

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 940 585**

51 Int. Cl.:

G07D 7/20	(2010.01)	G07D 7/206	(2006.01)
G07D 7/128	(2006.01)		
B42D 25/305	(2014.01)		
B42D 25/36	(2014.01)		
B42D 25/324	(2014.01)		
B42D 25/328	(2014.01)		
B42D 25/378	(2014.01)		
B42D 25/337	(2014.01)		
G06T 7/13	(2007.01)		
G07D 7/00	(2008.01)		

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **28.11.2014** **PCT/EP2014/075909**

87 Fecha y número de publicación internacional: **11.06.2015** **WO15082332**

96 Fecha de presentación y número de la solicitud europea: **28.11.2014** **E 14812151 (0)**

97 Fecha y número de publicación de la concesión europea: **15.02.2023** **EP 3078004**

54 Título: **Procedimiento para la autenticación de un elemento de seguridad**

30 Prioridad:

02.12.2013 DE 102013113340
18.07.2014 DE 102014110103

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
09.05.2023

73 Titular/es:

LEONHARD KURZ STIFTUNG & CO. KG (33.3%)
Schwabacher Strasse 482
90763 Fürth, DE;
OVD KINEGRAM AG (33.3%) y
ADORSYS GMBH & CO. KG (33.3%)

72 Inventor/es:

SCHILLING, ANDREAS;
FRIESER, UWE;
SCHMITZER, BENNO;
TOMPKIN, WAYNE ROBERT;
METZGER, JÜRGEN;
WRONDRATSCHEK, RALF y
GUGEL, ALEXANDER

74 Agente/Representante:

PONTI & PARTNERS, S.L.P.

ES 2 940 585 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

Procedimiento para la autenticación de un elemento de seguridad

5 **[0001]** La invención se refiere a un procedimiento para la autenticación de un elemento de seguridad y un equipo para llevar a cabo el procedimiento.

[0002] Los elementos de seguridad ópticamente variables se utilizan a menudo para autenticar documentos, billetes o productos y protegerlos contra la falsificación. Dado que estos elementos de seguridad generan diferentes
10 efectos ópticos en diferentes ángulos de observación y/o de iluminación, no se pueden recrear simplemente mediante fotocopia, duplicación o simulación.

[0003] Habitualmente tales elementos de seguridad poseen un diseño óptico definido, que se puede verificar visualmente con una simple observación. Sin embargo, las falsificaciones de alta calidad, que difieren del original solo
15 en unos pocos detalles, no siempre se pueden detectar de forma fiable durante una inspección visual. Incluso si se debe autenticar una pluralidad de documentos o productos, por ejemplo, una gran cantidad de objetos como billetes, documentos o productos, la inspección visual no es conveniente. Una inspección visual a menudo tampoco es suficiente, porque a menudo el usuario no sabe qué elemento de seguridad concreto con qué funciones de seguridad ópticas y otras funciones está asignado sobre todo al objeto respectivo. Debido a la pluralidad de elementos de
20 seguridad existentes en todos los objetos posibles diferentes, a menudo es difícil obtener un conocimiento preciso del elemento de seguridad concreto presente y sus propiedades específicas de memoria.

[0004] Además, se conocen sistemas para la autenticación automática de elementos de seguridad. Para ello, el elemento de seguridad se ilumina habitualmente con un ángulo predeterminado con un láser y la luz difractada se
25 detecta con uno o varios ángulos de observación predeterminados por medio de sensores adecuados. En este caso se trata de instalaciones estacionarias que son adecuadas para la verificación de una gran cantidad de objetos en particular idénticos en un corto período de tiempo.

[0005] Sin embargo, a menudo existe la necesidad de autenticar espontáneamente *in situ* los elementos de
30 seguridad de los objetos individuales. Para ello, tales instalaciones estacionarias no son adecuadas.

[0006] Por lo tanto, el objetivo de la presente invención es mejorar la autenticación de elementos de seguridad.

[0007] Este objetivo se logra mediante un procedimiento con las características de la reivindicación 1 y
35 mediante un equipo con las características de la reivindicación 10.

[0008] En un procedimiento semejante para la autenticación de un elemento de seguridad ópticamente variable, en particular un elemento de seguridad difractivo, se llevan a cabo las siguientes etapas:

- 40 a) captura de una secuencia de imágenes con al menos una imagen individual del elemento de seguridad por medio de un sensor, en particular de un equipo de mano, preferentemente un teléfono inteligente, tableta o una PDA, o un "dispositivo de realidad aumentada" tal como, por ejemplo, "Google Glass";
b) verificación de si está presente al menos una información óptica predeterminada en al menos una imagen individual de la secuencia de imágenes.

45 **[0009]** Para llevar a cabo un procedimiento semejante es adecuado en particular un elemento de seguridad ópticamente variable, que comprende al menos una información óptica predeterminada, que se puede detectar a máquina con un sensor de un equipo de mano, en particular un teléfono inteligente o PDA, o "dispositivo de realidad aumentada". Esto permite verificar la autenticidad de un elemento de seguridad en cualquier momento y en cualquier
50 lugar, independientemente de los equipos instalados fijos de forma más fiable de lo que sería posible con una simple inspección visual. Por lo tanto, los documentos o productos protegidos con un elemento de seguridad semejante y autenticados mediante un procedimiento semejante están especialmente bien protegidos contra la imitación.

[0010] Por autenticación se entiende a este respecto el reconocimiento de un elemento de seguridad original
55 y su diferenciación de una falsificación.

[0011] Los elementos de seguridad ópticamente variables también se conocen como dispositivos ópticamente variables (OVD, optical variable devices). Se trata de elementos que muestran diferentes efectos ópticos en diferentes condiciones de observación o de iluminación. Un elemento de seguridad ópticamente variable presenta
60 preferiblemente una estructura en relieve ópticamente activa, por ejemplo, una estructura en relieve difractiva, en particular un holograma o un Kinegram®, una estructura de difracción de orden cero, una macroestructura, en particular un campo de microlente de acción refractiva o un campo de microprisma, una estructura mate, en particular una estructura mate isotrópica o una estructura mate anisotrópica, estructuras de rejilla sinusoidal o estructuras de rejilla binaria lineales o cruzadas, estructuras de rejilla Blaze asimétricas, una superposición de una macroestructura con
65 una microestructura difractiva y/o mate, un sistema de capas interferencial, que genera preferentemente un efecto de

desplazamiento de color dependiente del ángulo de visión, una capa que contiene cristales líquidos, en particular cristales líquidos colestéricos y/o una capa que contiene pigmentos ópticamente variables, por ejemplo, pigmentos de capa de lámina delgada o pigmentos de cristal líquido. En particular, mediante combinaciones de uno o varios de los elementos mencionados anteriormente, se puede proporcionar un OVD especialmente a prueba de falsificaciones, porque un falsificador tiene que recrear esta combinación específica, lo que aumenta considerablemente el grado de dificultad técnica de la falsificación.

[0012] Por un equipo de mano se debe entender a este respecto cualquier equipo transportable que se pueda retener por un usuario durante la realización del procedimiento o portarse por un usuario y manipularse manualmente.

Además de los teléfonos inteligentes, tabletas o PDAs ya mencionados, también se pueden utilizar otros equipos. Por ejemplo, en lugar de los equipos polivalentes mencionados, también es posible utilizar equipos que estén contruidos específicamente solo para llevar a cabo este procedimiento. Por ejemplo, un escáner de documentos presente se puede adaptar a la realización del procedimiento según la invención mediante la adaptación de su software y/o hardware.

[0013] El sensor utilizado es por lo general un sensor electrónico digital, por ejemplo, un sensor CCD (CCD = charge coupled device [dispositivo acoplado por carga]). A este respecto, se emplean preferiblemente matrices CCD, es decir, disposiciones CCD en las que los CCD individuales están dispuestos en una matriz bidimensional. Las imágenes individuales generadas por un sensor semejante están presentes entonces en forma de una matriz de píxeles, donde cada píxel corresponde a un único CCD del sensor. Preferiblemente, el sensor CCD presenta en cada caso sensores separados para los colores rojo, verde y azul (RGB), por lo que estos colores individuales o colores mezclados de los mismos son especialmente fáciles de detectar.

[0014] Para muchos casos de aplicación es preferible proporcionar un OVD que se pueda verificar con una pluralidad de equipos de mano disponibles. Sin embargo, debido al desarrollo técnico tormentoso, hay fuertes diferencias técnicas entre los equipos de mano individuales, en particular en términos de potencia de cálculo, calidad de imagen óptica del sensor (por ejemplo, resolución óptica). Por lo tanto, en algunos casos es inevitable definir, a partir de la pluralidad de los equipos manuales, una subselección con la que se puede llevar a cabo el procedimiento según la invención.

[0015] Preferentemente, la secuencia de imágenes comprende una pluralidad de imágenes individuales del elemento de seguridad, en particular comprende más de 2 imágenes individuales del elemento de seguridad. Además, se prefiere que cada imagen individual presente más de 480 x 320 píxeles, en particular más de 1920 x 1280 píxeles.

[0016] La secuencia de imágenes puede ser a este respecto una pluralidad de imágenes individuales creadas discretamente, que no están en relación temporal, pero también se puede tratar de una lámina, es decir, se puede componer de imágenes individuales, que están capturadas a un intervalo temporal predeterminado, en particular con una frecuencia de captura de 5 a 60 imágenes por segundo.

[0017] Según la invención, en la etapa b) se verifica sobre la base de al menos dos imágenes individuales de la secuencia de imágenes si el elemento de seguridad comprende una estructura ópticamente variable. Esto permite distinguir un elemento de seguridad auténtico de una copia (por ejemplo, una copia en color) que presenta solo una representación estática, es decir, no ópticamente variable, de la al menos una información óptica predeterminada. En este caso, es ventajoso verificar explícitamente la pertenencia de la imagen individual respectiva o definir un intervalo de tiempo predeterminado entre dos imágenes individuales como condición para que un usuario no pueda usar dos imágenes individuales separadas como engaño para simular una variabilidad óptica.

[0018] Según la invención, en la etapa b) se verifica en primer lugar si un objeto predeterminado está presente en al menos una imagen individual de la secuencia de imágenes. A este respecto, este objeto puede ser todo el diseño del propio elemento de seguridad o representar solo un aspecto parcial del mismo. De este modo se garantiza que la al menos una imagen individual represente sobre todo el elemento de seguridad a autenticar. Si este no es el caso, se puede prescindir de investigaciones adicionales y se advierte al usuario que las imágenes capturadas por medio del sensor son inadecuadas para el propósito de la autenticación y, si es necesario, se deben capturar nuevamente.

[0019] De forma alternativa se le puede pedir al usuario que realice otros pasos para la identificación o autenticación. Por ejemplo, se le puede exigir al usuario que capture una imagen de un código de barras presente en el objeto (por ejemplo, impreso) u otra región legible a máquina (por ejemplo, la MRZ (MRZ = machine readable zone [zona de lectura de máquina]) de un documento de identificación) o una región parcial determinada del paquete o de un documento y que la envíe a un organismo de inspección oficial o comercial para su posterior análisis. Estas imágenes capturadas adicionalmente se pueden vincular entonces con información adicional y, dado el caso, se transmiten al usuario todavía otras instrucciones para la identificación o autenticación, por ejemplo, a través de una conexión de Internet.

[0020] A este respecto, es conveniente que para verificar si está presente el objeto predeterminado se utilice un algoritmo de reconocimiento de imágenes, en particular un algoritmo de Haar-Cascade. Tales algoritmos permiten

una clasificación rápida y fiable del contenido de las imágenes.

[0021] El algoritmo de Haar-Cascade se basa en la evaluación de una pluralidad de las llamadas características "similares a Haar" en la imagen individual. En este caso se trata de estructuras que están relacionadas con ondas de Haar, es decir, ondas rectangulares de una longitud de onda predeterminada. A este respecto, en dos dimensiones se trata simplemente de una región rectangular adyacente, alternativamente clara y oscura en la imagen. Al desplazar una máscara rectangular sobre la imagen individual, se determinan las características "similares a Haar" presentes. Las características "similares a Haar" presentes se comparan entonces con las que deben estar presentes en el objeto a reconocer. Esto se puede realizar mediante una cascada de filtro.

[0022] El algoritmo de Haar-Cascade tiene la ventaja de necesitar especialmente poco tiempo de cálculo y recursos informáticos. Sin embargo, también es posible utilizar otros algoritmos de reconocimiento de imágenes.

[0023] Para verificar si el objeto predeterminado está presente, preferiblemente por medio del algoritmo de reconocimiento de imágenes se lleva cabo una comparación de la al menos una imagen individual con un conjunto de datos de entrenamiento previamente capturado. Esto se puede realizar en el marco del algoritmo de Haar-Cascade descrito, pero también por medio de otros algoritmos.

[0024] Por lo tanto, el reconocimiento de imágenes se basa de manera ventajosa en una forma de aprendizaje por ordenador. Al algoritmo no se le especifican parámetros concretos mediante los cuales se realiza una clasificación del contenido de la imagen, sino que el algoritmo aprende estos parámetros sobre la base del conjunto de datos de entrenamiento.

[0025] Preferiblemente, a este respecto, para la captura del conjunto de datos de entrenamiento se crean una pluralidad de imágenes, donde un primer subconjunto de las imágenes presenta en cada caso el objeto predeterminado y un segundo subconjunto de las imágenes no presenta en cada caso el objeto predeterminado, y donde a cada imagen del primer subconjunto se le asignan todas las coordenadas de imagen respectivas de las características a reconocer del objeto predeterminado.

[0026] Sobre la base del primer y segundo subconjunto, así como de las coordenadas de imagen asignadas, entonces se lleva a cabo preferiblemente un entrenamiento del algoritmo de reconocimiento de imágenes. De este modo, el algoritmo aprende a clasificar correctamente las imágenes y, dado el caso, a ignorar factores de interferencia incorporados conscientemente en el conjunto de datos de entrenamiento, tales como, por ejemplo, reflexiones en las imágenes, casos de sombras aleatorios o similares. De este modo se posibilita un reconocimiento de imágenes rápido y fiable.

[0027] Es según la invención que al verificar si está presente la al menos una información óptica predeterminada del elemento de seguridad ópticamente variable, a partir de al menos una imagen individual de la secuencia de imágenes se determina el contorno del objeto predeterminado.

