de múltiples bits del flujo de datos (en este ejemplo 4 bits) se genera un símbolo específico y se asigna a esta palabra de múltiples bits. En el presente ejemplo, la palabra de bits 1011 como el símbolo específico 11. Las marcas 31, 32 tienen un tamaño, forma y localización específicos en una cierta área, campo, región y/o porción del objeto 1. La palabra de múltiples bits 1100 (12) puede entonces ser otra palabra de múltiples bits del flujo de datos a procesarse. Como se ha descrito anteriormente, este flujo de datos, puede ser los datos sin procesar 4, los datos codificados de corrección de errores 8 o los datos encriptados 10. La palabra de múltiples bits 1100 también tiene un símbolo predeterminado específico 11 con marcas 33 y 34. Todas las marcas 31, 32, 33 y 34 están sustancialmente adaptadas para tener la apariencia física de marcas ya presentes en un objeto 1. Adicionalmente, la distribución de las marcas 31, 32 y 33, 34 en un área específica así como el número de las marcas 31, 32, 33 y 34 en el área específica pueden estar adaptados también a las características del objeto 1 dadas. En otras palabras, también los bloques (área de símbolos) pueden adaptarse para ocultar las marcas adicionales. Cada palabra de múltiples bits (en caso de una palabra de 4 bits hay  $2^4=16$  diferentes palabras de múltiples bits), puede generarse un símbolo específico que es ventajosamente diferente de todos los otros símbolos. Para aumentar la fiabilidad y para reducir la tasa de error durante la detección, el número de las marcas en cada símbolo 11 puede aumentarse siempre que no se deteriore el disimulo del rasgo de seguridad.

El proceso de asignación de marcas adicionales/grupos de marcas adicionales/símbolos a los datos/información predeterminados de manera que la apariencia física del rasgo de seguridad sea similar a una característica física específica del objeto es el proceso de codificación de canal. Las marcas/grupos de marcas/símbolos están entonces dispuestos apropiadamente en el objeto mientras se tiene cuidado de que la apariencia física de las marcas preexistentes (la característica existente) no se vea afectada.

Las marcas originales pueden ser debido al proceso de fabricación del objeto. Las marcas originales están distribuidas aleatoriamente. La característica original del objeto se imita añadiendo marcas/grupos de marcas/símbolos sin cambiar sustancialmente la apariencia física original del objeto. Las marcas originales pueden ser defectos y/o impurezas y/o partículas y/u orificios y/o fibras y/o pigmentos, etc., el rasgo de seguridad puede comprender entonces marcas adicionales que tienen una apariencia similar que las marcas originalmente existentes. Las marcas adicionales pueden ser similares a las marcas originales en términos de tamaño, forma, número, distribución, color, etc. Cada uno de estos aspectos de la invención mejora adicionalmente el disimulo del rasgo de seguridad. Todas las características preexistentes o marcas preexistentes pueden ser sustancialmente invisibles al ojo desnudo. Esto significa que las marcas no son evidentes cuando se inspeccionan por el ojo desnudo sin usar una lupa, un microscopio u otros medios

de inspección. Las marcas adicionales pueden entonces tener la misma apariencia y también ser sustancialmente invisibles al ojo desnudo. La localización (relativa y/o absoluta), tamaño y/o forma y/o color de las marcas adicionales individuales etc., se usa para almacenar la información legible predeterminada por máquina en el objeto.

5 Un grupo de marcas o un símbolo puede identificarse más fácilmente que una única marca. Un grupo o símbolo puede estar basado ventajosamente en información redundante. Cuanto más redundante sea la información de un símbolo o grupo de marcas, menor será la tasa de error durante la lectura de la información.

10 Todos los parámetros y propiedades detectables de las marcas, sean individuales, sean con respecto entre sí (localización/posición relativa) o con respecto al objeto pueden usarse ventajosamente para representar información (datos).

15 Cada uno de los grupos de marcas/símbolos tiene un número predeterminado de marcas. El número de marcas por grupo puede ser, por ejemplo,  $n$  (siendo  $n$  un número entero positivo). En realizaciones ventajosas  $n = 1, 2, 3, 4, 5, 6$  o mayor. En la presente realización,  $n$  es igual a 2 ( $n=2$ ).

El número de bits de la palabra de múltiples bits puede ser  $j$  (siendo  $n$  un número entero positivo). En esta realización,  $j$  es igual a 4 ( $j=4$ ). Sin embargo, también es posible elegir  $j = 2, 3, 4, 5, 6, 7, 8, 9, 10$  o mayor.

20 Aunque el número de marcas adicionales por símbolo puede ser igual al número de bits de la palabra de múltiples bits, en la presente realización, el número de marcas adicionales por grupo es diferente del número de bits de la palabra de múltiples bits que se representa por el grupo de marcas adicionales. En otras palabras, una marca adicional no representa necesariamente un único bit.

25 Dos o más símbolos diferentes pueden usarse para la palabra de múltiples bits. Esto es ventajoso ya que se aumenta entonces la redundancia en el rasgo de seguridad adicionalmente mientras se mejora también la apariencia aleatoria. Uno de los múltiples posibles símbolos se selecciona a continuación aleatoriamente y se dispone en el objeto.

30 La Figura 7 muestra un diagrama de flujo simplificado que ilustra el proceso de generación del rasgo de seguridad durante el proceso de codificación de canal. En la etapa S1 se pasan datos de entrada al proceso de la codificación de canal. Simplemente como un ejemplo, se indica un flujo de datos 4, 8, 10 al lado de la derecha de la etapa S1. En la etapa S2, se selecciona una palabra de múltiples bits (en este ejemplo 4 bits) del flujo de datos. En la etapa S3, se selecciona un símbolo específico para la palabra de múltiples bits específica. En la etapa S3 puede usarse un conjunto predefinido de símbolos que se genera en un generador de símbolos. Pueden usarse diferentes conjuntos de símbolos  
35 en un único objeto (dependiendo del número de rasgos de seguridad presentes en el objeto) o para diferentes objetos.

También es posible usar el rasgo de seguridad de acuerdo con aspectos de la invención jerárquicamente. Esto significa que un rasgo de seguridad puede tener diferentes niveles de modo que un primer nivel es detectable por detectores bastante sencillos. Algunas marcas proporcionadas en el rasgo de seguridad pueden entonces no ser detectables por  
40 los detectores sencillos sino únicamente por detectores más sofisticados. Por consiguiente, es posible incorporar diferentes niveles de seguridad en un único rasgo de seguridad.

Para definir una codificación de canal apropiada (definición de las propiedades del rasgo de seguridad), un objeto 1 o un componente, elemento, área, región y/o porción del objeto puede a continuación analizarse para una característica  
45 específica, como por ejemplo una apariencia física del objeto y/o el componente, elemento, región, área, y/o porción del objeto. El elemento de seguridad puede a continuación aplicarse al objeto y/o al componente, elemento, región, área, y/o porción del objeto, ya sea después de fabricar el objeto y/o el componente, elemento, región, área, y/o porción del objeto, mientras se fabrica el objeto y/o el componente, elemento, región, área, y/o porción del objeto, o después de fabricar el objeto y/o el componente, elemento, región, área, y/o porción del objeto  
50

La Figura 8 muestra un diagrama simplificado de una realización de la invención. En la presente realización, el objeto 1 es un documento valioso, y más específicamente un billete. En otras realizaciones, el objeto 1 al que se aplica el rasgo de seguridad puede ser un objeto valioso, un objeto de seguridad, un producto de consumidor, un documento de seguridad, un certificado (por ejemplo de nacimiento, residencia, estado marital, nombre, etc.), una copia certificada  
55 de un documento, una tarjeta, como por ejemplo una tarjeta inteligente, una tarjeta de acceso, una tarjeta de crédito, una tarjeta de bonificación, una tarjeta de identidad, un pasaporte, etc.