[0028] En comparación con el reconocimiento de imágenes simple descrito anteriormente, que solo proporciona una clasificación de sí/no o una declaración de probabilidad de si el objeto predeterminado está presente en la imagen individual, así se proporciona información adicional. En particular, sobre la base del contorno determinado se puede verificar la presencia o ausencia de características detalladas del objeto. Esto proporciona información adicional que puede contribuir a autenticar el elemento de seguridad.

[0029] La información predeterminada, que sirve para la autenticación, solo se puede referir a un detalle de todo el objeto. Esto permite ocultar también características de seguridad visualmente reconocibles en el diseño del elemento de seguridad. Preferentemente, para determinar el contorno se ejecuta un algoritmo de reconocimiento de bordes, en particular un algoritmo de Canny. El algoritmo de Canny es un algoritmo de detección de bordes especialmente robusto y proporciona resultados rápidos y fiables.

[0030] Para aplicar el algoritmo de Canny a las imágenes en color, estas se deben convertir en primer lugar a escala de grises. En las imágenes en escala de grises, los bordes se caracterizan por fuertes fluctuaciones de brillo, es decir, un fuerte contraste, entre píxeles adyacentes y, por lo tanto, se pueden describir como discontinuidades de la función de valor de grises de la imagen.

[0031] Dado que tales discontinuidades también se pueden causar por ruido de imagen, es conveniente que en la ejecución del algoritmo de detección de bordes se lleve a cabo un filtrado de ruido, en particular por medio de un filtro gaussiano con un tamaño de núcleo (kernel) preferido de 3 a 7.

[0032] Por núcleo se entiende en este caso una matriz de convolución que se aplica a la información de la imagen. La matriz de convolución del filtro gaussiano corresponde a la distribución normal y actúa como filtro de paso bajo. Por lo tanto, el valor de gris de un píxel filtrado corresponde a la media ponderada con la distribución normal de los valores grises de los píxeles circundantes hasta una distancia máxima, definida por el tamaño de núcleo. Las

estructuras más pequeñas, que se originan por el ruido se pierden, mientras que las estructuras principales del objeto reproducido se conservan.

[0033] Preferentemente, en la realización del algoritmo de reconocimiento de bordes se lleva a cabo una
5 detección de bordes mediante la aplicación de un operador Sobel en al menos una dirección preferida de la al menos una imagen individual, preferentemente en dos direcciones preferidas ortogonales de la al menos una imagen individual.

[0034] El operador Sobel también es un operador de pliegue que actúa como un diferenciador discreto. Debido
10 al pliegue de la imagen con el operador Sobel se obtienen las derivadas parciales de la función de valor de gris en las dos direcciones preferidas ortogonales. A partir de esto se puede determinar entonces la dirección del borde y el grosor del borde.

[0035] Además, es preferible que en la ejecución del algoritmo de detección de bordes se lleve a cabo un
15 filtrado de bordes. Esto se puede realizar, por ejemplo, por medio de una llamada "non-maximum suppression", que garantiza que solo se conserven los máximos a lo largo de un borde, de modo que un borde no sea más ancho que un píxel perpendicular a su dirección de extensión.

[0036] Preferentemente, en la ejecución del algoritmo de reconocimiento de bordes se lleva a cabo además
20 una determinación basada en el valor umbral de las coordenadas de imagen del contorno del objeto. Por lo tanto, se determina a partir de qué grosor de borde se debe contar un píxel para un borde.

[0037] Para ello se puede utilizar, por ejemplo, un procedimiento basado en histéresis. Para ello se establecen
25 dos valores umbral T_1 y T_2 , donde T_2 es mayor que T_1 . Un píxel con un grosor de borde mayor que T_2 se considera parte de un borde. Todos los píxeles conectados a este píxel con un grosor de borde mayor que T_1 se atribuyen igualmente a este borde.

[0038] Por lo tanto, se obtienen las coordenadas de imagen de todos los píxeles correspondientes a un borde
30 del objeto en la imagen individual examinada. Estos se pueden analizar más a fondo, por ejemplo, para reconocer formas geométricas simples.

[0039] Además, es conveniente que, sobre la base de las coordenadas de imagen determinadas del contorno,
al menos una imagen individual de la secuencia de imágenes se divida en dos o más regiones parciales y para cada
35 región parcial se comparen las coordenadas de imagen determinadas del contorno con las coordenadas de consigna correspondientes y, a partir de esto, se determine en particular la presencia y/o el tamaño y/o la posición relativa de contornos predeterminados. Aquí puede ser ventajoso adaptar la subdivisión en regiones parciales o las limitaciones de las regiones parciales al diseño concretamente presente del elemento de seguridad y, por lo tanto, analizar de forma aislada regiones parciales especialmente interesantes del diseño.

[0040] Estos contornos predeterminados pueden corresponder con la información óptica predeterminada, de
40 modo que se hace posible una comprobación precisa de la imagen individual con respecto a la correspondencia con la información óptica del elemento de seguridad real.

[0041] Para autenticar como auténtico un elemento de seguridad así examinado, a este respecto no debe
45 existir necesariamente una correspondencia absoluta, también es posible especificar rangos de tolerancia para desviaciones permitidas. Las desviaciones no deben indicar necesariamente una falsificación, ya que los artefactos ópticos, las distorsiones de perspectiva, el desgaste o la contaminación del elemento de seguridad en uso o efectos similares, que puedan ocurrir al capturar la imagen individual, también pueden menoscabar la correspondencia con la imagen de referencia del original. Para reducir tales desviaciones, es ventajoso que estén previstos medios auxiliares
50 para facilitar al usuario la realización del procedimiento según la invención. Por ejemplo, en la pantalla del equipo de mano puede estar representado uno o varios marcos de orientación en los que se debe colocar el elemento de seguridad o partes del motivo para el reconocimiento. De forma alternativa o complementaria a ello, pueden estar previstos otros medios auxiliares ópticos o indicadores para reducir, por ejemplo, distorsiones y/o torsiones en perspectiva. Por ejemplo, pueden ser el cruce de hilo móvil u otros elementos que se deben posicionar entre sí por
55 medio del movimiento del equipo de mano. Aunque esto dificulta la manipulación del equipo de mano para el usuario, puede mejorar la tasa de reconocimiento para el elemento de seguridad.

[0042] Es según la invención que se selecciona al menos una región parcial de la imagen individual, que está
60 posicionada en una posición predeterminada con respecto al contorno de un objeto predeterminado y que comprende al menos un píxel y/o al menos un grupo de píxeles de la imagen individual, y al menos una propiedad del al menos un píxel y/o del al menos un grupo de píxeles de la al menos una región parcial seleccionada se compara con un valor de consigna correspondiente.

[0043] Por lo tanto, la información óptica predeterminada o también partes de la misma también se pueden
65 analizar a nivel de píxel. Esto permite utilizar detalles muy finos del diseño del elemento de seguridad para su

autenticación. Por ejemplo, las desviaciones de color o brillo ya dirigidas en regiones muy pequeñas del elemento de seguridad, que se reproducen solo como píxeles individuales al capturar la secuencia de imágenes, se pueden usar para la autenticación. A este respecto, esta área muy pequeña puede ser especialmente discreta para que el falsificador potencial no tenga conocimiento de la importancia especial de esta pequeña región.

[0044] A este respecto, es conveniente si la posición de la al menos una región parcial de la imagen individual se determina sobre la base de las coordenadas de imagen determinadas del contorno. De esta manera, los pequeños detalles del elemento de seguridad se pueden encontrar e investigar de forma segura sobre la base de su posición relativa con respecto al contorno.

[0045] La al menos una región parcial comprende a este respecto preferentemente menos del 50% de la superficie de la imagen individual.

[0046] Además, es ventajoso que durante la captura de la secuencia de imágenes en el paso a) se modifique un ángulo entre el sensor y el elemento de seguridad y/o un ángulo entre una fuente de luz (por ejemplo, la lámpara de destello del equipo de mano) y el elemento de seguridad. Por ángulo entre una fuente de luz y el elemento de seguridad se debe entender el ángulo de incidencia de la luz que ilumina el OVD con respecto a la superficie normal del OVD. Cuando se utiliza la fuente de luz del equipo de mano, el ángulo de incidencia de la luz coincide de forma relativamente precisa con el eje óptico del sensor (que va desde el OVD a través de su lente hasta el sensor de imagen).

[0047] Dado que se trata de un elemento de seguridad ópticamente variable, al cambiar el ángulo de observación y/o el ángulo de iluminación también se modifica su aspecto detectable/medible. De esta manera se puede verificar en primer lugar si el elemento de seguridad detectado en la secuencia de imágenes es realmente ópticamente variable, o si se trata de una copia estática de un OVD.

[0048] Además, así se posibilita vincular la información óptica predeterminada con la variabilidad óptica. Por ejemplo, una parte de la información óptica predeterminada puede ser visible en un primer ángulo de observación y otra parte de la información óptica predeterminada puede ser visible en un segundo ángulo de observación. Una copia estática de un elemento de seguridad semejante nunca mostraría la información completa, de modo que el elemento de seguridad no se puede copiar de forma convencional, en particular desde el punto de vista de la técnica de impresión.

[0049] Además, es ventajoso si durante la captura de la secuencia de imágenes en la etapa a) se registra una posición relativa del equipo de mano con respecto a una posición predeterminada por medio de un sensor de posición del equipo de mano para cada imagen individual de la secuencia de imágenes y se asigna a la imagen individual respectiva.

[0050] Al menos cuando se conoce la posición relativa del elemento de seguridad con respecto a la posición predeterminada, así se puede determinar con precisión el ángulo de observación. Esto es posible, por ejemplo, si el elemento de seguridad se deposita durante la captura de la secuencia de imágenes sobre una superficie plana, en particular horizontal.

[0051] Los sensores de posición o sensores de movimiento habituales de teléfonos inteligentes o similares pueden determinar entonces sin problemas la orientación relativa del teléfono inteligente con respecto a esta superficie y, por tanto, con respecto al elemento de seguridad durante la captura de la secuencia de imágenes. La exactitud de los sensores de posición o sensores de movimiento habituales se mueve en particular en un rango de $\pm 1^\circ$ con una calibración previa del sensor en cuestión y en particular en un rango de $\pm 5^\circ$ sin una calibración previa del sensor en cuestión. A este respecto, se debe tener en cuenta que tales sensores de posición o sensores de movimiento habituales solo pueden detectar su posición relativa con respecto a una horizontal o vertical, pero no su posición relativa con respecto al elemento de seguridad. Por lo tanto, el usuario debe ser instruido preferiblemente para colocar el elemento de seguridad en una posición horizontal o vertical lo más precisa posible, para permitir un reconocimiento lo más preciso posible.

[0052] Para verificar si el elemento de seguridad comprende una estructura ópticamente variable, preferentemente en la etapa b) se comparan dos imágenes individuales de la secuencia de imágenes, que se han capturado con diferentes ángulos de observación y/o de iluminación y/o condiciones de iluminación.

[0053] Si estas imágenes individuales difieren en una medida predeterminada en uno o varios parámetros, entonces se puede partir de la presencia de una estructura ópticamente variable. Si este no es el caso, entonces lo más probable es que esté presente una copia estática.

[0054] A este respecto, es ventajoso que, para verificar si el elemento de seguridad comprende una estructura ópticamente variable, se comparen respectivamente píxeles y/o grupos de píxeles correspondientes, en particular las regiones parciales, de las imágenes individuales.

[0055] De esta manera, se puede determinar la identidad o no identidad de las imágenes individuales sin un gran esfuerzo de procesamiento.

5 **[0056]** Es conveniente si se verifica en este caso si los respectivos píxeles y/o grupos de píxeles, en particular de las regiones parciales, de las imágenes individuales se diferencian en un valor de color y/o valor de brillo.

[0057] Por lo tanto, para verificar la identidad de las imágenes individuales no se deben reconocer estructuras en las imágenes individuales, es suficiente considerar los cambios típicos de OVD debido al ángulo de observación o
10 iluminación modificado a nivel de píxeles. Esto es especialmente eficiente y ahorra tiempo de cálculo. A este respecto, se pueden transmitir al usuario preferentemente instrucciones sobre cómo el usuario debe modificar el ángulo de observación o de iluminación para provocar modificaciones ópticamente variables específicas, en particular mediante inclinación y/o giro.

15 **[0058]** Preferentemente, la información óptica predeterminada comprende uno o varios ítems de información seleccionados del grupo: objeto, contorno del objeto, parte del contorno del objeto, propiedades de los píxeles y/o grupo de píxeles de la al menos una región parcial seleccionada.

[0059] Por lo tanto, la información óptica predeterminada se puede integrar de muchas maneras en el diseño
20 del elemento de seguridad. En particular, las opciones mencionadas también se pueden combinar. Esto permite, por ejemplo, representar una información óptica que, si bien puede ser visible visualmente, está oculta o distribuida en el diseño general de modo que no se percibe como información propia. Por lo tanto, es difícil para un falsificador reconocer lo que se utiliza exactamente para autenticar el elemento de seguridad, de modo que las falsificaciones son especialmente difíciles de fabricar.

25 **[0060]** Para la autenticación del elemento de seguridad es conveniente a este respecto en particular que uno o varios ítems de información seleccionados del grupo: objeto, contorno del objeto, parte del contorno del objeto, propiedades de los píxeles y/o grupo de píxeles de la al menos una región parcial seleccionada, se comparan con valores de consigna para determinar si la información óptica predeterminada está presente.

30 **[0061]** Aquí también se pueden permitir tolerancias a los valores de consigna para permitir desviaciones debido a artefactos fotográficos y similares. Tales tolerancias son ventajosas porque los OVD reaccionan generalmente de forma sensible a pequeñas diferencias en las condiciones de observación y de iluminación.

35 **[0062]** Además, es ventajoso si durante la captura de la secuencia de imágenes en el paso a) se captura al menos una imagen de la secuencia de imágenes con flash y al menos una imagen de la secuencia de imágenes sin flash.

40 **[0063]** Es ventajoso si la al menos una información óptica predeterminada es o comprende una información visualmente reconocible.

[0064] Esto permite llevar a cabo también una inspección visual además de la autenticación automática descrita, en caso de que no exista la posibilidad de una verificación automática. Por visualmente reconocible se debe
45 entender a este respecto que la información se puede clarificar por el ojo humano a una distancia de observación habitual de aproximadamente 30 cm, preferiblemente de 10 cm a 50 cm, y con una iluminancia habitual de 1000 lx, preferiblemente de 10 lx a 100000 lx.