60 El rasgo de seguridad se incorpora en la banda o parche metalizado 15 (por ejemplo una capa, hoja o lámina que tiene una capa metálica fina) del documento valioso (billete). En otras palabras el elemento del objeto 1 al que se aplica el rasgo de seguridad, puede ser la banda o parche metalizado.

En esta realización, el rasgo de seguridad es una estructura escrita con láser. Las marcas añadidas 3 del rasgo de seguridad son desmetalizaciones con tamaño micrométrico locales. La capa metálica (u otra) de las bandas metalizadas de billetes (y otros documentos) tiene defectos en forma de pequeños orificios que parecen estar  
65 distribuidos aleatoriamente a través de la banda. El rasgo de seguridad se extiende a través de la totalidad de la banda añadiendo las marcas adicionales 3 en forma de orificios. Estos orificios se generan por un láser (no mostrado) y

parecen como todos los otros puntos desmetalizados que son debido al proceso de fabricación. El rasgo de seguridad se escribe usando un sistema litográfico de láser de alta resolución que permite desmetalización directa de capas metálicas finas.

5 La desmetalización tiene tamaños de punto muy pequeños (únicamente unos pocos micrómetros, como por ejemplo 1, 2, 3, 4 hasta 10, 16 o 20  $\mu\text{m}$ ) y una precisión posicional muy alta de por ejemplo 0,1, 0,2 hasta 0,5  $\mu\text{m}$ . No se muestran las marcas originales (puntos/orificios) que también están presentes en la banda.

10 El rasgo de seguridad únicamente comprende unos pocos puntos con tamaño de micrómetro adicionales que aparecen distribuidos aleatoriamente. Si estos puntos son suficientemente pequeños, no pueden observarse con el ojo desnudo, ni en reflejo ni en transmisión. Incluso con una lupa o microscopio, los puntos no pueden detectarse en modo de reflejo por el ojo desnudo. Únicamente en modo de transmisión y por el uso de un microscopio, pueden identificarse los puntos.

15 El número de puntos (marcas adicionales) por área de la banda puede ser entonces muy bajo. En esta realización, el número total de puntos en la banda entera o en un campo de datos puede encontrarse entre 100 y 200 (la Figura 8 es únicamente un dibujo simplificado). Esto mejora el disimulo del rasgo.

20 Las posiciones de las marcas en cada símbolo están distribuidas aleatoriamente (pseudo-aleatoriamente). Las marcas (o puntos) parecen entonces como un patrón aleatorio similar a los defectos originales en las bandas de lámina metalizada de los documentos valiosos tales como billetes.

Una composición individual o conjunto de símbolos puede usarse para cada objeto (billete).

25 Las marcas añadidas están dispuestas en grupos (símbolos) 11 como se ha descrito anteriormente y los grupos/símbolos 11 están dispuestos en la banda metalizada del documento valioso. Se determina un área específica en la que se hallan las (todas) marcas de un grupo/símbolo. Esta área se denomina como un bloque. Todos los bloques del rasgo de seguridad pueden entonces estar dispuestos lado a lado (no solapantes). Esto simplifica la detección. También es posible una disposición solapante de los bloques. Un bloque puede ser un área rectangular. Sin embargo, en otra realización, pueden usarse diferentes formas de un bloque.

30 Puede combinarse un cierto número de bloques. Esta combinación de bloques se denomina como un campo de datos 12. Un único campo de datos 12 puede entonces llevar toda la información/datos almacenados. El campo de datos puede repetirse a lo largo de la banda (en este punto tres veces). Esto aumenta adicionalmente la redundancia y por lo tanto la robustez del rasgo de seguridad. Si se destruye uno de los campos de datos, puede usarse otro campo de datos para leer los datos/información almacenados en el rasgo de seguridad. Cada campo de datos puede usar diferentes símbolos o conjuntos de símbolos para los mismos datos. Esto proporciona que la banda 15 no muestre ninguna regularidad (repetición de patrones).

35 Por ejemplo, un código de error de Reed-Solomon  $RS(m,k)$  transforma  $k$  símbolos de datos en  $j$  bits añadiendo  $2 \cdot t$  símbolos de paridad de  $j$  bits. El resultado es  $m$  símbolos de  $j$  bits. En la etapa de decodificación pueden detectarse y corregirse  $t=(m-k)/2$  símbolos incorrectos.

40 En general, el número de bits a almacenarse en el rasgo depende del algoritmo de corrección de errores usado y del número de errores que han de detectarse y/o corregirse.

45 De acuerdo con una realización de la invención, pueden incorporarse datos de usuario individuales en el billete. Si por ejemplo, la capacidad de almacenamiento del usuario del rasgo de seguridad es  $x$  bits ( $k$  múltiples palabras de bits de  $j$  bits, es decir  $x=k \cdot j$ ), es posible incorporar por ejemplo un número de serie que puede representarse por  $y$  bits, mientras que  $y$  es igual o inferior a  $x$ . Los datos pueden ser un número de serie del documento valioso. En otra realización, únicamente puede usarse una parte de los datos de usuario (por ejemplo para un número de serie) y los restantes  $z=x-y$  bits pueden usarse para otra información.

50 Un ejemplo que incluye corrección de errores (Reed-Solomon) puede tener la siguiente estructura de datos:

- 55
- Número de bits por palabra de múltiples bits (=símbolo):  $j = 4$
  - Información de usuario:  $x = 12 \cdot 4$  bits = 48 bits de usuario ( $k = 12$ )
  - 60 - Corrección de errores (Reed-Solomon): 48 bits de usuario + 48 bits (paridad) = 96 bits de error codificados ( $t=6$  incorrectos 4-bits-símbolos pueden corregirse)

65 Los datos almacenados en el rasgo de seguridad en la banda pueden ser datos de usuario individuales. Si por ejemplo, la capacidad de almacenamiento del rasgo de seguridad es  $x$  bits de datos ( $k$  palabras de múltiples bits de  $j$  bits), es posible incorporar por ejemplo un número de serie que puede representarse por  $y$  bits, y  $y \leq x$ . En esta realización, los datos son el número de serie del documento valioso (billete). Únicamente se usa una parte de los  $x$  bits para el

número de serie y los restantes  $z = x - y$  bits se usan para otra información.

Los datos de usuario individuales a almacenarse en el rasgo de seguridad, pueden ser el número de serie 18, pero también un número de lote, una denominación, un país de producción, un año de producción u otra información.

5 La información adicional/datos almacenados en el rasgo de seguridad pueden ser datos estadísticos u otros rasgos del documento valioso. Esto puede a continuación conducir a la posibilidad de correlacionar rasgos de seguridad o datos del documento valioso. Usar correlación puede mejorar el nivel de seguridad contra copiado y falsificación.

10 Los datos/información adicional pueden indicar variaciones de producción del objeto 1. Estas variaciones de producción pueden comprender propiedades como densidad óptica, alineación, distorsiones geométricas, agudeza de bordes, orificios, etc.

15 Los datos/información en el rasgo de seguridad pueden estar correlacionados con otro rasgo de seguridad del objeto. Este otro rasgo de seguridad puede ser una impresión UV (ultravioleta), magnética o de infrarrojos (IR).

20 Dos símbolos 11 de un conjunto de símbolos (por ejemplo todos los símbolos de un campo de datos en este ejemplo) nunca comparten ninguna marca. Esto significa que las marcas adicionales de dos símbolos nunca están en la misma localización y/o las marcas adicionales de símbolos diferentes pueden variar también en forma y/o tamaño.