[0065] A este respecto, es posible que la al menos una información óptica predeterminada sea o comprenda un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número.

50 **[0066]** Las estructuras mencionadas también pueden estar integradas en otros diseños y son especialmente fáciles de reconocer y también de verificar visualmente.

[0067] Además, es posible y ventajoso que la al menos una información óptica predeterminada sea o
55 comprenda un elemento parcial de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número.

[0068] De esta manera, la información óptica predeterminada puede estar integrada de manera especialmente sutil y discreta en un diseño. Por ejemplo, un carácter alfanumérico puede tener una ligera modificación o desviación con respecto al escrito utilizado en otros caracteres. De esta manera, la información óptica se puede ocultar, de modo
60 que no se puede ver inmediatamente que parte del elemento de seguridad se utiliza como característica de autenticación. Por ejemplo, un texto en la fuente serif "Times Roman" puede estar en 18 puntos, con la excepción de una sola letra, cuya serifa es un poco más corta de lo predeterminado o cuya serifa falta por completo.

[0069] Con este fin, es especialmente ventajoso si la al menos una información óptica predeterminada está
65 presente junto con otra información óptica, visualmente perceptible del elemento de seguridad difractivo, en particular

en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número.

[0070] Además, es posible que la al menos una información óptica predeterminada sea o comprenda una disposición de píxeles y/o una disposición de líneas y/o la posición relativa de una disposición de píxeles y/o una disposición de líneas para otra información óptica, visualmente perceptible del elemento de seguridad difractivo, en particular en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número.

[0071] De este modo, la información óptica también se puede integrar de forma discreta en el diseño del elemento de seguridad.

[0072] Otra posibilidad para la integración de la información óptica en el elemento de seguridad consiste en que la al menos una información óptica predeterminada es o comprende una desviación de una propiedad gráfica, en particular de un grosor de línea, un valor de color, un valor de tono, una claridad, una densidad de trama, una orientación de trama o un escrito, entre una primera región parcial y una segunda región parcial de otra información óptica, visualmente perceptible del elemento de seguridad ópticamente variable, en particular en forma de un símbolo, logotipo, imagen, dibujo, carácter alfanumérico o número.

[0073] De esta manera, la información también se puede ocultar en el elemento de seguridad y, por lo tanto, ser difícil de reconocer para los falsificadores. En particular, una desviación semejante puede ser pequeña y estar localizada, de modo que un falsificador tiene la impresión de que en este caso se trata de un error de producción del elemento de seguridad, que eventualmente tiene que "corregir" en el caso de la falsificación. La falsificación, por supuesto, ya no presenta la información óptica especificada y es fácil de reconocer como tal.

[0074] Para el mismo fin también es posible que la al menos una información óptica predeterminada sea o comprenda una desviación de una simetría entre una primera región parcial y una segunda región parcial de otra información óptica, visualmente perceptible del elemento de seguridad difractivo, en particular en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número.

[0075] Por supuesto, todas las posibilidades mencionadas para la representación de la información óptica dada también se pueden combinar entre sí.

[0076] De forma alternativa o adicional, también puede ser ventajoso que la al menos una información óptica predeterminada sea o comprenda una información visualmente no reconocible o solo difícilmente reconocible, que se pueda detectar a máquina con el sensor.

[0077] Por visualmente no reconocible se debe entender a este respecto que la información a una distancia de observación habitual de aproximadamente 30 cm, preferiblemente de 10 cm a 50 cm, y con una iluminancia habitual de 1000 lx, preferiblemente de 10 lx a 100000 lx, no se puede clarificar por el ojo humano.

[0078] En particular, también se pueden combinar información óptica, visualmente reconocible y no reconocible para obtener así un elemento de seguridad especialmente a prueba de falsificaciones. Además del reconocimiento descrito anteriormente de la información óptica visualmente reconocible, se pueden llevar a cabo entonces otras tareas de autenticación sobre la base de la información óptica visualmente no reconocible. La información óptica visualmente reconocible se puede examinar con el ojo humano a simple vista, en particular si el usuario correspondiente ha practicado o está entrenado.

[0079] A este respecto es conveniente que la al menos una información óptica predeterminada se forme mediante una variación de al menos un parámetro de relieve de una estructura en relieve del elemento de seguridad entre al menos una primera zona y al menos una segunda zona del elemento de seguridad, donde la estructura en relieve prevista en la primera y/o segunda zona es en particular una estructura difractiva una estructura de rejilla sinusoidal o estructura de rejilla binaria lineal o cruzada, una rejilla longitudinal de subonda o una estructura de difracción de orden cero, una rejilla Blaze, una macroestructura, en particular una estructura de lente refractiva o estructura de microprisma, una superficie de espejo, una estructura mate, en particular una estructura mate anisotrópica o isotrópica. La estructura en relieve también puede presentar preferiblemente una combinación, en particular una superposición de una macroestructura con una microestructura.

[0080] Por medio de las estructuras mencionadas se pueden generar múltiples efectos ópticos, que son especialmente difíciles de copiar y al mismo tiempo contribuyen a proporcionar un diseño ópticamente atractivo del elemento de seguridad. Las ligeras variaciones de los parámetros estructurales de estas estructuras se pueden incorporar sin más de modo que permanezcan por debajo del umbral de percepción del ojo humano, pero se pueden detectar por medio de un sensor. De esta manera, una información óptica se puede integrar en el elemento de seguridad sin que se menoscabe el diseño visualmente perceptible.

[0081] A este respecto, es ventajoso que una dimensión lateral de la al menos una primera y/o de la al menos una segunda zona sea menor de 600 µm, preferiblemente menor de 300 µm, más preferiblemente menor de 150 µm.

[0082] De este modo se garantiza de la manera más sencilla que las diferentes zonas no se puedan clarificar con el ojo humano y aparezcan como una estructura homogénea. En particular, si el sensor del equipo de mano presenta una resolución óptica especialmente alta, esto puede ser ventajoso para ello.

[0083] Es ventajoso si la al menos una primera zona esté configurada en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número y la al menos una segunda zona configura un fondo para la al menos una primera zona.

[0084] De este modo se pueden integrar objetos visualmente no reconocibles en el diseño que se pueden reconocer a máquina con los mismos métodos que se explicaron anteriormente sobre la base de la información óptica visualmente reconocible. Por lo tanto, no se necesitan algoritmos de detección adicionales, lo que hace que la implementación de los programas necesarios sea especialmente fácil y, además, ahorra espacio de almacenamiento en el equipo utilizado para la autenticación.

[0085] Preferiblemente, las primeras y segundas zonas se reticulan entre sí con un período de trama predeterminado.

[0086] El periodo de trama se selecciona preferiblemente de modo que no se pueda clarificar con el ojo humano. A este respecto, los períodos de trama preferidos son de 10 μm a 300 μm . Para el observador, las zonas reticuladas entre sí aparecen entonces como una superficie homogénea, solo para el sensor se pueden distinguir las zonas y, por lo tanto, se pueden utilizar para la autenticación del elemento de seguridad.

[0087] Preferiblemente, el al menos un parámetro de rejilla es una frecuencia espacial, un ángulo de azimut, una profundidad de relieve, una forma de relieve, una fase de la estructura en relieve, un período de una variación de azimut, una variación de profundidad de relieve y/o una variación de frecuencia espacial de una rejilla de una o dos dimensiones, una rugosidad media de una estructura mate y/o la dirección preferida de una estructura mate anisotrópica.

[0088] Además, es conveniente que la estructura en relieve del elemento de seguridad sea una rejilla, en particular con líneas de rejilla curvadas de forma circular, parabólica o en serpentín, con una variación periódica de azimut, donde en al menos una de las regiones parciales el período de variación de azimut y/o el ancho de trama de la trama de una o dos dimensiones sea menor de 300 μm . Por ejemplo, las variaciones de azimut definen el rango de condiciones de visualización o iluminación en las que el OVD aparece brillante u oscuro cuando el OVD se inclina y/o gira.

[0089] Debido al pequeño período, tales rejillas aparecen como superficies homogéneas para el ojo humano a simple vista. Con el sensor, sin embargo, se pueden clarificar, de modo que la al menos una información óptica predeterminada también se puede codificar aquí a nivel de los parámetros de la rejilla.

[0090] A este respecto, la variación periódica de azimut cubre preferiblemente un rango de $\pm 30^\circ$ alrededor de un ángulo medio de azimut abt .

[0091] A este respecto, es ventajoso si la frecuencia espacial de la rejilla es de entre 3000 líneas/mm y 500 líneas/mm y en particular es de entre 1800 líneas/mm y 300 líneas/mm, de manera especialmente preferida de entre 1400 líneas/mm y 700 líneas/mm.

[0092] A este respecto, preferentemente, la fase de la variación periódica de azimut está desplazada entre la primera y la segunda región parcial en 180° .

[0093] Este desplazamiento de fase a su vez no se puede reconocer con el ojo humano, pero se puede clarificar por medio del sensor y, por lo tanto, se puede utilizar para integrar la al menos una información óptica predeterminada en el diseño del elemento de seguridad.

[0094] Además, es ventajoso si la estructura en relieve del elemento de seguridad es una estructura en relieve asimétrica y en la primera región parcial presenta un ángulo de azimut, que es diferente de un ángulo de azimut de la segunda región parcial en 180° .

[0095] También una variación semejante de la rejilla no se puede reconocer a simple vista, pero se puede clarificar por medio del sensor. Idealmente, a este respecto se trata de una rejilla asimétrica, que presenta en una de las regiones parciales un ángulo de azimut de 0° con una fuerte difracción de orden +1 y en la otra región parcial un ángulo de azimut de 180° con una débil difracción de orden -1. A este respecto, si el sensor se encuentra aproximadamente perpendicularmente por encima del OVD, es decir, su eje óptico es aproximadamente paralelo a la normal a la superficie del OVD y la iluminación es aproximadamente lateral, es decir, inclinada hacia la normal a la superficie, entonces la una región parcial (ángulo de azimut de 0° con una fuerte difracción de orden +1) es clara y la

otra región parcial (ángulo de azimut de 180° con una débil difracción de orden -1) es oscura.

[0096] La estructura en relieve en la primera región parcial presenta preferiblemente una frecuencia espacial que se diferencia en al menos 100 líneas/mm de la frecuencia espacial de la segunda región parcial.

5

[0097] Además, es ventajoso si la al menos una información óptica predeterminada se genera durante la captura de la secuencia de imágenes por un efecto Moiré entre una trama periódica del elemento de seguridad y una trama periódica del sensor.

10 **[0098]** En otras palabras, la al menos una información predeterminada surge solo en la interacción entre una estructura periódica del elemento de seguridad y una estructura periódica del sensor, por ejemplo, una matriz CCD dispuesta periódicamente. Un elemento de seguridad semejante es específico para un tipo de sensor determinado o al menos una resolución de sensor específica.

15 **[0099]** Además, es conveniente si la al menos una información óptica predeterminada se genera por un efecto difractivo en un rango de longitud de onda fuera del espectro visible, en particular en el infrarrojo.

[0100] Tal información generada no tiene que estar por debajo del límite de resolución del ojo humano, sino que también puede ser macroscópica. En particular, la información óptica predeterminada puede estar superpuesta a otra información visualmente perceptible, sin que se menoscabe el diseño del elemento de seguridad.

[0101] A este respecto, el efecto difractivo se genera preferiblemente mediante una estructura difractiva de orden cero, en particular una rejilla sinusoidal o rejilla binaria con una capa transparente de un material altamente refractivo, en particular de ZnS. "Alto refractivo" o "high refractive" significa en este contexto que la parte real del índice de refracción complejo debe ser comparativamente alta, en particular entre 1,5 y 2,5. Tales efectos difractivos con materiales de alta refracción como ZnS o TiO₂ se utilizan a menudo en aplicaciones de protección de documentos de identificación, donde los sistemas de lámina transparentes de gran superficie con efectos visuales difractivos protegen los datos personalizados de la manipulación o falsificación (tarjetas de identificación, pasaportes, tarjetas de licencia de conducir, etc.).

30

[0102] Tales estructuras presentan efectos de difracción suficientes en el rango infrarrojo, de modo que el efecto deseado se puede generar fácilmente. Además del sulfuro de zinc, también se pueden utilizar otros materiales altamente refractivos (HRI = high refractive index, materiales HRI), tales como, por ejemplo, pentóxido de niobio, dióxido de titanio entre otros.

35

[0103] Preferentemente, la estructura difractiva de orden cero presenta a este respecto una profundidad de rejilla de 50 nm a 500 nm, en particular 200 nm, y/o una frecuencia espacial de 500 líneas/mm a 3000 líneas/mm, en particular de 1100 líneas/mm a 2500 líneas/mm.

40 **[0104]** La capa de un material altamente refractivo presenta preferentemente un espesor de 30 nm a 200 nm, en particular 100 nm, y/o presenta un índice de refracción (parte real) de al menos 1,7, preferiblemente de al menos 1,9, más preferiblemente de al menos 2,1 para el rango espectral visible.

[0105] Preferiblemente, un efecto óptico generado por la estructura en relieve presenta al menos por zonas una paralaje en dos direcciones espaciales ortogonales entre sí.

45

[0106] Esto se puede utilizar para mostrar una o más direcciones de observación preferidas del elemento de seguridad, que también se pueden utilizar al capturar la secuencia de imágenes. Por ejemplo, el efecto óptico puede ser una cruz o un punto que aparentemente se mueve en dos direcciones espaciales al inclinar el elemento de seguridad. La dirección preferida se puede mostrar entonces porque, con una orientación correcta del elemento de seguridad, la cruz o el punto aparecen centrados en un marco circundante. Este efecto óptico es preferiblemente difractivo (por ejemplo, por medio de una rejilla cruzada difractiva y/o una estructura mate) y sirve como referencia óptica para la dirección preferida.

50

[0107] Preferiblemente, para verificar si está presente la al menos una información óptica predeterminada, se aplica un filtro, en particular un filtro de trama y/o un filtro de color a la al menos una imagen individual de la secuencia de imágenes.

55

[0108] De esta manera, la al menos una información óptica predeterminada se puede extraer y verificar de manera sencilla a partir de la imagen individual. La aplicación de un filtro semejante no significa un gran esfuerzo de cálculo y, por lo tanto, también se puede llevar a cabo en dispositivos de mano con poca potencia de cálculo.