25 El número de marcas por símbolo puede aumentarse siempre que la apariencia física del objeto no se vea afectada (al menos no por encima de un nivel que haga diez marcas adicionales visibles al ojo desnudo). Esto reduce la tasa de error ya que un símbolo aún puede detectarse correctamente y leerse, incluso si no todas las marcas fueran legibles. La detección se hace más robusta, cuantas más marcas se usan por símbolo.

Las posiciones de las marcas en los símbolos se eligen aleatoriamente. El rasgo de seguridad de cada billete se calcula individualmente. Esto proporciona una estructura individual única para cada objeto 1 (billete).

30 De acuerdo con un aspecto de la invención, puede proporcionarse un marcado adicional 13, 14 o estructura en el objeto 1 que lleva el rasgo de seguridad. El marcado adicional 13, 14 sirve para alinear el objeto con un detector para leer el rasgo de seguridad.

35 En esta realización de la invención, el objeto 1 comprende un primer marcado adicional 13 para alineación aproximada y un segundo marcado adicional 14 para alineación precisa. El segundo marcado 14 (para alineación precisa) se fabrica por las mismas etapas de fabricación y/o dispositivos usados para las marcas adicionales 3 del rasgo de seguridad.

40 En otras palabras, el láser usado para las marcas adicionales puede usarse también para el segundo marcado 14. Esto proporciona que se consiga la misma precisión para las marcas adicionales 14.

La Figura 9 muestra un dibujo simplificado que ilustra la detección del rasgo de seguridad. El rasgo de seguridad se lee con un sensor especializado o aparato de detección.

45 Con respecto a la realización anteriormente descrita que usa la banda o parche y puntos desmetalizados, el rasgo de seguridad puede leerse usando una disposición óptica que incluye por ejemplo una fuente de luz 16 y un microscopio 17 (que incluye una cámara). Una fuente de luz 16 puede estar localizada detrás del documento valioso (en la parte trasera) y el microscopio 17 (que incluye una cámara) está localizado en el lado opuesto del documento valioso (parte delantera). Las marcas adicionales 3 del rasgo de seguridad pueden ser un poco mayores (en diámetro máximo o área en sección transversal) que las marcas/puntos originales, de manera que los puntos desmetalizados parecen un poco más brillantes que el fondo.

50 Se toma una imagen (por la cámara interna 17) del área donde está localizado el rasgo de seguridad. La imagen se procesa a continuación (procesamiento de imagen). Puesto que las localizaciones de marcas añadidas son conocidas, el algoritmo de reconocimiento de patrón puede buscar directamente las marcas adicionales específicas. Si se detectan las marcas, se confirma la autenticidad del objeto. Debido a redundancia, puede confirmarse también la autenticidad, si únicamente se detectan unas pocas y no todas las marcas adicionales.

60 La robustez de la codificación permite lectura muy estable del rasgo de seguridad a velocidades de transporte altas del documento valioso, en particular de billetes. La misma estructura básica del elemento de seguridad puede usarse en diferentes documentos valiosos.

Cada símbolo puede estar localizado en un área específica, región o porción del objeto.

65 De acuerdo con otro aspecto más de la invención el rasgo de seguridad está organizado jerárquicamente. Esto significa que un rasgo de seguridad puede tener diferentes niveles de modo que un primer nivel es detectable por detectores bastante sencillos. Algunas marcas proporcionadas en el rasgo de seguridad pueden entonces no ser detectables por

los detectores sencillos sino únicamente por detectores más sofisticados. Por consiguiente, es posible incorporar diferentes niveles de seguridad en un único rasgo de seguridad.

5 Los niveles jerárquicos diferentes en el rasgo de seguridad pueden proporcionarse usando diferentes formas, tamaños, colores, números, distribuciones y/o patrones para las marcas de diferentes niveles del rasgo de seguridad. Por ejemplo, un tamaño menor de las marcas puede hacer imposible detectar estas marcas con un detector bastante sencillo.

10 La Figura 10 muestra otra realización de la invención. En esta realización, se añaden marcas adicionales a una hoja o capa o superficie de un objeto. No hay marcas originales. Las marcas adicionales están adaptadas a una característica del objeto. Las marcas adicionales pueden estar adaptadas en una cualquiera de las siguientes características para no ser visibles al ojo desnudo: distribución y/o tamaño y/o la forma y/o el color. La información legible por máquina predeterminada puede entonces representarse por las localizaciones relativas y/o tamaños y/o formas y/o colores de las marcas adicionales. La codificación de error y/o codificación de canal así como la encriptación  
15 pueden entonces realizarse como se describe con respecto a las otras realizaciones de la invención. Las marcas adicionales pueden estar dispuestas en bloques (área limitada predefinida). Estos bloques pueden ser solapantes o no solapantes. Los bloques pueden tener una forma predeterminada como por ejemplo rectangular o circular, etc.

20 En la presente realización, esta característica es la apariencia de la superficie de un objeto 1, como por ejemplo una hoja de papel o plástico.

25 El objeto 1 incluye marcas adicionales 3 que parecen estar distribuidas aleatoriamente. El rasgo de seguridad está oculto por la apariencia aleatoria de las marcas. Las marcas adicionales 3 pueden estar también adaptadas en tamaño y número por área (distribución) para ocultarse al ojo visible. Ventajosamente, únicamente se añaden unas pocas marcas, de modo que la apariencia general de la superficie del objeto 1 permanece sustancialmente sin variar. Las marcas adicionales del rasgo de seguridad se mezclan en el área, región y/o porción del objeto en los que se crean las marcas adicionales.

30 La localización y/o forma y/o color y/o distribución de las marcas adicionales representa o representan información (datos) legible por máquina predeterminada. Están adaptadas a la característica del objeto (o un elemento de un objeto) al que se aplica el rasgo de seguridad. La característica (color, etc.) del objeto 1 (o elemento del objeto) puede ser debido ventajosamente a un proceso de fabricación del objeto 1. La característica puede ser un efecto secundario o consecuencia inevitable del proceso de fabricación. La característica puede también ser un efecto deseado o apariencia física deseada del objeto. El rasgo de seguridad es, al menos no inmediatamente visible cuando se  
35 inspecciona el objeto por el ojo desnudo.

40 Similar a las otras realizaciones de la invención, los datos sin procesar 4 pueden procesarse de acuerdo con un algoritmo de codificación de canal para generar los datos codificados de canal 6. Los datos codificados de canal 6 tienen la apariencia física necesaria para ocultar los datos codificados de canal en el objeto 1.

45 En esta realización, los datos sin procesar 4 pueden procesarse en primer lugar de acuerdo con un algoritmo de corrección de errores (por ejemplo corrección de errores de Reed-Solomon) para generar los datos codificados de corrección de errores 8. Estos datos codificados de corrección de errores 8 pueden a continuación procesarse de acuerdo con el algoritmo de codificación de canal 5 para generar los datos codificados de canal 6. El proceso de corrección de errores adicional puede usarse ventajosamente para incorporar datos adicionales en los datos sin procesar. Estos datos redundantes o adicionales pueden a continuación servir para detectar y/o corregir errores durante un proceso de lectura (proceso de detección) de los datos codificados de canal 6. Los algoritmos de corrección de errores, como por ejemplo el algoritmo Reed-Solomon, son bien conocidos en la técnica y la cantidad de datos redundantes pueden estar adaptados a los requisitos específicos de la aplicación.  
50

55 Los datos sin procesar 4 pueden procesarse también de acuerdo con un algoritmo de encriptación (como por ejemplo AES - norma de encriptación avanzada) en la que por ejemplo se usa una clave de encriptación antes de que se aplique el algoritmo de corrección de errores. Los datos encriptados 10 pueden a continuación procesarse de acuerdo con el algoritmo de corrección de errores 7 (como se ha descrito anteriormente). Los datos codificados de corrección de errores 8 se procesan a continuación usando un algoritmo de codificación de canal 5 para obtener los datos codificados de canal 6 (como se ha descrito anteriormente).

60 En otras palabras, la información o datos predeterminados que se representan por el rasgo de seguridad pueden ser datos encriptados sin procesar. Cualquier información/datos predeterminados (típicamente datos digitales) puede entonces encriptarse antes de que se codifique por canal. Esto aumenta la seguridad del rasgo. Adicionalmente, puede aplicarse un algoritmo de corrección de errores, como por ejemplo el algoritmo Reed-Solomon, a los datos para hacer posible detectar y/o corregir errores de detección/lectura.

65 Un proceso de codificación de canal 5 ventajoso se muestra en la Figura 6, que puede aplicarse también a la realización de la Figura 10. El proceso de asignación de marcas/grupos de marcas/símbolos a los datos/información predeterminados de manera que la apariencia física del rasgo de seguridad es similar a una característica física

específica del objeto es el proceso de codificación de canal. Las marcas/grupos de marcas/símbolos están entonces dispuestos apropiadamente en el objeto mientras se tiene cuidado de que la apariencia física de la característica existente de la superficie del objeto no se vea afectada hasta un punto que las marcas adicionales se hagan visibles al ojo desnudo. La característica preexistente puede ser sustancialmente invisible al ojo desnudo.

5 Un grupo de marcas adicionales o un símbolo pueden detectarse más fácilmente que una única marca. Un grupo o símbolo puede estar basado ventajosamente en información redundante. Cuanto más redundante sea la información de un símbolo o grupo de marcas, menor será la tasa de error durante la lectura de la información.

10 Todos los parámetros y propiedades detectables de las marcas adicionales (añadidas), sean individuales, sean con respecto entre sí o con respecto al objeto pueden usarse ventajosamente para representar información (datos).

15 Cada uno de los grupos de marcas/símbolos tiene un número predeterminado de marcas. El número de marcas por grupo puede ser, por ejemplo,  $n$  (siendo  $n$  un número entero positivo). En realizaciones ventajosas  $n = 1, 2, 3, 4, 5, 6$  o mayor. En la presente realización  $n=2$ .

20 El número de marcas por símbolo puede ser igual al número de bits de la palabra de múltiples bits o el número de marcas por grupo puede ser diferente del número de bits de la palabra de múltiples bits que se representa por el grupo de marcas. En otras palabras, una marca no representa necesariamente un único bit.

25 Dos o más símbolos diferentes pueden usarse para la misma palabra de múltiples bits. Esto es ventajoso ya que se aumenta adicionalmente entonces la redundancia en el rasgo de seguridad mientras que se mejora la apariencia aleatoria. Uno de los múltiples posibles símbolos se selecciona a continuación aleatoriamente y se dispone en el objeto.

Este proceso de codificación de canal mostrado en la Figura 7 puede aplicarse también a la realización mostrada en la Figura 10.

30 También es posible usar el rasgo de seguridad de acuerdo con aspectos de la invención jerárquicamente. Esto significa que un rasgo de seguridad puede tener diferentes niveles de modo que un primer nivel es detectable por detectores bastante sencillos. Algunas marcas proporcionadas en el rasgo de seguridad pueden entonces no ser detectables por los detectores sencillos sino únicamente por detectores más sofisticados. Por consiguiente, es posible incorporar diferentes niveles de seguridad en un único rasgo de seguridad.

35 Para definir una codificación de canal apropiada (definición de las propiedades del rasgo de seguridad), un objeto 1 o un componente, elemento, área, región y/o porción del objeto puede a continuación analizarse para una característica específica, como por ejemplo una apariencia física del objeto y/o el componente, elemento, región, área, y/o porción del objeto. El elemento de seguridad puede entonces aplicarse al objeto y/o al componente, elemento, región, área, y/o porción del objeto, ya sea después de fabricar el objeto y/o el componente, elemento, región, área, y/o porción del objeto, mientras se fabrica el objeto y/o el componente, elemento, región, área, y/o porción del objeto.

45 El objeto 1 al que se aplica el rasgo de seguridad puede ser un objeto valioso, un objeto de seguridad, un producto de consumidor, un documento de seguridad, un certificado (por ejemplo de nacimiento, residencia, estado marital, nombre, etc.), una copia certificada de un documento, una tarjeta, como por ejemplo una tarjeta inteligente, una tarjeta de acceso, una tarjeta de crédito, una tarjeta de bonificación, una tarjeta de identidad, un pasaporte, etc.

50 El rasgo de seguridad puede aplicarse a la superficie en forma de puntos u orificios o fibras. Estos puntos u orificios o fibras a continuación forman las marcas adicionales. En la presente realización, las marcas son puntos impresos. Las marcas añadidas 3 del rasgo de seguridad son puntos con tamaño micrométrico. Las marcas añadidas parecen distribuidas aleatoriamente a través de la superficie del objeto. El rasgo de seguridad puede extenderse a través de la superficie total del objeto añadiendo las marcas adicionales 3 en forma de puntos.

55 El tamaño (diámetro) de punto de las marcas adicionales 3 puede ser de unos pocos micrómetros, como por ejemplo 1, 2, 3, 4 hasta 10, 16 o 20  $\mu\text{m}$ , el rasgo de seguridad únicamente comprende unos pocos puntos de tamaño micrométrico adicionales que parecen distribuidos aleatoriamente. Si estos puntos son suficientemente pequeños, no pueden observarse con el ojo desnudo, ni en reflejo ni en transmisión. Incluso con una lupa o microscopio, los puntos no pueden detectarse.

60 El número de puntos por área de la superficie del objeto puede entonces ser muy bajo. Las posiciones de las marcas en cada símbolo (bloque) están distribuidas pseudo-aleatoriamente, que significa que están predeterminadas pero parecen estar distribuidas aleatoriamente. Las marcas (o puntos) entonces parecen como un patrón aleatorio.

Una composición individual o conjunto de símbolos puede usarse para cada objeto (billete).

65 Las marcas añadidas están dispuestas en grupos (símbolos) 11 como se ha descrito anteriormente y los grupos/símbolos 11 están dispuestos en la superficie del objeto 1. Se determina un área específica en la que se hallan

5 las (todas) marcas de un grupo/símbolo, que se denomina como un bloque. Todos los bloques del rasgo de seguridad pueden entonces estar dispuestos lado a lado (no solapantes). También es posible una disposición solapante de los bloques. Un bloque puede ser un área rectangular. Sin embargo, en otra realización, pueden usarse diferentes formas de un bloque. Los bloques pueden combinarse hasta un campo de datos 12 como se ha descrito anteriormente. Un  
10 único campo de datos 12 puede entonces llevar toda la información/datos almacenados. El campo de datos puede repetirse a través de la superficie del objeto. Esto aumenta adicionalmente la redundancia y por lo tanto la robustez del rasgo de seguridad. Si se destruye uno de los campos de datos 12, puede usarse otro campo de datos para leer los datos/información almacenados en el rasgo de seguridad. Cada campo de datos puede usar diferentes símbolos o conjuntos de símbolos para los mismos datos. Esto proporciona que la superficie del objeto 1 no muestre regularidad alguna (repetición de patrones).

15 El objeto 1 comprende un primer marcado adicional 13 para alineación aproximada y un segundo marcado adicional 14 para alineación precisa. El segundo marcado 14 (para alineación precisa) está fabricado ventajosamente por las mismas etapas de fabricación y/o dispositivos (es decir, por ejemplo, la misma impresora, etc.) usados para las marcas adicionales 3 del rasgo de seguridad.