60

[0109] Además, es conveniente si la al menos una información óptica predeterminada configura un código, en particular un código de barras difractivo.

65

[0110] De este modo también se puede integrar información compleja en el elemento de seguridad, que hace que la autenticación sea especialmente segura. En el uso de técnicas adecuadas para la fabricación del elemento de seguridad, por ejemplo, en el uso de hologramas generados por ordenador, entonces también se puede incorporar información de individualización, tal como, por ejemplo, números de serie, códigos de barras o similares, en el elemento de seguridad. Por ejemplo, la información de individualización se puede reconocer como efecto que aparece flotante ópticamente cuando se activa la lámpara de flash del equipo de mano. Sin embargo, el efecto ópticamente flotante no debe ser visible con iluminación difusa y puede presentar una relación en su significado y/o posición con el motivo restante del OVD, lo que aumenta la seguridad contra la falsificación.

10 **[0111]** Se prefiere además cuando se verifica si está presente al menos otra información óptica en al menos una imagen individual de la secuencia de imágenes.

[0112] Por ejemplo, la al menos otra información óptica puede ser a este respecto una información de individualización, en particular una información de individualización aleatoria, pseudoaleatoria y/o generada algorítmicamente.

[0113] De este modo se puede autenticar individualmente cada objeto individual, provistos de una característica de seguridad semejante. Por ejemplo, la información de individualización puede estar vinculada a un número de serie que se puede consultar durante la identificación y autenticación en una base de datos para proporcionar información adicional y mejorar la seguridad de la autenticación.

[0114] A este respecto, es conveniente si la información de individualización se forma por una distancia de al menos un elemento de imagen de la al menos una información óptica con respecto a al menos un elemento de imagen de la al menos otra información óptica.

25 **[0115]** Así, la información óptica adicional se puede integrar, por ejemplo, sin problemas en la al menos una información óptica, de modo que no se pueda reconocer a simple vista o solo de forma costosa.

[0116] Además, es conveniente si la información de individualización se forma por un código de barras, en particular un código de barras difractivo.

[0117] Este código de barras difractivo puede contener una información fija general o una información que está expuesta de forma idéntica en un cierto número de elementos de seguridad, por ejemplo, un número de lote o un código de identificación del producto. Pero, la información también puede ser diferente en cada elemento de seguridad individual y, por lo tanto, única, por ejemplo, contener una información individualizada o específica del ítem, es decir, una información no recurrente. Esta información única se puede calcular a este respecto a través de un algoritmo, ser o generarse de forma pseudoaleatoria o aleatoria.

[0118] Por ejemplo, la información óptica predeterminada puede presentar un código de barras individual como código de barras 1D o código de barras 2D, o un grupo de al menos dos o más códigos de barras semejante, que en conjunto dan como resultado una información que se produce varias veces como se ha descrito anteriormente o que es única, o que la información de los códigos de barras individuales se complementa a este respecto. A este respecto, los códigos de barras individuales pueden estar dispuestos uno al lado del otro, en particular adyacentes o completamente superpuestos o solo por secciones.

45 **[0119]** Por ejemplo, los códigos de barras pueden estar formados en cada caso por una capa de reflexión estructurada y codificada con ello, en particular una capa metálica eliminada por zonas o también por una capa de estructura superficial, que representa un código difractivo, con estructuras en relieve difractivas y/o no difractivas. Uno de los planos de información también puede presentar una codificación no ópticamente variable, por ejemplo, en forma de una codificación de color impresa, por ejemplo, un código QR. Sin embargo, la codificación de color impresa también puede presentar componentes ópticamente variables y/u ópticamente activos, por ejemplo, pigmentos, que muestran efectos dependientes del ángulo de observación y/o dependientes del espectro de luz irradiado, por ejemplo, que son fosforescentes o luminiscentes.

55 **[0120]** En una realización preferida, un código de barras difractivo como código de barras predeterminado fijo se puede modificar por medio de una modificación posterior, de modo que el código de barras contenga una información individual después de la modificación. Para ello, por ejemplo, la capa de reflexión del código de barras difractivo se puede eliminar o modificar localmente, por ejemplo, mediante ablación por láser, de modo que se elimina o modifica igualmente el efecto difractivo ópticamente variable en la zona de la capa de reflexión eliminada o modificada. Otra posibilidad es la sobreimpresión local y, por lo tanto, la cobertura local y, por lo tanto, la eliminación del efecto difractivo ópticamente variable del código de barras difractivo.

60 **[0121]** Según la disposición de los planos de información individuales, los códigos de barras individuales se pueden leer individualmente o conjuntamente, en particular bajo un ángulo de observación o ángulo de iluminación común o también bajo diferentes ángulos de observación o ángulos de iluminación. Los planos de información también

se pueden combinar a este respecto con planos de información legibles no ópticamente, sino en particular eléctrica o electrónicamente, por ejemplo, una capa magnética con codificación magnética inscrita y/o un chip de memoria con codificación de memoria electrónica inscrita.

5 **[0122]** En general, a este respecto, la al menos otra información óptica se puede superponer a la al menos una información óptica predeterminada. La información óptica adicional puede estar integrada a este respecto directamente en la al menos una información óptica predeterminada, o se puede formar, por ejemplo, por otra capa superpuesta. Alternativamente, también es posible separar la al menos otra información óptica de la al menos una información óptica, por ejemplo, mediante una disposición adyacente que no se superponga.

10

[0123] Además, es conveniente que la al menos otra información óptica comprenda una o varias estructuras de los siguientes grupos:

- estructuras en relieve, en particular una estructura difractiva, una estructura de difracción de orden cero, una rejilla
- 15 Blaze, una macroestructura, en particular una estructura de lente o una estructura de micropisma, una superficie de espejo, una estructura mate, en particular una estructura mate anisotrópica o isotrópica,
- estructuras impresas, en particular que comprenden colorantes y/o pigmentos en color, ópticamente activos y/u ópticamente variables
- estructuras magnéticas,
- 20 - capas parcialmente metalizadas y/o capas HRI parciales.

[0124] Preferiblemente, la al menos una información óptica predeterminada es un retrato, que se reconoce en la etapa b) por medio de un algoritmo biométrico.

25 **[0125]** Las características biométricas son especialmente complejas, de modo que se obtiene un elemento de seguridad especialmente a prueba de falsificaciones. Al mismo tiempo, la autenticación fiable con algoritmos biométricos conocidos también es posible sin problemas en el marco de la capacidad de cálculo de un equipo de mano.

30 **[0126]** Preferentemente, antes y/o durante la captura de la secuencia de imágenes en la etapa a) se muestran instrucciones a un usuario del equipo de mano en una pantalla del equipo de mano sobre en qué posición relativa y/o a qué distancia con respecto al elemento de seguridad se debe sujetar y/o mover el equipo de mano durante la captura de la secuencia de imágenes. Estas instrucciones se pueden basar en datos de medición del sensor de posición y/o sensor de movimiento del equipo de mano o también ser independientes de los mismos.

35

[0127] Por lo tanto, se puede garantizar que incluso los usuarios inexpertos puedan capturar una secuencia de imágenes que sea adecuada para la autenticación fiable del elemento de seguridad. Si la captura de una secuencia de imágenes no produce imágenes individuales adecuadas, entonces también se puede mostrar al usuario información adicional que, por ejemplo, le indique un error en la captura de la secuencia de imágenes y le instruya cómo evitarlo.

40 Al usuario también se le puede mostrar información concreta adicional sobre la base de que características puede reconocer falsificaciones o se puede mostrar información sobre donde es más probable encontrar elementos de seguridad/objetos reales y donde se encuentra con alta probabilidad falsificaciones.

[0128] Además, es conveniente que en la etapa a) se capture las imágenes individuales de la secuencia de

45 imágenes con una resolución de al menos 0,5 pares de líneas/mm, preferiblemente de al menos 5 pares de líneas/mm, más preferiblemente de al menos 20 pares de líneas/mm.

[0129] Una resolución semejante es suficiente para posibilitar un reconocimiento fiable de la al menos una información óptica predeterminada y se puede alcanzar sin problemas por equipos de mano comunes, tales como

50 teléfonos inteligentes, tabletas o PDAs.

[0130] Preferiblemente, antes de la captura de las imágenes individuales en la etapa a) se mide una iluminancia y con una iluminancia de menos de 800 lx se activa una fuente de luz del equipo de mano. Esto se puede realizar automáticamente desde el equipo de mano o también manualmente por el usuario.

55

[0131] De este modo se garantiza que el elemento de seguridad esté suficientemente iluminado para posibilitar una autenticación fiable. Una iluminancia de 800 lx corresponde a este respecto aproximadamente a una

oficina normalmente iluminada.

60

[0132] Además, es ventajoso si en presencia de la al menos una información óptica predeterminada se emite una confirmación de autenticación en un dispositivo de salida, en particular una pantalla.

[0133] Por tanto se le comunica claramente al usuario si el elemento de seguridad examinado es auténtico o

65 no. Sobre esta base, a continuación se puede transmitir información adicional al usuario.

[0134] Preferentemente, el paso b) se lleva a cabo por medio de un programa de software ejecutado en un dispositivo de cálculo del equipo de mano.

5 **[0135]** En este caso, la autenticación se puede realizar directamente *in situ*, sin que los datos de la secuencia de imágenes tengan que transmitirse desde el equipo de mano a otro equipo. Esto permite una realización especialmente flexible del procedimiento.

10 **[0136]** Además, es ventajoso que el programa de software y/o una base de datos asociada al programa de software se actualicen a intervalos predeterminados, en particular antes de cada realización del procedimiento, a través de una conexión de telecomunicación, en particular conexión a Internet.

15 **[0137]** De este modo, la información sobre elementos de seguridad nuevos o modificados se puede transmitir al programa de software y la al menos una información óptica predeterminada o los algoritmos utilizados para su verificación se pueden adaptar en consecuencia. Además, el software y/o el usuario pueden recibir información sobre nuevas falsificaciones conocidas, así como sus particularidades específicas, de modo que se facilite su reconocimiento.

20 **[0138]** También es posible que la etapa b) se lleve a cabo por medio de un programa de software ejecutado en un dispositivo de cálculo diferente del equipo de mano, al que se transmite la secuencia de imágenes capturada en la etapa a) a través de una conexión de telecomunicación, en particular una conexión de Internet.

25 **[0139]** En el caso de un dispositivo de cálculo semejante se trata preferentemente de un servidor centralizado que puede hacerse cargo de la evaluación de las secuencias de imágenes de una pluralidad de equipos manuales. El servidor comprende a este respecto al menos un procesador, dispositivos de almacenamiento de datos volátiles y no volátiles, así como dispositivos de entrada y salida adecuados. En este caso, el equipo de mano actúa como cliente en una estructura cliente-servidor.

30 **[0140]** Dado que en un servidor semejante está a disposición una capacidad de cálculo claramente mayor que en un equipo de mano, también se pueden ejecutar algoritmos de procesamiento de imágenes y algoritmos de reconocimiento de patrones más complejos. Además, también hay más espacio de almacenamiento disponible en un servidor semejante, de modo que se pueden almacenar bases de datos más grandes con características de elementos de seguridad auténticos y falsificaciones conocidas.

35 **[0141]** Ventajosamente, en ausencia de la al menos una información óptica y/o de la estructura difractiva en la etapa b), se envía un mensaje al dispositivo de cálculo diferente del equipo de mano, que comprende una información de lugar y/o tiempo.

40 **[0142]** En otras palabras, las falsificaciones encontradas de elementos de seguridad se transmiten al dispositivo de cálculo, que preferiblemente es un servidor central. A partir de la información de lugar y/o tiempo asociada a las falsificaciones encontradas se pueden extraer conclusiones, en su caso, sobre el origen de las falsificaciones, lo que facilita la localización de los falsificadores y adicionalmente se puede transmitir a otros usuarios como información de advertencia.

45 **[0143]** Preferiblemente, en otra etapa c) se verifica si al menos otra información óptica predeterminada está presente en al menos una imagen individual de la secuencia de imágenes, que está presente en el caso de una falsificación conocida del elemento de seguridad ópticamente variable y no está presente en el caso de un verdadero elemento de seguridad ópticamente variable.

50 **[0144]** Además, es conveniente que, en ausencia de la al menos una información óptica predeterminada y en ausencia de la al menos otra información óptica predeterminada, se transmita un mensaje al dispositivo de cálculo diferente del equipo de mano, que comprenda una información de lugar y/o tiempo, así como al menos una imagen individual de la secuencia de imágenes.

55 **[0145]** Por lo tanto, si un elemento de seguridad verificado resulta no ser auténtico y al mismo tiempo no se puede identificar como una falsificación conocida, entonces está presente una nueva falsificación. La información de la imagen capturada del elemento de seguridad falso hasta ahora desconocido se transmite entonces al servidor, de modo que la nueva falsificación se puede investigar. Las características propias de la nueva falsificación se pueden transmitir entonces de nuevo de vuelta a los equipos de mano como información óptica adicional predeterminada, de modo que la nueva falsificación se pueda reconocer de manera especialmente fiable. Esto puede ser apoyado por un software "de aprendizaje" con algoritmos de entrenamiento correspondientes. Las nuevas falsificaciones reconocidas alimentan a este respecto una base de datos sobre la base de la que el software se entrena recursivamente y, por lo tanto, puede reconocer mejor de nuevo las falsificaciones emergentes.

65 **[0146]** Para llevar a cabo un procedimiento semejante es adecuado un equipo, en particular un equipo de mano

con un sensor para capturar una secuencia de imágenes con al menos una imagen individual de un elemento de seguridad y un dispositivo de control, que está configurado de modo que realiza las siguientes etapas:

- 5 a) captura de una secuencia de imágenes con al menos una imagen individual del elemento de seguridad por medio del sensor;
- b) verificación de si está presente al menos una información óptica predeterminada en al menos una imagen individual de la secuencia de imágenes.