En otras palabras, el láser puede usarse también para el segundo marcado 14. Esto proporciona que se consiga la misma precisión para las marcas adicionales 14.

20 Pueden aplicarse algoritmos de corrección de errores y/o algoritmos de encriptación como se ha descrito anteriormente con respecto a otras realizaciones de la invención. La información adicional/datos almacenados en el rasgo de seguridad pueden ser datos estadísticos u otros rasgos del objeto 1. Esto puede conducir a continuación a la posibilidad de correlacionar rasgos de seguridad o datos del objeto 1. Usar correlación de datos como se ha descrito anteriormente puede mejorar el nivel de seguridad contra copiado y falsificación.

25 Todos los otros aspectos y características de la invención pueden aplicarse también a esta realización de la invención.

**REIVINDICACIONES**

- 5 1. Un método de fabricación de un objeto que comprende un rasgo de seguridad que almacena datos legibles por máquina predeterminados y que están adaptados a una característica inherente del objeto (1) al que se aplica el rasgo de seguridad, **en el que**
- la característica del objeto (1) es una pluralidad de marcas originales (2) en la que
  - las marcas originales (2) son una consecuencia del proceso de fabricación del objeto (1),
  - en el que el rasgo de seguridad comprende adicionalmente marcas adicionales (3),
  - 10 - las marcas adicionales representan los datos legibles por máquina predeterminados y tienen una apariencia similar que las marcas originales (2),
- caracterizado por que**
- 15 dichas marcas adicionales (3) se aplican al objeto (1) después de que el proceso de fabricación del objeto ha creado las marcas originales (2).
- 20 2. El método de acuerdo con la reivindicación 1, en el que las marcas adicionales (3) son similares a las marcas originales (2) en términos de tamaño, forma, y/o color.
3. El método de acuerdo con la reivindicación 1 o 2, en el que las marcas adicionales (3) y las marcas originales (2) son sustancialmente invisibles al ojo desnudo.
- 25 4. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos legibles por máquina predeterminados se representan por las localizaciones relativas y/o absolutas, tamaños, formas y/o colores de las marcas adicionales (3).
5. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que las marcas adicionales (3) están dispuestas en grupos (11).
- 30 6. El método de acuerdo con la reivindicación 5, en el que cada grupo (11) de marcas adicionales (3) representa una palabra de múltiples bits de los datos legibles por máquina predeterminados.
7. El método de acuerdo con una cualquiera de las reivindicaciones 5 o 6, en el que dos o más grupos diferentes (11) representan la misma palabra de múltiples bits.
- 35 8. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos legibles por máquina predeterminados están encriptados.
9. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos legibles por máquina predeterminados están codificados con error.
- 40 10. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que las marcas adicionales (3) se escriben por un láser o se imprimen.
- 45 11. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que las marcas adicionales (3) del rasgo de seguridad son desmetalizaciones con tamaño micrométrico locales y/o las marcas adicionales (3) están localizadas en una banda o parche metalizado de un documento valioso.
- 50 12. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos legibles por máquina predeterminados comprenden datos de usuario individuales.
13. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los datos legibles por máquina predeterminados están correlacionados con datos relacionados con el objeto (1).
- 55 14. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende adicionalmente un marcado adicional (14) para alineación precisa.
- 60 15. El método (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el objeto es un billete.

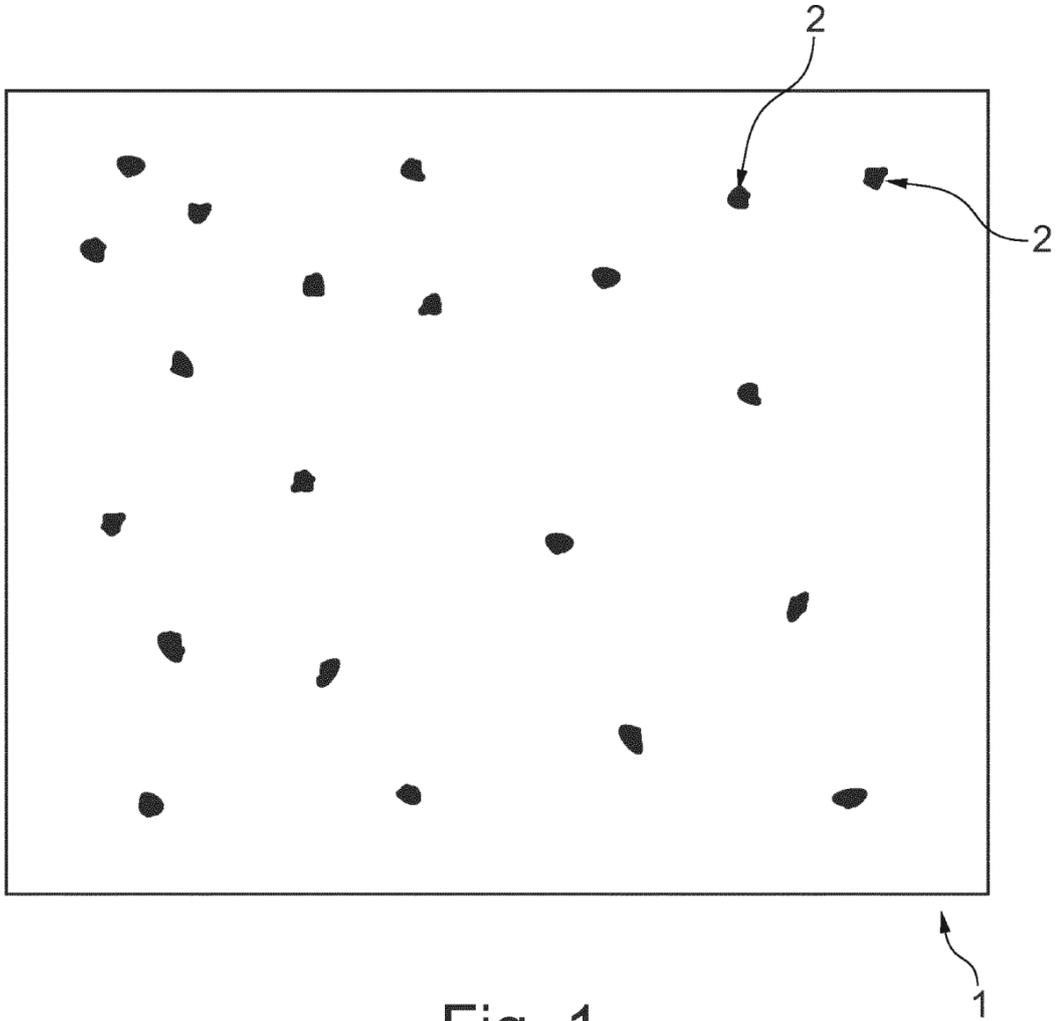


Fig. 1

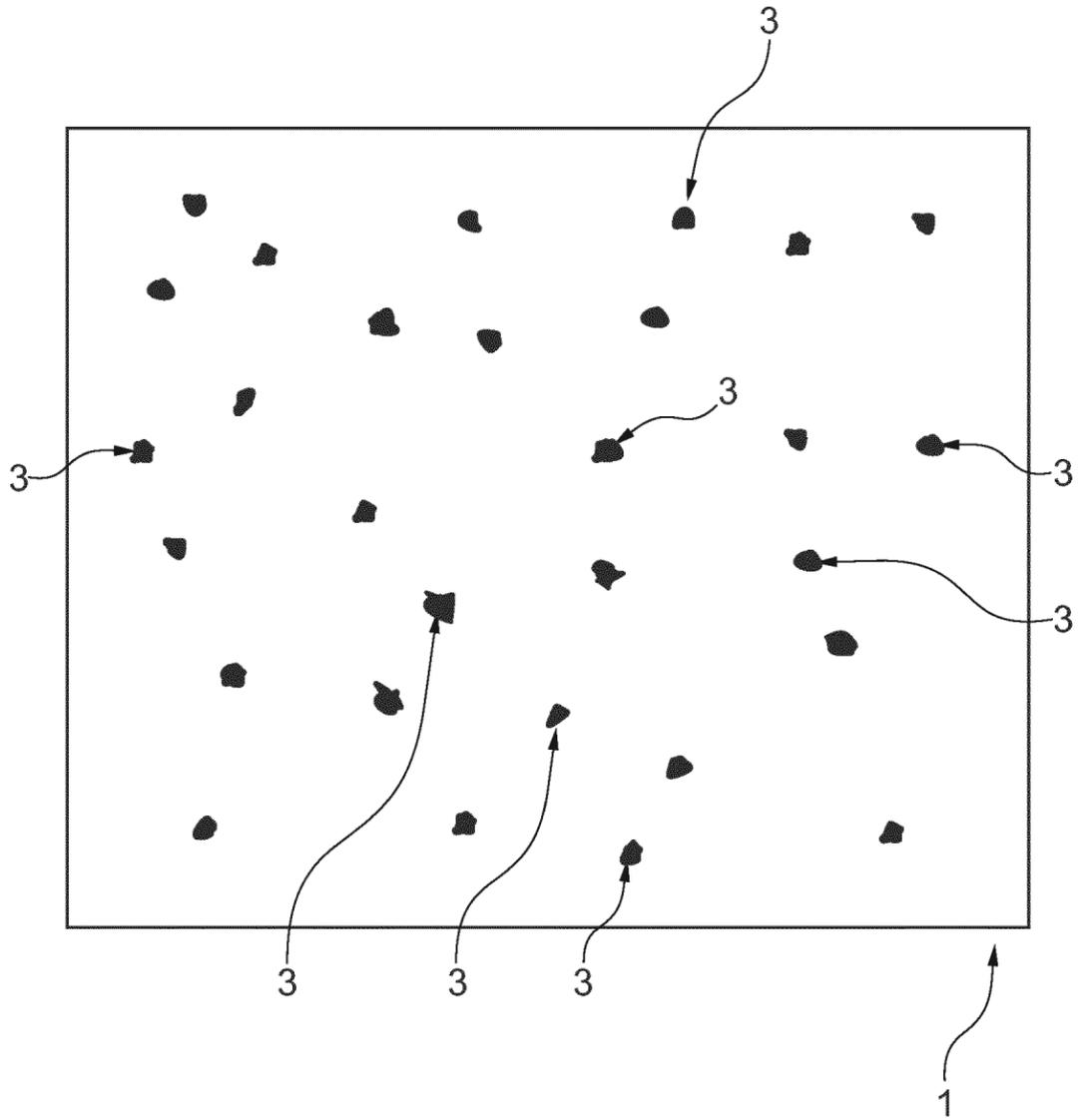


Fig. 2

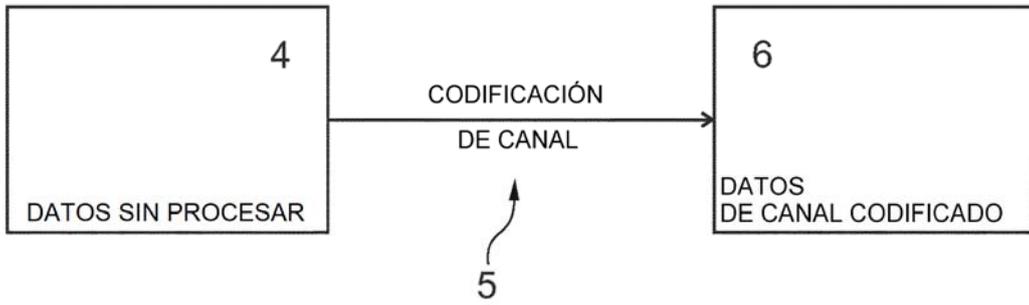


Fig. 3