10 **[0147]** Ejemplos de realización de la invención se explican a continuación a modo de ejemplo con ayuda de las figuras. Muestran:

- Fig. 1: una representación esquemática de un elemento de seguridad y un equipo de mano durante la autenticación del elemento de seguridad;
- 15 Fig. 2: una representación esquemática de un elemento de seguridad con una característica de autenticación visualmente reconocible;
- Fig. 3: una representación esquemática de un elemento de seguridad con una característica de autenticación visualmente no reconocible ópticamente variable;
- Fig. 4: una representación esquemática de un elemento de seguridad alternativo con una característica de autenticación visualmente no reconocible ópticamente variable;
- 20 Fig. 5: una representación esquemática de un elemento de seguridad alternativo con una característica de autenticación visualmente reconocible;
- Fig. 6: una vista en detalle de la estructura de rejilla de un elemento de seguridad con una rejilla curvada en forma de serpentín;
- Fig. 7: una vista en detalle alternativa de la estructura de rejilla de un elemento de seguridad con rejilla curvada en
- 25 forma de serpentín;
- Fig. 8: una vista en detalle alternativa de la estructura de rejilla de un elemento de seguridad con rejilla curvada en forma de serpentín;
- Fig. 9: un registro de microscopio electrónico de una rejilla según una de las figuras 7 u 8;
- Fig. 10: una vista en detalle de un elemento de seguridad con zonas reticuladas con diferentes ángulos de azimut;
- 30 Fig. 11: una vista en detalle de un elemento de seguridad con zonas reticuladas con diferentes frecuencias espaciales;
- Fig. 12: una representación esquemática de un elemento de seguridad alternativo con una característica de autenticación visualmente no reconocible ópticamente variable con y sin filtrado de trama de la imagen capturada;
- Fig. 13: una representación esquemática de un elemento de seguridad alternativo con una característica de autenticación visualmente no reconocible ópticamente variable con zonas de diferentes colores reticuladas entre sí,
- 35 así como un diagrama de color correspondiente;
- Fig. 14: una representación esquemática de un elemento de seguridad alternativo con efecto de paralaje a lo largo de dos ejes ortogonales;
- Fig. 15: una representación esquemática de otro elemento de seguridad alternativo con efecto de paralaje a lo largo de dos ejes ortogonales;
- 40 Fig. 16: una ilustración del efecto Moiré entre una estructura de trama en un elemento de seguridad y un fotosensor reticulado;
- Fig. 17: un diagrama para ilustrar la intensidad de difracción en función de la longitud de onda y el período de rejilla;
- Fig. 18: diagramas comparativos del espectro solar y del espectro de una luz de flash de un teléfono inteligente; en este gráfico se muestra solo una curva.
- 45 Fig. 19: un diagrama para ilustrar la intensidad de difracción en función de la longitud de onda y el período de rejilla en caso de polarización eléctrica transversal;
- Fig. 20: un diagrama para ilustrar la intensidad de difracción en función de la longitud de onda y el período de rejilla en caso de polarización magnética transversal;
- Fig. 21: una representación esquemática de un elemento de seguridad con una estructura mate anisotrópica;
- 50 Fig. 22 A-C: una representación esquemática de tres formas de realización alternativas de un elemento de seguridad con código de barras bidimensional;
- Fig. 23 A-C: una representación esquemática de tres formas de realización alternativas de un elemento de seguridad con un código de barras bidimensional y un código aleatorio individualizado;
- Fig. 24 A-C: una representación esquemática de una superposición de un código difractivo y una información de
- 55 individualización aleatoria;
- Fig. 25: una representación esquemática de una información de individualización con dos estructuras difractivas, adyacentes y que varían a lo largo de su longitud;
- Fig. 26: una representación esquemática de una superposición adicional de un código difractivo y una información de individualización aleatoria;
- 60 Fig. 27: una representación esquemática de una superposición de un código impreso y una información de individualización aleatoria;
- Fig. 28 A-D: una representación esquemática de una combinación de un código de barras y un código de individualización difractivo en forma de tira.

65 **[0148]** Un elemento de seguridad 1 para la protección contra la falsificación de un documento 2 presenta

información ópticamente detectable que comprende preferentemente al menos un motivo 11 visualmente perceptible, como muestra la fig. 1. El motivo 11 puede ser un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número. En lugar de un documento, también puede ser un producto comercial y su etiqueta y/o embalaje, o un tique o cupón.

- 5 **[0149]** Preferentemente, el motivo visualmente perceptible se genera al menos parcialmente mediante una estructura de rejilla del elemento de seguridad 1. Por una estructura de rejilla se debe entender a este respecto una estructura difractiva, una estructura de difracción de orden cero, una rejilla Blaze, una estructura de rejilla sinusoidal lineal o cruzada o una estructura de rejilla binaria, una macroestructura, en particular una estructura de lente o estructura de micropisma que actúa de forma refractiva, una superficie de espejo, una estructura mate, en particular
- 10 una estructura mate anisotrópica o isotrópica o combinaciones de las mismas. Tales estructuras de rejilla son ópticamente variables, es decir, así muestran diferentes efectos ópticos con diferentes ángulos de iluminación o de observación. El motivo 11 también se puede generar parcialmente a partir de estructuras no ópticamente variables, por ejemplo, capas aplicadas por medio de impresión, en particular capas de pintura. Otro ejemplo de una estructura no ópticamente variable es el sustrato sobre el que está aplicado el elemento de seguridad 1, por ejemplo, de
- 15 materiales como papel o plástico, que no presentan propiedades ópticamente variables.

- [0150]** Para garantizar una seguridad contra la falsificación especialmente buena, es posible incorporar información en la estructura de rejilla o en el motivo 11, que no se puede reconocer sin más como tal. Un ejemplo de ello se muestra en la fig. 2. Al motivo 11 visualmente reconocible está superpuesta aquí una disposición de píxeles 12
- 20 distribuidos según un patrón predeterminado. La superposición puede ser aditiva, es decir, la estructura de motivo 11 y la estructura de patrón 12 se complementan entre sí, o la superposición es una operación XOR, es decir, la estructura de patrón 12 reemplaza la estructura de motivo 11 en las posiciones de superposición de ambas estructuras. La disposición de los píxeles 12 y su posición relativa con respecto al motivo 11 forma otra información, que se puede utilizar para la autenticación del elemento de seguridad 1.

- 25 **[0151]** La figura 3 muestra otra posibilidad para la integración de otra información en el motivo 11. En este caso, una superficie libre 13 en el motivo 11 está llena con una estructura difractiva 14, que configura la información adicional. Tales estructuras difractivas 14 también se pueden integrar en disposiciones de líneas de guillotina 15, como muestra la fig. 4.

- 30 **[0152]** La información visualmente reconocible también se puede integrar en el motivo 11 como se representa en la fig. 5. Aquí, el motivo 11 es una palabra escrita en la que una letra 16 está colocada en otro tipo de letra y, por lo tanto, es diferente de las otras letras de la palabra escrita.

- 35 **[0153]** Es especialmente ventajoso si el elemento de seguridad 1 se autentifica automáticamente. Para ello se captura con un sensor de imagen 31 de un equipo 3 una secuencia de imágenes del elemento de seguridad 1. En el caso del equipo 3 se trata preferentemente de un teléfono inteligente, una tableta, una PDA u otro equipo de mano con un sensor de imagen.

- 40 **[0154]** La secuencia de imágenes comprende al menos dos imágenes individuales. En condiciones de poca luz, en particular con una iluminancia de menos de 800 lx, es decir, una iluminación que es más oscura que la iluminación media de la habitación, también se puede conectar un dispositivo de iluminación 32, es decir, una lámpara o un flash, del equipo 3. Debido a la variabilidad óptica de la apariencia óptica de los OVD, es conveniente que se conozcan las propiedades específicas del dispositivo de iluminación 32 del equipo 3 empleado, en particular el
- 45 espectro de la luz emitida y la posición relativa del dispositivo de iluminación 32 con respecto al sensor de imagen 31, a partir de lo cual se puede determinar de forma fiable la dirección de la luz irradiada por el dispositivo de iluminación 32 hacia el OVD. De este modo se puede determinar al menos esta magnitud de influencia sobre el efecto óptico de manera comparativamente exacta.

- 50 **[0155]** Además del sensor de imagen 31, el equipo 3 presenta preferentemente uno o varios procesadores y/o módulos de entrada y salida, un sistema operativo que se ejecuta en esta plataforma de hardware y otros componentes de software que se ejecutan sobre este, en particular programas de control, a través de cuyo desarrollo se realizan las funciones del equipo 3.

- 55 **[0156]** El sensor utilizado es por lo general un sensor electrónico digital, por ejemplo, un sensor CCD (CCD = charge coupled device [dispositivo acoplado por carga]). A este respecto, se emplean preferiblemente matrices CCD, es decir, disposiciones CCD en las que los CCD individuales están dispuestos en una matriz bidimensional. Las imágenes individuales generadas por un sensor semejante están presentes entonces en forma de una matriz de píxeles, donde cada píxel corresponde a un único CCD del sensor. Preferiblemente, un sensor semejante presenta al
- 60 menos una resolución de 0,5 megapíxeles, de manera especialmente preferible de más de 2 megapíxeles. Para la resolución óptica resultante de ello es importante la calidad de la óptica de la lente que interactúa con el sensor.

- [0157]** Para detectar la variabilidad óptica del elemento de seguridad 1, la secuencia de imágenes comprende una pluralidad de imágenes individuales del elemento de seguridad, en particular más de 2 imágenes individuales del
- 65 elemento de seguridad. La secuencia de imágenes puede ser a este respecto una pluralidad de imágenes individuales

creadas discretamente, que no están en relación temporal, pero también se puede tratar de una lámina, es decir, se puede componer de imágenes individuales, que están capturadas a un intervalo temporal predeterminado, en particular con una frecuencia de captura de 5 a 60 imágenes por segundo.

5 **[0158]** Preferentemente, a este respecto, durante la captura se modifica el ángulo de observación, es decir, se pivota el equipo 3 con respecto al elemento de seguridad, de modo que durante la captura la información óptica formada por la estructura de rejilla del elemento de seguridad 1 cambia desde la dirección de observación del equipo 3.

10 **[0159]** Preferentemente, al usuario se le muestra a este respecto en una pantalla del equipo 3, como tiene que mover el teléfono inteligente con respecto al elemento de seguridad 1, para obtener una secuencia de imágenes evaluable de forma óptima. Durante la captura de la secuencia de imágenes se puede medir además, por medio de un sensor de posición del equipo 3, la posición relativa entre el equipo 3 y el elemento de seguridad 1, de modo que para cada imagen individual se conozca el respectivo ángulo de observación.

15 **[0160]** La evaluación de la secuencia de imágenes así capturada se puede realizar directamente en el equipo 3. A este respecto, las imágenes de la secuencia de imágenes se almacenan digitalmente en una memoria del equipo 3 y se procesan por medio de un procesador del equipo 3, que ejecuta un software adecuado.

20 **[0161]** A este respecto se verifica en primer lugar si el motivo 11 está presente en al menos una imagen individual de la secuencia de imágenes. A este respecto, el motivo 11 puede ser todo el diseño del propio elemento de seguridad o representar solo un aspecto parcial del mismo. De este modo se garantiza que la al menos una imagen individual represente sobre todo el elemento de seguridad a autenticar. Si este no es el caso, se puede prescindir de investigaciones adicionales y se advierte al usuario que las imágenes capturadas por medio del sensor 31 son
25 inadecuadas para el propósito de la autenticación y, si es necesario, se deben capturar nuevamente.

[0162] Las imágenes individuales de la secuencia de imágenes se analizan entonces con el algoritmo de Haar-Cascade. Esto se basa en la evaluación de una pluralidad de las llamadas características "similares a Haar" en la imagen individual. En este caso se trata de estructuras que están relacionadas con ondas de Haar, es decir, ondas
30 rectangulares de una longitud de onda predeterminada. A este respecto, en dos dimensiones se trata simplemente de una región rectangular adyacente, alternativamente clara y oscura en la imagen. Al desplazar una máscara rectangular sobre la imagen individual, se determinan las características "similares a Haar" presentes. Las características "similares a Haar" presentes se comparan entonces con aquellas que deben estar presentes en el motivo 11. Esto se puede realizar mediante una cascada de filtro.

35 **[0163]** El algoritmo de Haar-Cascade tiene la ventaja de necesitar especialmente poco tiempo de cálculo y recursos informáticos. Sin embargo, también es posible utilizar otros algoritmos de reconocimiento de imágenes.

[0164] Para verificar si el motivo 11 está presente, se lleva a cabo una comparación de al menos un cuadro
40 individual con un conjunto de datos de entrenamiento previamente capturado. Esto se puede realizar en el marco del algoritmo de Haar-Cascade descrito, pero también por medio de otros algoritmos.

[0165] El reconocimiento de imágenes se basa en una forma de aprendizaje por ordenador. Al algoritmo no se le especifican parámetros concretos mediante los cuales se realiza una clasificación del contenido de la imagen, sino
45 que el algoritmo aprende estos parámetros sobre la base del conjunto de datos de entrenamiento.

[0166] Para crear el conjunto de datos de entrenamiento, se captura una pluralidad de imágenes, donde un primer subconjunto de las imágenes presenta en cada caso un motivo 11 y un segundo subconjunto de las imágenes no presenta en cada caso el motivo 11, y donde a cada imagen del primer subconjunto se asignan todas las
50 coordenadas de imagen respectivas de las características a reconocer del motivo 11.

[0167] Sobre la base del primer y segundo subconjunto, así como de las coordenadas de imagen asignadas, entonces se lleva a cabo un entrenamiento del algoritmo de reconocimiento de imágenes. De este modo, el algoritmo aprende a clasificar correctamente las imágenes y, dado el caso, a ignorar factores de interferencia incorporados
55 conscientemente en el conjunto de datos de entrenamiento, tales como, por ejemplo, reflexiones en las imágenes, casos de sombras aleatorios o similares.

[0168] Si se puede confirmar la presencia del motivo 11, a continuación se determina el contorno del motivo 11 a partir de al menos una imagen individual de la secuencia de imágenes. En comparación con el reconocimiento
60 de imágenes simple descrito anteriormente, que solo proporciona una clasificación de sí/no o una declaración de probabilidad de si el motivo 11 está presente en la imagen individual, así se proporciona información adicional. En particular, sobre la base del contorno determinado se puede comprobar la presencia o ausencia de características detalladas del motivo 11. Esto proporciona información adicional que puede contribuir a autenticar el elemento de seguridad.

65

[0169] Para la autenticación del elemento de seguridad 1, por lo tanto, solo se puede usar un detalle de todo el diseño. Esto permite ocultar también características de seguridad visualmente reconocibles en el diseño del elemento de seguridad 1.

5 **[0170]** Para determinar el contorno del motivo 11, se puede utilizar un algoritmo de detección de bordes como el algoritmo Canny.

[0171] Para aplicar el algoritmo de Canny a las imágenes en color, estas se deben convertir en primer lugar a escala de grises. En las imágenes en escala de grises, los bordes se caracterizan por fuertes fluctuaciones de brillo
10 entre píxeles adyacentes y, por lo tanto, se pueden describir como discontinuidades de la función de valor de grises de la imagen.

[0172] Dado que tales discontinuidades también se pueden causar por ruido de imagen, es conveniente que en la ejecución del algoritmo de detección de bordes se lleve a cabo un filtrado de ruido, en particular por medio de
15 un filtro gaussiano con un tamaño de núcleo (kernel) preferido de 3 a 7.

[0173] Por núcleo se entiende en este caso una matriz de convolución que se aplica a la información de la imagen. La matriz de convolución del filtro gaussiano corresponde a la distribución normal y actúa como filtro de paso bajo. Por lo tanto, el valor de gris de un píxel filtrado corresponde a la media ponderada con la distribución normal de
20 los valores grises de los píxeles circundantes hasta una distancia máxima, definida por el tamaño de núcleo. Las estructuras más pequeñas, que se originan por el ruido se pierden, mientras que las estructuras principales del motivo 11 se conservan.

[0174] Preferentemente, en la realización del algoritmo de reconocimiento de bordes se lleva a cabo una
25 detección de bordes mediante la aplicación de un operador Sobel en al menos una dirección preferida de la al menos una imagen individual, preferentemente en dos direcciones preferidas ortogonales de la al menos una imagen individual.

[0175] El operador Sobel también es un operador de pliegue que actúa como un diferenciador discreto. Debido
30 al pliegue de la imagen con el operador Sobel se obtienen las derivadas parciales de la función de valor de gris en las dos direcciones preferidas ortogonales. A partir de esto se puede determinar entonces la dirección del borde y el grosor del borde.

[0176] Después de la diferenciación de los datos de valor de grises se lleva a cabo a continuación un filtrado
35 de bordes. Esto se puede realizar, por ejemplo, por medio de una llamada non-maximum suppression, que garantiza que solo se conserven los máximos a lo largo de un borde, de modo que un borde no sea más ancho que un píxel perpendicular a su dirección de extensión.

[0177] Después del filtrado se puede llevar a cabo entonces una determinación basada en el valor umbral de
40 las coordenadas de imagen del contorno del motivo 11. Por lo tanto, se determina a partir de qué grosor de borde se debe contar un píxel para un borde.

[0178] Para ello se puede utilizar, por ejemplo, un procedimiento basado en histéresis. Para ello se establecen
45 dos valores umbral T_1 y T_2 , donde T_2 es mayor que T_1 . Un píxel con un grosor de borde mayor que T_2 se considera parte de un borde. Todos los píxeles conectados a este píxel con un grosor de borde mayor que T_1 se atribuyen igualmente a este borde.

[0179] Por lo tanto, se obtienen las coordenadas de imagen de todos los píxeles correspondientes a un borde
50 del motivo 11 en la imagen individual examinada. Estos se pueden analizar más a fondo, por ejemplo, para reconocer formas geométricas simples.

[0180] A continuación, la imagen individual se puede dividir en al menos dos regiones parciales sobre la base de las coordenadas de imagen determinadas del motivo 11 y para cada región parcial las coordenadas de imagen determinadas del contorno se pueden comparar con las coordenadas de consigna correspondientes y a partir de esto
55 se determina en particular la presencia y/o el tamaño y/o la posición relativa de contornos predeterminados. A este respecto, las regiones parciales se seleccionan teniendo en cuenta la posición de consigna de las características del motivo 11 utilizadas para la autenticación.

[0181] Para autenticar como auténtico un elemento de seguridad así examinado, a este respecto no debe
60 existir necesariamente una correspondencia absoluta, también es posible especificar rangos de tolerancia para desviaciones permitidas. Las desviaciones no deben indicar necesariamente una falsificación, ya que los artefactos ópticos, las distorsiones de perspectiva, el desgaste o la contaminación en uso o efectos similares, que pueda ocurrir al capturar la imagen individual, también pueden menoscabar la correspondencia con el original.

65 **[0182]** Por ejemplo, se puede seleccionar una región parcial de la imagen individual, que está posicionada en

una posición predeterminada con respecto al contorno del motivo 11 y que comprende al menos un píxel 12 y/o al menos un grupo de píxeles de la imagen individual, y se compara al menos una propiedad del al menos un píxel 12 y/o del al menos un grupo de píxeles de la al menos una región parcial seleccionada con un valor de consigna correspondiente. Con ello se puede verificar, por ejemplo, la presencia del patrón de píxeles mostrado en la fig. 2.

5

[0183] También se pueden verificar desviaciones en la tipografía, como se representa en la fig. 5, sobre la base de los datos de contorno determinados.

[0184] Adicionalmente se puede verificar si el elemento de seguridad comprende una estructura ópticamente variable. Para ello, se comparan dos imágenes individuales de la secuencia de imágenes, que se han capturado con diferentes condiciones de visualización y/o de iluminación.

[0185] Si estas imágenes individuales difieren lo suficiente, entonces se puede partir de la presencia de una estructura ópticamente variable. Si este no es el caso, entonces está presente una copia estática. A este respecto, es suficiente comparar en cada caso píxeles y/o grupos de píxeles correspondientes de las imágenes individuales, por ejemplo, con respecto a su brillo o su valor de color. De esta manera, se puede determinar la identidad o no identidad de las imágenes individuales sin un gran esfuerzo de procesamiento.

[0186] Por lo tanto, para verificar la identidad de las imágenes individuales no se deben reconocer estructuras en las imágenes individuales, es suficiente considerar los cambios típicos de OVD debido al ángulo de observación o iluminación modificado a nivel de píxeles. Esto es especialmente eficiente y ahorra tiempo de cálculo.

[0187] De forma alternativa o adicional al reconocimiento descrito de características macroscópicas del motivo 11, también se pueden integrar características de autenticación visualmente no reconocibles en el elemento de seguridad 11, por ejemplo, en la estructura de rejilla 14 mostrada en las fig. 3 y 4. Estas se pueden utilizar para una autenticación adicional del elemento de seguridad 11 para aumentar la seguridad contra la falsificación.

[0188] Por ejemplo, es posible rastrillar regiones que se diferencian en al menos un parámetro de rejilla entre sí (disposición entrelazada), de modo que se obtenga visualmente una superficie homogénea. Sin embargo, las diferencias en la estructura de rejilla se pueden clarificar con el sensor 31 del equipo 3.

[0189] El periodo de rejilla se selecciona a este respecto de modo que no se puede clarificar con el ojo humano. A este respecto, los periodos de trama preferidos son de 10 μm a 300 μm . Las regiones pueden diferir, por ejemplo, en la frecuencia espacial, el ángulo de azimut, la profundidad de relieve, la forma de relieve, una fase de la estructura en relieve, un período de una variación de azimut, una variación de profundidad de relieve y/o una variación de frecuencia espacial de una rejilla de una o dos dimensiones, una rugosidad media de una estructura mate y/o la dirección preferida de una estructura mate anisotrópica.

[0190] Un ejemplo de una estructura semejante se muestra en las figuras 6 a 9. Mientras que las rejillas habituales presentan líneas de rejilla rectas con una frecuencia espacial predeterminada y un ángulo de azimut predeterminado, el ángulo de azimut de la rejilla 14 varía en las figuras mencionadas con la posición espacial. De esta manera se pueden generar las rejillas 14 curvadas en forma de serpentín, parabólica o circular. La periodicidad de esta variación se encuentra por debajo del límite de resolución del ojo humano, en particular por debajo de 300 μm , preferentemente por debajo de 150 μm , de modo que la rejilla 14 parezca homogénea en su totalidad y muestre el mismo efecto óptico en toda su superficie cuando se inclina. Tales rejillas 14 se pueden usar para definir mejor en qué condiciones de visualización y de iluminación aparece un OVD claro u oscuro o específicamente en color.

[0191] Además, con la misma periodicidad que la variación del ángulo azimutal, las regiones 141, 142 de la rejilla 14 se reticulan entre sí. Por lo tanto, esta reticulación no se puede clarificar para el ojo humano. La región 141 forma a este respecto un fondo para las regiones 142 configuradas como motivo.

[0192] En los ejemplos mostrados, las rejillas de las regiones 141 y 142 se distinguen porque la fase de la variación de azimut está desplazada entre las regiones 141 y 142 en 180°. Mientras que esto no es perceptible con el ojo humano a una distancia de observación habitual de 30 cm, estas regiones se pueden clarificar por el sensor 31, de modo que la información representada por la disposición y la forma de las regiones 141, 142 se puede utilizar para autenticar el elemento de seguridad 1.

[0193] Las fig. 7 y 8 muestran una rejilla 14 alternativa bajo distintos ángulos de observación. Las áreas depositadas de forma oscura aparecen bajo el respectivo ángulo de observación para el sensor 31 de forma clara sobre un fondo oscuro. Se puede reconocer que estas áreas se mueven durante la inclinación del elemento de seguridad 1 con respecto al sensor 31. Este efecto también solo se puede percibir con el sensor 31, mientras que la rejilla 14 parece homogénea a simple vista.

[0194] Las regiones 141, 142 se reticulan entre sí en este caso con un período de trama de 100 μm , la frecuencia espacial de la rejilla es de 667 líneas/mm, el período de la variación de azimut es de 80 μm con un cambio

de azimut de +/- 30°.

[0195] Una realización concreta de la rejilla 14 mostrada en las fig. 7 y 8 se muestra en la fig. 9 en una captura de microscopio electrónico. La línea diagonal 143 que recorre la imagen representa el límite entre una región de fondo 5 141 y la región de motivo 142.

[0196] Como muestra la fig. 10, también se pueden reticular entre sí regiones 141, 142 con un ángulo de azimut en cada caso constante, que sin embargo se diferencia entre las regiones 141 y 142 en 180° (disposición intercalada). Las regiones se disponen a este respecto de modo que resulta un motivo 144 desplazado en fase. Para ello es 10 necesaria una rejilla asimétrica, por ejemplo, una rejilla Blaze. A este respecto, las rejillas pueden ser cromáticas (rejillas Blaze con un periodo de aprox. 1 mm) o acromáticas (rejillas Blaze con un periodo de más de 5 mm).

[0197] En las regiones 141, el ángulo de azimut es de 0°, de modo que se hace visible una fuerte flexión de primer orden, mientras que en las regiones 142 con un ángulo de azimut de 180° es visible una ligera difracción de 15 orden -1. El ancho de las regiones, es decir, el periodo de la reticulación, es de aproximadamente 100 µm, de modo que la superficie a su vez parece visualmente homogénea. Sin embargo, mediante la aplicación de un filtro de trama a la imagen capturada con el sensor 31 se puede clarificar el motivo 144.

[0198] Análogamente, también es posible una reticulación de regiones 141, 142, que representan 20 respectivamente estructuras mate anisotrópicas con diferentes orientaciones de azimut o estructuras mate isotrópicas con diferentes características de dispersión. A este respecto, las dimensiones de la trama son las mismas que en la fig. 10. Las regiones 141, 142 se diferencian entonces en su valor de grises. Toda la estructura aparece a su vez visualmente homogénea, pero también se puede clarificar aplicando un filtro de trama sobre la imagen capturada con el sensor 31.

[0199] Asimismo es posible una reticulación de regiones 141, 142 con diferente frecuencia espacial, como se 25 muestra en la fig. 11. Para un ángulo de observación dado, las regiones 141, 142 tienen entonces diferentes colores, pero toda la superficie de la rejilla 14 parece homogénea para el ojo humano. En el ejemplo de la fig. 10, las regiones 141 tienen una frecuencia espacial de 1000 líneas/mm y las regiones 142 de 800 líneas/mm, las regiones están 30 reticuladas entre sí con un periodo de trama de 300 mm. Para el sensor 31 se puede reconocer a su vez el motivo 144 desplazado en fase.

[0200] Para evitar aún mejor que los diferentes colores de las regiones 141, 142 se hagan visibles al bascular el elemento de seguridad 1, es conveniente que las frecuencias espaciales de la rejilla se encuentren más próximas 35 entre sí en las regiones 141, 142. Por ejemplo, la región 141 se puede formar por una rejilla sinusoidal con una frecuencia espacial de 900 líneas/mm y la región 142 por una rejilla sinusoidal con una frecuencia espacial de 800 líneas/mm.

[0201] Otra opción se muestra en la fig. 12. Aquí, las regiones 141, 142 difieren ligeramente en la profundidad 40 de rejilla y, por lo tanto, en la eficiencia, de modo que resulta un par de colores metaméricos. Si, por ejemplo, la eficiencia de la rejilla en las regiones 141, 142 es ligeramente diferente para el rojo, entonces el motivo 144 se puede hacer visible a través de un filtro rojo, como se muestra totalmente a la derecha en la figura. El tamaño de las regiones 141 y 142 se selecciona preferentemente tan pequeño que las regiones son invisibles para el ojo humano, pero aún 45 se pueden clarificar bien con el sensor.

[0202] Como muestra la fig. 13, también se pueden utilizar más de dos regiones 141, 142, 145, 146 diferentes 50 de la rejilla 14. Las regiones 141, 142, que forman el fondo para el motivo 144, aparecen a este respecto en los colores G1 (485 nm) y G2 (620 nm). Las regiones 145 y 146, que forman el motivo 144, aparecen en los colores G3 (450 nm) y G4 (568 nm).

[0203] Debido al escaso periodo de la reticulación de las regiones (menos de 300 µm), el motivo 144 y el fondo 55 aparecen homogéneos, como color mixto de los colores G1+G2 o G3+G4. Como muestra el diagrama de colores representado a la izquierda, los colores se pueden seleccionar de modo que G1+G2 y G3+G4 formen respectivamente el mismo color de mezcla. Para simple vista, por lo tanto, toda la rejilla 14 parece homogénea.

[0204] Sin embargo, mediante el filtrado de color por medio del equipo 3 se puede clarificar a su vez el motivo 144. Esto también es posible con iluminación con diferentes fuentes de luz. Por ejemplo, el equipo 3 puede comparar 60 una imagen individual que se ha capturado a la luz del día con una imagen individual que se ha tomado con luz de flash.

[0205] También se pueden utilizar efectos de color similares para integrar motivos ocultos 144 en un holograma de color real.