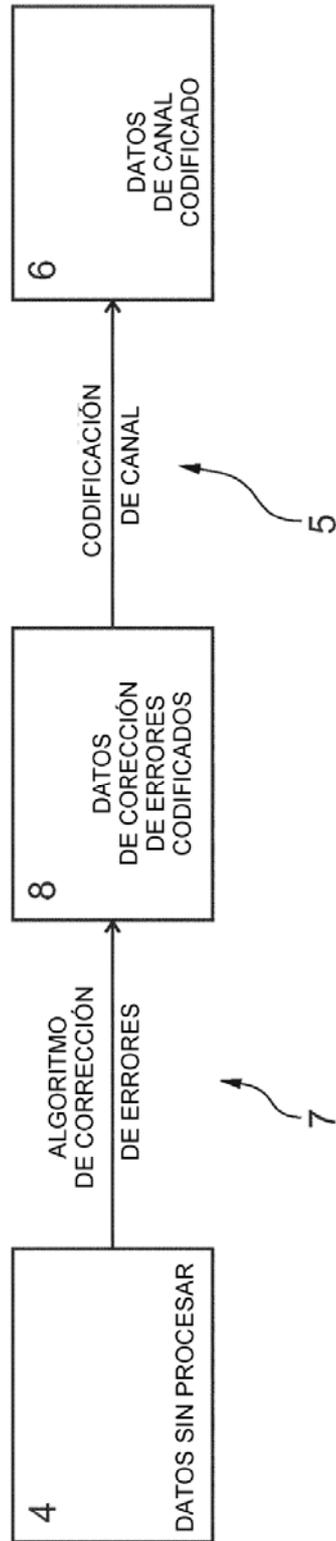


Fig. 4

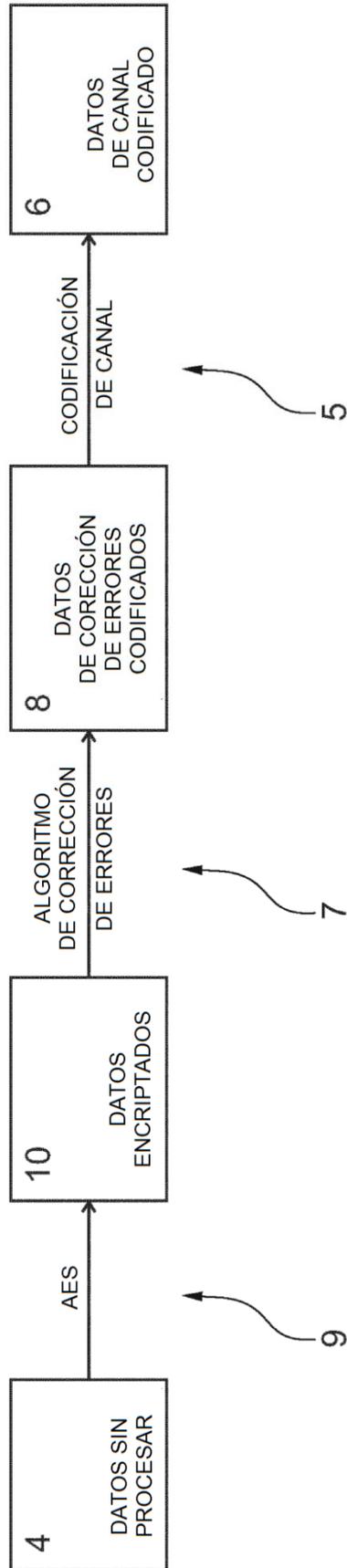


Fig. 5

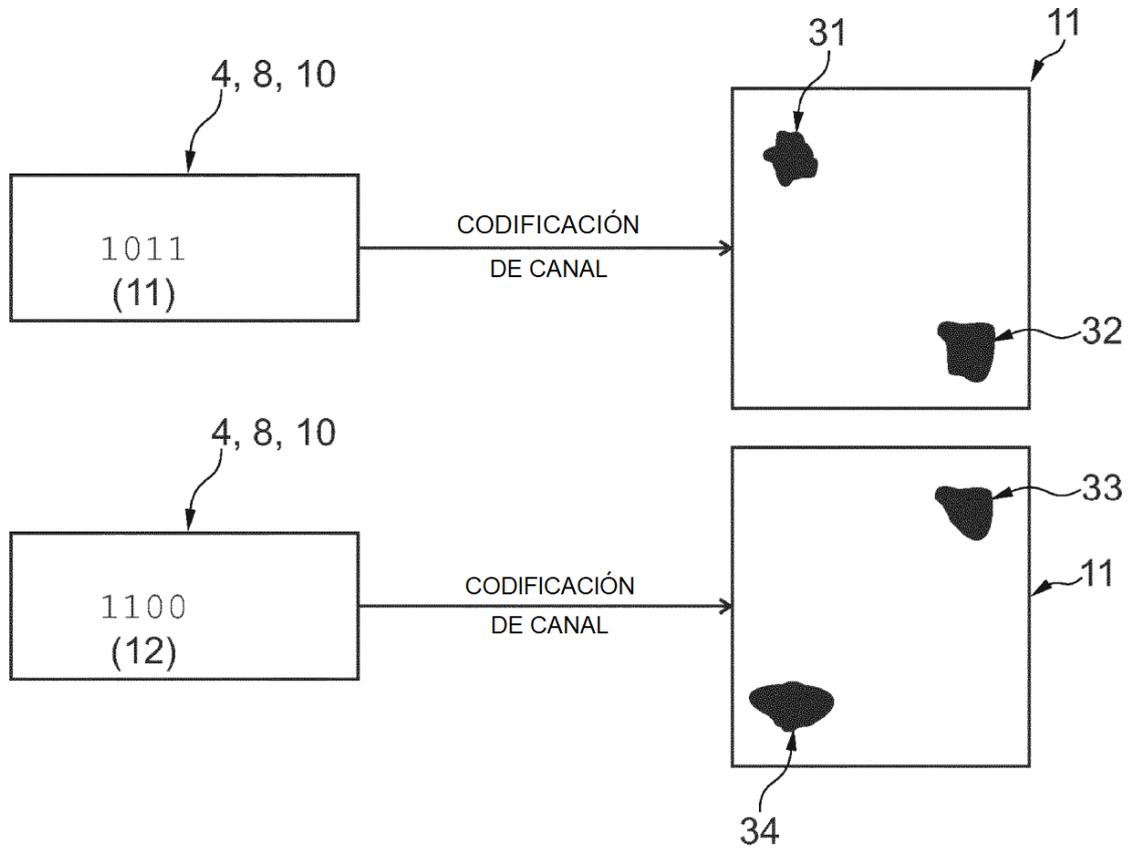


Fig. 6

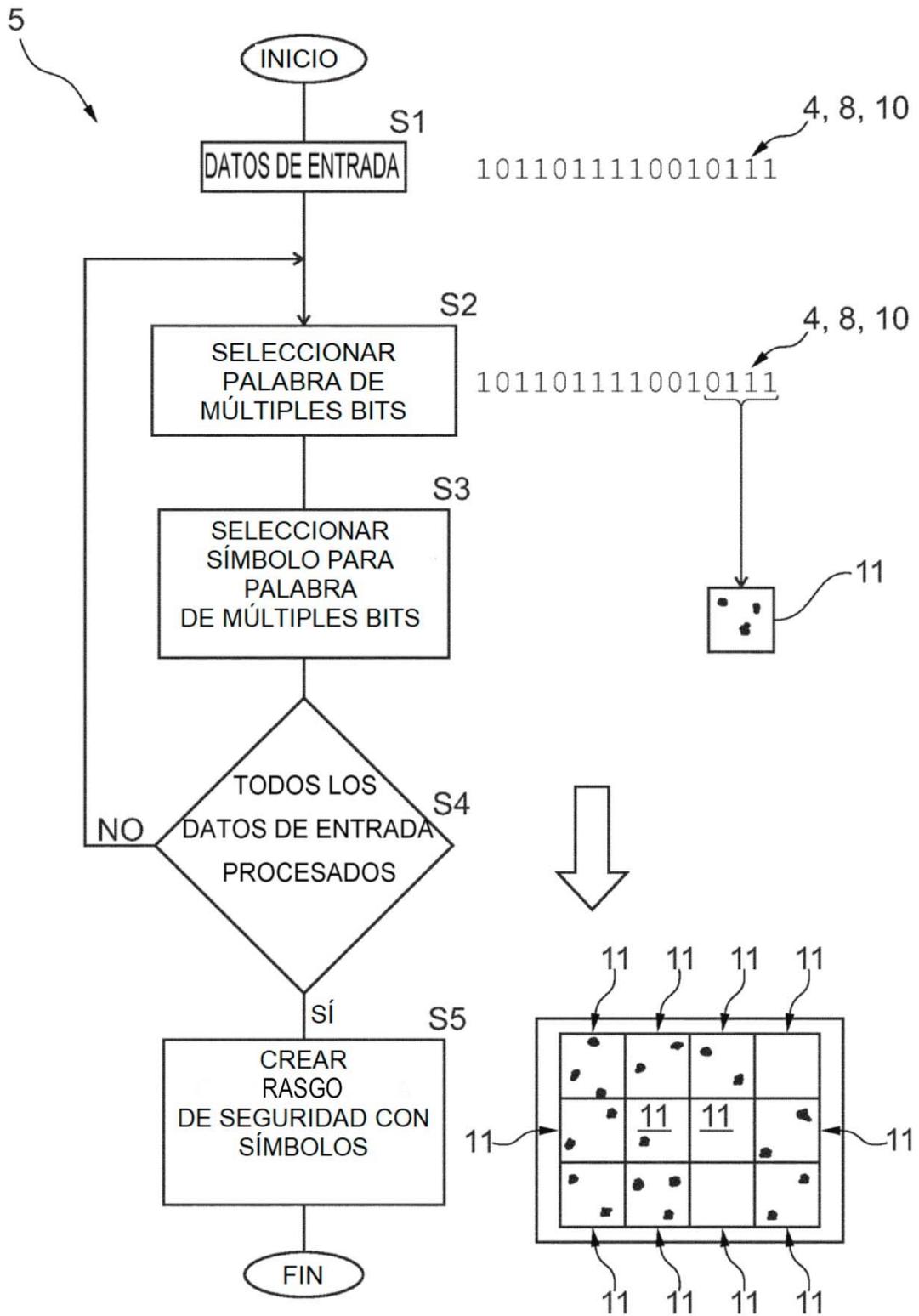