[0206] Como muestran las fig. 14 y 15, también se pueden incorporar motivos 11 en el elemento de seguridad 65 1, que al bascular el elemento de seguridad 1 muestran un efecto de paralaje en dos direcciones espaciales. Por lo

tanto, dependiendo del ángulo de observación, el motivo 11 se mueve aparentemente en dos direcciones con respecto a las estructuras circundantes. Bajo condiciones de iluminación típicas, los motivos simples 11, como círculos o cruces, son adecuados en particular para esto, ya que los motivos más complejos se difuminan fácilmente aquí.

5 **[0207]** La posición relativa del motivo 11 con respecto a las estructuras circundantes se puede utilizar ahora para reconstruir a partir de una imagen individual capturada que posición relativa tenía el elemento de seguridad 1 al capturar la imagen individual con respecto al sensor 31. Además de las estructuras circundantes difractivas definidas, también se puede aprovechar la posición relativa con respecto a una imagen de fondo difractiva (imagen fantasma).

10 **[0208]** Tales motivos 11 se pueden reconocer más claramente en la iluminación con fuentes de luz puntuales. Cuando se utilizan motivos complejos se pueden desvanecer casi por completo con la iluminación ambiental difusa. Aquí, una vez más, es posible una comparación entre una imagen individual con iluminación ambiental y una imagen individual con luz de flash. La luz de flash puede hacer visibles a este respecto motivos ocultos 11 que solo se pueden reconocer en caso de iluminación puntual. La posición relativa conocida de la luz del flash con respecto al sensor de
15 imagen también es útil a este respecto.

[0209] En general, las estructuras visualmente no reconocibles, que solo se pueden clarificar con el sensor 31, también se pueden integrar en hologramas generados por ordenador. A este respecto, se puede tratar, por ejemplo, de patrones de puntos o de líneas ocultos, como en la figura 2.

20 **[0210]** Como muestra la fig. 16, además se puede aprovechar el hecho de que los sensores 31 de teléfonos inteligentes o similares están realizados habitualmente como matrices CCD. Los sensores 31 presentan, por tanto, una trama periódica 311 de elementos fotosensibles individuales. Si sobre el elemento de seguridad 1 se aplica una estructura de trama 17 con un ancho de trama adecuado, entonces al capturar la secuencia de imágenes a una
25 distancia adecuada se produce un efecto Moiré entre las dos tramas 311 y 17.

[0211] Los elementos fotosensibles individuales del sensor 31 presentan habitualmente un tamaño de 1,5 a 2 μm y están asimismo distanciados entre sí. Por lo tanto, el período de la trama es de 3 a 4 μm . Por lo tanto, el efecto Moiré con la trama 17 se produce en función del ancho de rejilla de la trama 17 y de la distancia de observación. Esto
30 también se puede utilizar para la autenticación de un elemento de seguridad 1.

[0212] Los efectos ópticos utilizados para la autenticación del elemento de seguridad 1 no tienen que estar a este respecto en el espectro visualmente perceptible. La fig. 17 muestra el comportamiento de reflexión de diferentes rejillas sinusoidales de orden cero en función del período de rejilla y de la longitud de onda. Precisamente en el caso
35 de las rejillas de orden cero, que están provistas de una capa transparente de un material altamente refractivo, tal como, por ejemplo, ZnS, también se puede utilizar la reflexión en la zona infrarroja. Por ejemplo, una rejilla de orden cero con un período de rejilla de 350 nm posee un pico de reflexión en el rango espectral visible a aprox. 470 nm y al mismo tiempo un segundo pico de reflexión a aprox. 760 nm. El pico de reflexión de onda más larga es prácticamente irreconocible para el ojo humano.

40 **[0213]** Sin embargo, la capacidad de evaluación del efecto óptico también depende de la calidad de la luz utilizada para capturar la secuencia de imágenes. La fig. 18 muestra una comparación del espectro solar (arriba) con el espectro de una típica luz de flash de teléfono inteligente (abajo). Como se puede reconocer, está disponible una intensidad IR suficiente en el espectro solar, mientras que la luz de flash apenas posee componentes infrarrojos. Por
45 lo tanto, para este tipo de autenticación se recomienda utilizar la luz solar.

[0214] En las figuras 19 y 20 se muestra el comportamiento de reflexión de un ejemplo de realización concreto en función del período de rejilla y de la longitud de onda en caso de polarización magnética transversal y eléctrica transversal. La profundidad de rejilla de la rejilla sinusoidal es a este respecto de 200 nm. La rejilla está provista de
50 una capa de 80 nm de espesor de ZnS con un índice de refracción de aprox. 2,3 en el rango espectral visible (parte real del índice de refracción complejo), donde la rejilla está embebida en polímero con un índice de refracción de aprox. 1,59. El ángulo de observación es de 25°.

[0215] Se puede ver que una rejilla con un período de 700 nm en la polarización eléctrica transversal muestra
55 una clara reflexión característica en el infrarrojo cercano, que se puede utilizar para una autenticación.

[0216] Además, es posible utilizar motivos 11 que muestran efectos mate dinámicos o estáticos sobre un fondo negro difusivo, un fondo negro reflectante o en color. Tales estructuras se pueden evaluar como se describió anteriormente con algoritmos de reconocimiento de imágenes y borde. El tamaño de las estructuras, en el caso más
60 simple de los puntos, es preferiblemente de 100 μm a 600 μm . Las estructuras también pueden diferir del fondo por pequeñas desviaciones en el ángulo de azimut. Cuantos más elementos se integren con un efecto semejante en el motivo 11, tanto mejor será la precisión de autenticación.

[0217] Opcionalmente, el motivo 11 también se puede seleccionar con el llamado efecto mate dinámico en una
65 gran superficie, de modo que el efecto mate sea claramente reconocible para el ojo. Si durante la autenticación se

captura una secuencia de imágenes con al menos una imagen con y sin flash, entonces se puede evaluar la inversión del contraste que se produce al menos por zonas. Esta inversión de contraste tiene su origen en la propiedad especial de dispersión de las estructuras mate anisotrópicas que se utilizan para este efecto mate dinámico. Con el flash, el motivo 11 se ilumina desde casi la misma dirección desde la que se captura con el sensor. Sin flash, por el contrario, muy poca luz proviene de esta dirección, por lo que la iluminación se produce desde otras direcciones. En conjunto, esto resulta en una inversión de contraste del motivo 11. La fig. 21 muestra capturas de imagen con y sin flash para dos motivos a modo de ejemplo con estructuras mate anisotrópicas.

[0218] El motivo 11 puede comprender además un retrato, que se puede realizar por medio de una imagen en escala de grises, holograma de color real, holograma generado por ordenador o como retrato en relieve de superficie. Para la autenticación del elemento de seguridad 1 se puede aplicar entonces un algoritmo biométrico. Para ello son adecuadas en particular las variantes de retrato con un alto nivel de detalle.

[0219] El motivo 11 también se puede complementar en el lado del software en el dispositivo 3 con otros elementos, después de lo cual se examina a continuación si resulta una estructura de consigna. Por lo tanto, los métodos criptográficos se pueden integrar en el procedimiento, donde los elementos complementados por el software actúan como una clave privada y el motivo actúa como una clave pública.

[0220] Las estructuras del motivo 11 utilizadas para la verificación del elemento de seguridad 1 también pueden tener un significado, por ejemplo, en forma de un código lineal o un código de barras. Si estas estructuras son muy pequeñas, por ejemplo, menores de 100 μm , a su vez no son visibles a simple vista, pero se pueden reconocer por el sensor 31. Si para ello se utilizan estructuras difractivas, por ejemplo, un código de barras difractivo con estructuras en relieve que absorben mucha luz y, por lo tanto, ópticamente oscuras, preferentemente de aspecto negro, sobre un fondo con estructuras en relieve isotrópicamente mates, el equipo 3 puede distinguir sin problemas entre el elemento de seguridad real y una copia impresa estática. Para ello, por ejemplo, también se puede utilizar el color, intensidad o estructura de trama del código difractivo.

[0221] Las estructuras portadoras de significado del motivo 11 pueden ser a este respecto parte gráfica integral del motivo 11. Es decir, las estructuras portadoras de significado del motivo 11 son al mismo tiempo parte de una representación gráfica, por ejemplo, de un logotipo, escudo de armas, retrato o denominación. Pero, las estructuras portadoras de significado del motivo 11 pueden estar dispuestas asimismo por separado, es decir, ópticamente separadas del motivo gráfico propiamente dicho, en una zona separada, para poderse leer o verificar, por ejemplo, también por separado. Por ejemplo, además del motivo 11, en particular adyacente a él, puede estar dispuesto un código de barras difractivo. De forma alternativa a ello, el código de barras difractivo puede estar integrado en la disposición gráfica del motivo 11.

[0222] Tres realizaciones posibles de un elemento de seguridad 1 con un motivo 11 que comprende un código de barras 2D 111 están representadas en las figuras 22 A-C. Todos los ejemplos de realización comprenden a este respecto en cada caso el código de barras 111, un motivo gráfico 112, por ejemplo, un logotipo de marca, así como una superficie al menos parcialmente metalizada 113. En todos los ejemplos de realización, el motivo gráfico 112 está configurado como un motivo difractivo dispuesto sobre la superficie parcialmente metalizada 113.

[0223] En el ejemplo de realización mostrado en la fig. 22A, el código de barras 111 no se extiende sobre la superficie parcialmente metalizada 113, sino que está dispuesto como estructura impresa junto a esta superficie parcialmente metalizada 113.

[0224] En el ejemplo de realización según la fig. 22B, el código de barras 111 se encuentra dentro de la superficie 113 y se genera mediante desmetalización dirigida de la superficie 113, por ejemplo, por medio de ablación láser.

[0225] En el ejemplo de realización según la fig. 22C, el código de barras 111 está dispuesto igualmente dentro de la superficie 113 y, al igual que el motivo gráfico 112, está realizado como estructura difractiva.

[0226] En todos los casos, el código de barras 111 se puede leer utilizando el procedimiento descrito por medio de un equipo de mano 3, de modo que el elemento de seguridad 1 se puede autenticar. El propio código de barras 111 puede contener a este respecto información de individualización que posibilite la asignación del elemento de seguridad 1 a un objeto o documento determinado. Esto es posible en particular si el código de barras 111 se genera mediante impresión por chorro de tinta o ablación por láser.

[0227] No obstante, tal información de individualización también se puede incorporar adicionalmente al código de barras 111 en el elemento de seguridad 1. Tres posibilidades para ello están representadas en las figuras 23 A-C.

[0228] Tal información de individualización 114 adicional se puede leer, al igual que el código de barras 111, por medio de un equipo de mano 3. Para garantizar una seguridad adicional, a este respecto, también es posible si la información de individualización 114 solo se puede leer con equipos especiales, por ejemplo, con iluminación especial

o filtros de cámara especiales o también con un equipo especial del lado del software.

[0229] En los ejemplos de realización mostrados, la información de individualización 114 está configurada como un patrón de puntos aleatorio o pseudoaleatorio. Los números aleatorios o números pseudoaleatorios para generar el patrón de puntos se pueden obtener a este respecto a partir de fuentes físicas, por ejemplo, de distribuciones aleatorias que ocurren en la naturaleza, o también se pueden generar algorítmicamente.

[0230] Como muestra la fig. 23A, la información de individualización 114 se puede disponer por separado del código de barras 111. Por ejemplo, el código de barras 111 y la información de individualización 114 se pueden generar en láminas de transferencia separadas y se pueden aplicar por separado al elemento de seguridad 1.

[0231] Alternativamente, el código de barras 111 y la información de individualización 114 también se pueden superponer. Como muestra la fig. 23B, esto se puede materializar mediante la integración directa de la información de individualización 114 en la estructura del código de barras 111. Por ejemplo, ambos ítems de información se pueden formar por la misma estructura difractiva.

[0232] Alternativamente, el código de barras 111 y la información de individualización 114 también se pueden aplicar secuencialmente, como se muestra en la fig. 23C. En este caso, por ejemplo, el código de barras 111 se aplica por medio de una lámina de transferencia y a continuación se imprime la información de individualización 114 sobre la misma. Alternativamente, la información de individualización 114 también se puede generar mediante la incorporación de partículas, fibras u otros marcadores distribuidos aleatoriamente en la lámina de transferencia.

[0233] Si el código de barras 111 está configurado como una estructura en relieve, que se moldea mediante replicación en una capa de replicación y a continuación se metaliza, la información de individualización 114 también se puede generar además mediante desmetalización parcial posterior de la capa metálica 113, por ejemplo, mediante ablación láser.

[0234] Además, también es posible combinar una información de individualización aleatoria 114 con otra estructura en relieve aleatoria. Como estructuras en relieve se pueden utilizar a este respecto todas las variantes ya descritas anteriormente, en particular son adecuadas aquí estructuras mate isotrópicas o anisotrópicas, rejillas lineales, cruzadas, en forma de serpentín o circulares, estructuras de color basadas en microestructuras como hologramas generados por ordenador o estructuras de color aleatorias, estructuras de forma de cine o similares. Una individualización adicional se puede realizar entonces de nuevo mediante la aplicación de una información de individualización 114 por medio de ablación láser o impresión, en particular impresión por chorro de tinta.

[0235] Como muestra la fig. 24, a este respecto es ventajoso si el fondo para la información de individualización 114 se forma por un mosaico o una superposición de estructuras en relieve, que se pueden diferenciar por medio del equipo de mano 3. Preferentemente, los campos individuales 115 de un mosaico semejante son lo suficientemente pequeños como para que no se puedan clarificar con el ojo humano. Si la información de individualización 114, como se muestra en la fig. 24 A-C, se inscribe después de la generación del mosaico, por ejemplo, mediante ablación láser en forma de puntos individuales, entonces, solo por la tolerancia necesariamente existente del proceso de fabricación se produce una desviación aleatoria en el posicionamiento de la información de individualización 114 con respecto a los campos 115 del mosaico, que difiere para cada elemento de seguridad 1 y, por lo tanto, se puede utilizar para la identificación de elementos de seguridad individuales 1.

[0236] Una información de individualización 114 se puede generar además mediante la extinción parcial de una estructura en relieve mediante la impresión de una laca con el mismo índice de refracción que la capa de replicación en la que está moldeada la estructura en relieve. Donde se imprimió la laca, no se produce ningún efecto óptico a través de la estructura en relieve extinguida, después de una metalización posterior, estas regiones aparecen por lo tanto reflectantes y se pueden leer fácilmente por medio del equipo de mano 3.