Fig. 7

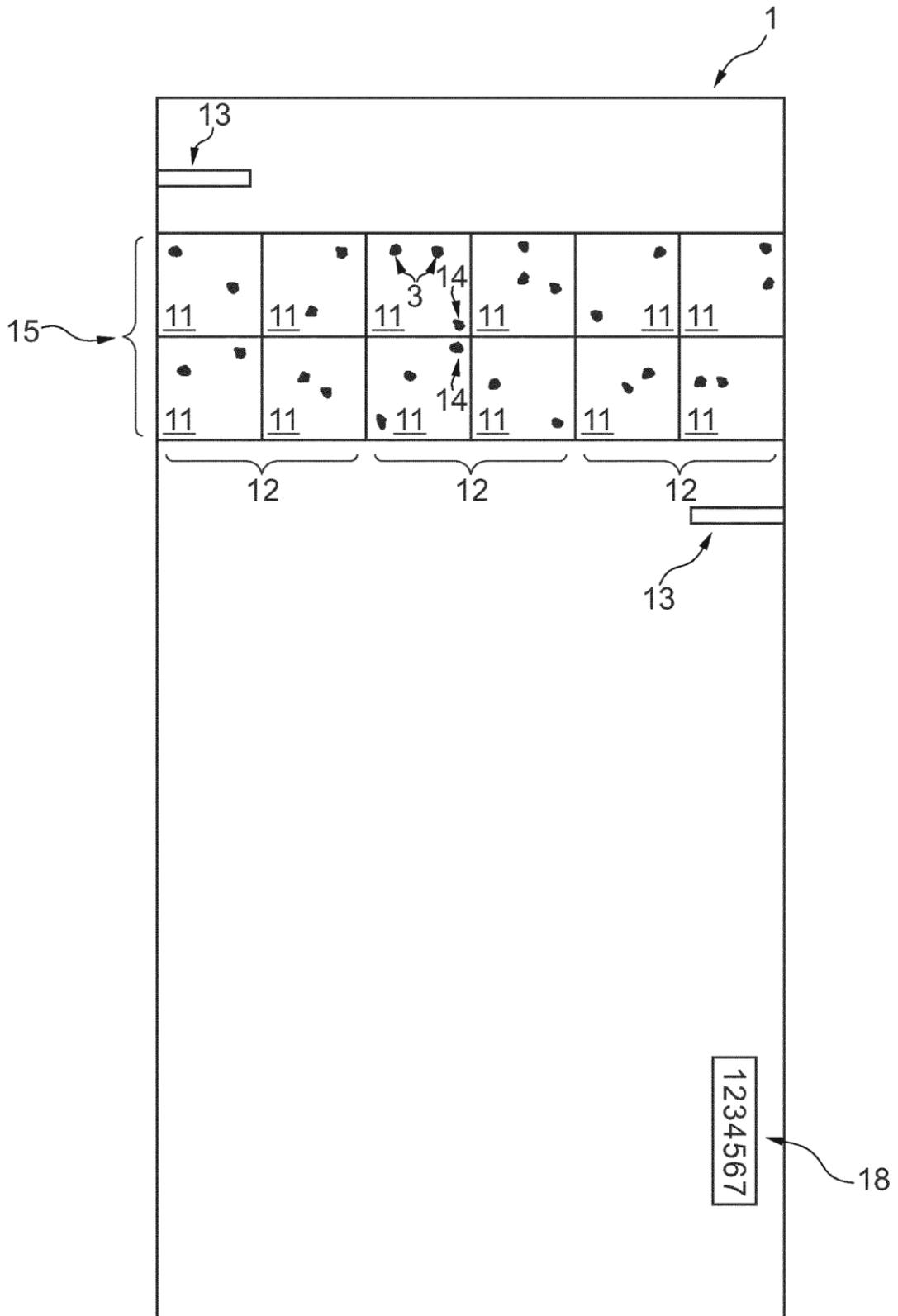


Fig. 8

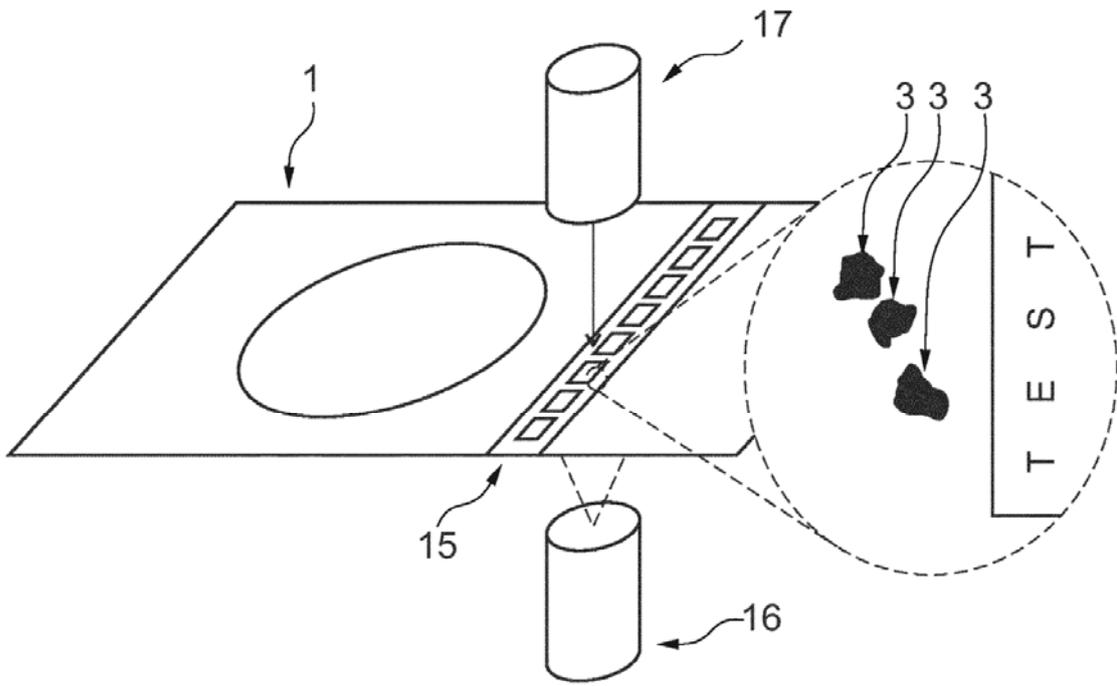


Fig. 9

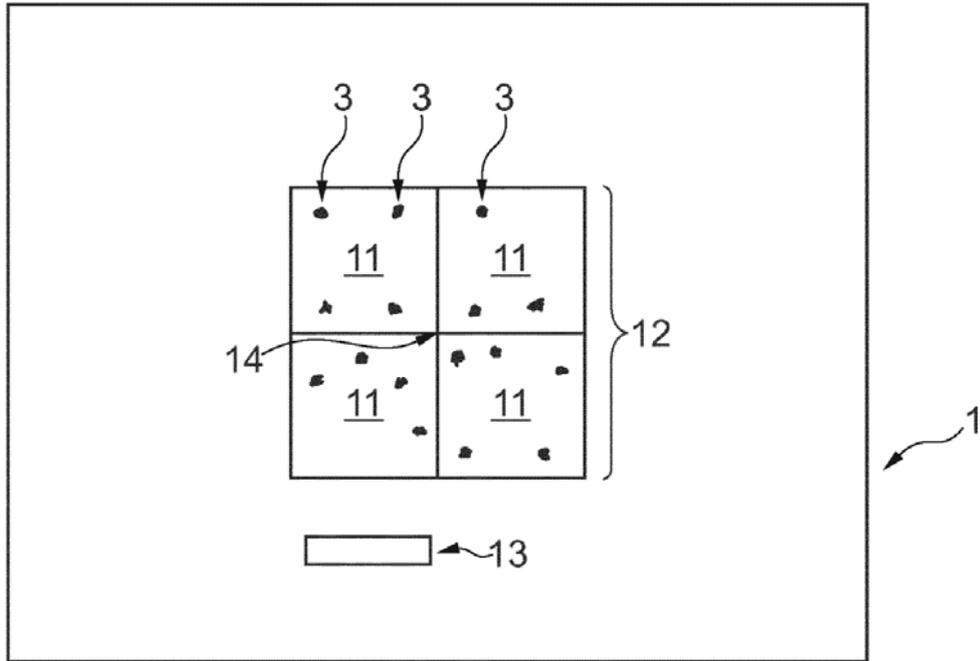


Fig. 10