[0237] Una información de individualización 114 se puede generar además, como se muestra en la fig. 25, por el hecho de que dos estructuras ópticamente variables en forma de tira, que varían en cada caso a lo largo de su longitud en al menos un parámetro, se disponen una al lado de la otra o una sobre la otra. Mediante la variación de los respectivos parámetros resulta cada vez de la disposición relativa de las dos estructuras entre sí para cada punto a lo largo de la extensión longitudinal un par de parámetros específico.

[0238] Por ejemplo, una estructura mate dinámica 114a que varía en su brillo, por ejemplo, con un cambio gradual del ángulo de azimut de 0° a 90°, se puede disponer junto a un gradiente de color difractivo 114b, por ejemplo, con un cambio gradual del período de rejilla de 500 líneas por mm a 1500 líneas por mm. Para cada punto a lo largo de la extensión longitudinal se puede leer entonces un par de valores de color y brillo. Mediante un decalado seleccionado al colocar las dos estructuras en la dirección longitudinal, estos pares de valores se pueden individualizar y utilizar para el reconocimiento de elementos de seguridad individuales específicos 1. Las dos estructuras también se pueden superponer con un patrón aleatorio 116, que define las zonas a leer.

[0239] En otra forma de realización, los marcadores en forma de punto 117 se pueden integrar en un patrón de fondo difractivo 118 para formar la información de individualización 114, como se representa en la fig. 26. Los marcadores pueden ser en general cualquier marcador químico o físico, en particular pigmentos, nanopartículas, partículas cristalinas y similares. Para una protección adicional también se pueden analizar los espectros de absorción, emisión o refracción de los marcadores 117 por medio del equipo de mano 3.

[0240] Preferiblemente, los marcadores se distribuyen aleatoriamente. Esto se puede realizar, por ejemplo, mediante la mezcla de una pequeña concentración de marcadores 117 en una laca. Al aplicar y endurecer la pintura se produce la distribución aleatoria deseada, que se puede utilizar para la individualización.

[0241] Si se imprime un código de barras 111 a través de un patrón de individualización 114, entonces también se puede recurrir a la superposición parcial y, por lo tanto, a la eliminación del patrón de individualización 114 por el código de barras 111 para la autenticación e identificación del elemento de seguridad 1. Un ejemplo de ello se muestra en la fig. 27. También se puede leer y analizar la relación de posición entre estructuras individuales del patrón de individualización 114 y el código de barras 111.

[0242] La fig. 28 muestra otro ejemplo de un patrón de individualización 114. En este caso, en primer lugar, un patrón de individualización difractivo 114 se replica sobre un sustrato en forma de tira (fig. 28A). La longitud máxima libre de repetición de la tira está condicionada a este respecto por la circunferencia del rodillo de replicación.

[0243] Sólo una parte de esta tira se aplica entonces junto al código de barras 111 sobre el elemento de seguridad 1. Como muestran las fig. 28B-D, según la sección seleccionada de la tira se produce por tanto una relación de posición individual entre el patrón de individualización 114 y el código de barras 111, que se puede leer y utilizar para la autenticación.

REIVINDICACIONES

1. Procedimiento para la autenticación de un elemento de seguridad (1) ópticamente variable, en particular de un elemento de seguridad difractivo, con las etapas:

a) captura de una secuencia de imágenes con al menos una imagen individual del elemento de seguridad (1) por medio de un sensor (31) en particular de un equipo de mano (3), preferentemente un teléfono inteligente, tableta o PDA;

b) verificación de si está presente al menos una información óptica predeterminada en al menos una imagen individual de la secuencia de imágenes, donde la secuencia de imágenes comprende una pluralidad de imágenes individuales del elemento de seguridad (1), en particular comprende más de 2 imágenes individuales del elemento de seguridad (1), donde mediante al menos dos imágenes individuales de la secuencia de imágenes se verifica si el elemento de seguridad (1) comprende una estructura ópticamente variable,

caracterizado porque en la etapa b) se verifica en primer lugar si un objeto predeterminado está presente en al menos una imagen individual de la secuencia de imágenes, donde al verificar si la al menos una información óptica predeterminada del elemento de seguridad (1) ópticamente variable está presente, se determina el contorno del objeto predeterminado a partir de al menos una imagen individual de la secuencia de imágenes y donde al menos una región parcial de la imagen individual, que está posicionada en una posición predeterminada con respecto al contorno de un objeto predeterminado y que comprende al menos un píxel y/o al menos un grupo de píxeles de la imagen individual, se selecciona y al menos una propiedad del al menos un píxel y/o al menos un grupo de píxeles de la al menos una región parcial seleccionada se compara con un valor de consigna correspondiente.

2. Procedimiento según la reivindicación 1,

caracterizado porque

para verificar si el objeto predeterminado está presente se lleva a cabo una comparación de la al menos una imagen individual con un conjunto de datos de entrenamiento capturada anteriormente por medio del algoritmo de reconocimiento de imágenes, donde en particular para capturar el conjunto de datos de entrenamiento se crea una pluralidad de imágenes, donde un primer subconjunto de las imágenes presenta en cada caso el objeto predeterminado y un segundo subconjunto de las imágenes no presenta en cada caso el objeto predeterminado, y donde a cada imagen del primer subconjunto se le asignan todas las coordenadas de imagen respectivas de las características a reconocer del objeto predeterminado.

3. Procedimiento según cualquiera de las reivindicaciones anteriores,

caracterizado porque

durante el registro de la secuencia de imágenes en la etapa a) se modifica un ángulo entre el sensor y el elemento de seguridad y/o un ángulo entre una fuente de luz y el elemento de seguridad (1), donde en particular durante la captura de la secuencia de imágenes en la etapa a) se registra una posición relativa del equipo de mano (3) con respecto a una posición predeterminada por medio de un sensor de posición del equipo de mano (3) para cada imagen individual de la secuencia de imágenes y se asigna a la imagen individual respectiva, y donde preferentemente para verificar si el elemento de seguridad (1) comprende una estructura ópticamente variable, en la etapa b) se comparan dos imágenes individuales de la secuencia de imágenes, que se han capturado con diferentes ángulos de observación y/o de iluminación.

4. Procedimiento según la reivindicación 3,

caracterizado porque

para verificar si el elemento de seguridad (1) comprende una estructura ópticamente variable, se comparan respectivamente los píxeles y/o grupos de píxeles correspondientes, en particular las regiones parciales, con las imágenes individuales.

5. Procedimiento según cualquiera de las reivindicaciones anteriores,

caracterizado porque

la al menos una información óptica predeterminada comprende una desviación de una propiedad gráfica, en particular un grosor de línea, un valor de color, un valor de tono, una luminosidad, una densidad de trama, una orientación de trama o un escrito, entre una primera región parcial y una segunda región parcial de otra información óptica, visualmente perceptible del elemento de seguridad difractivo, en particular en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número, y/o una desviación de una simetría entre una primera región parcial y una segunda región parcial de otra información óptica, visualmente perceptible del elemento de seguridad difractivo, en particular en forma de un símbolo, logotipo, imagen, signo, carácter alfanumérico o un número, y/o una información no visualmente reconocible, que se puede detectar a máquina con el sensor, y/o

porque la al menos una información óptica predeterminada se forma por una variación de al menos un parámetro de relieve de una estructura en relieve del elemento de seguridad (1) entre al menos una primera zona y al menos una segunda zona del elemento de seguridad, donde la estructura en relieve prevista en la primera y/o segunda zona es en particular una estructura difractiva, una estructura de difracción de orden cero, una rejilla Blaze, una

macroestructura, en particular una estructura de lente o estructura de micropisma, una superficie de espejo, una estructura mate, en particular una estructura mate anisotrópica o isotrópica.

6. Procedimiento según cualquiera de las reivindicaciones anteriores,

5 **caracterizado porque**

la al menos una información óptica predeterminada se genera al capturar la secuencia de imágenes por un efecto Moiré entre una trama periódica del elemento de seguridad (1) y una trama periódica del sensor (31), y/o por un efecto difractivo en un rango de longitud de onda fuera del espectro visible, en particular en el infrarrojo.

10 7. Procedimiento según cualquiera de las reivindicaciones anteriores,

caracterizado porque

se verifica si está presente al menos otra información óptica en al menos una imagen individual de la secuencia de imágenes, donde la al menos otra información óptica es en particular una información de individualización, en particular una información de individualización aleatoria, pseudoaleatoria y/o generada algorítmicamente.

15

8. Procedimiento según cualquiera de las reivindicaciones anteriores,

caracterizado porque

la etapa b) se lleva a cabo por medio de un programa de software realizado en un dispositivo de cálculo del equipo de mano (3), donde preferentemente el programa de software y/o una base de datos asociada al programa de software se actualiza a intervalos predeterminados, en particular antes de cada realización del procedimiento, a través de una conexión de telecomunicación, en particular conexión de Internet, o **porque** la etapa b) se lleva a cabo por medio de un programa de software realizado en un dispositivo de cálculo diferente del equipo de mano (3), al que se transmite la secuencia de imágenes capturada en la etapa a) a través de una conexión de telecomunicación, en particular una conexión de Internet.

25

9. Procedimiento según cualquiera de las reivindicaciones anteriores,

caracterizado porque

en otra etapa c) se verifica si al menos otra información óptica predeterminada está presente en al menos una imagen individual de la secuencia de imágenes, que está presente en una falsificación conocida del elemento de seguridad (1) ópticamente variable y no está presente en un elemento de seguridad (1) ópticamente variable real, donde preferiblemente en ausencia de la al menos una información óptica predeterminada y en ausencia de la al menos otra información óptica predeterminada se transmite un mensaje al dispositivo de cálculo diferente del equipo de mano (3), que comprende una información de ubicación y/o de tiempo, así como al menos una imagen individual de la secuencia de imágenes.

35

10. Equipo (3), en particular equipo de mano con un sensor (31) para capturar una secuencia de imágenes con al menos una imagen individual de un elemento de seguridad (1) y un equipo de control, que está configurado de modo que realiza las etapas siguientes:

- 40 a) captura de una secuencia de imágenes con al menos una imagen individual del elemento de seguridad (1) por medio del sensor (31);
- b) verificación de si está presente al menos una información óptica predeterminada en al menos una imagen individual de la secuencia de imágenes,

45 donde la secuencia de imágenes comprende una pluralidad de imágenes individuales del elemento de seguridad (1), en particular más de 2 imágenes individuales del elemento de seguridad (1), y donde sobre la base de al menos dos imágenes individuales de la secuencia de imágenes se verifica si el elemento de seguridad (1) comprende una estructura ópticamente variable, **caracterizado porque** en la etapa b) se verifica en primer lugar si un objeto predeterminado está presente en al menos una imagen individual de la secuencia de imágenes, donde al verificar si la al menos una información óptica predeterminada del elemento de seguridad ópticamente variable está presente, se determina el contorno del objeto predeterminado a partir de al menos una imagen individual de la secuencia de imágenes y donde al menos una región parcial de la imagen individual, que está posicionada en una posición predeterminada con respecto al contorno de un objeto predeterminado y que comprende al menos un píxel y/o al menos un grupo de píxeles de la imagen individual, se selecciona y al menos una propiedad del al menos un píxel y/o

50 al menos un grupo de píxeles de la al menos una región parcial seleccionada se compara con un valor de consigna correspondiente.

55

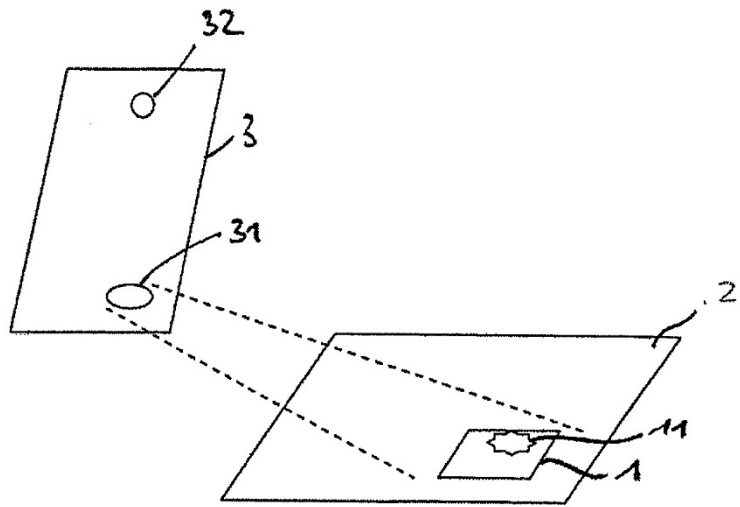


Fig. 1

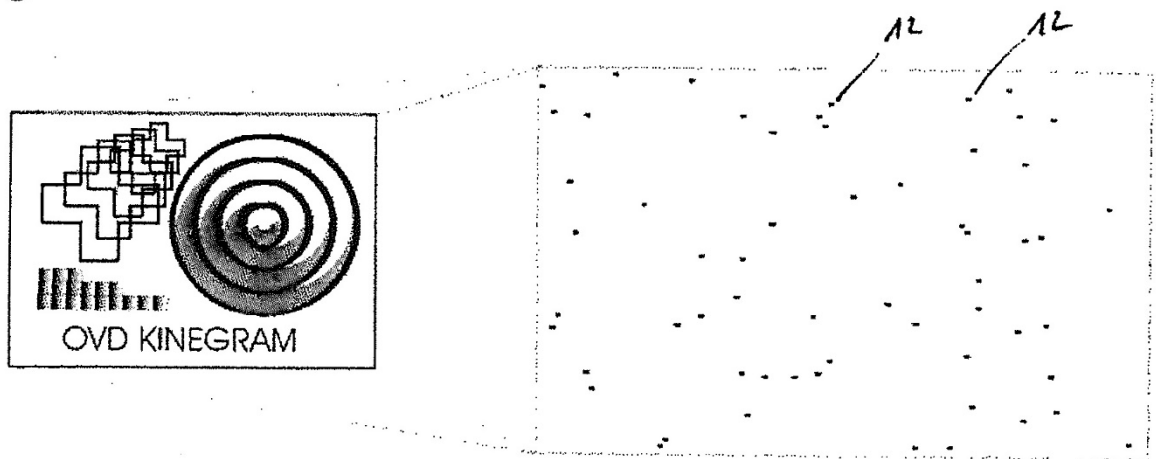


Fig. 2

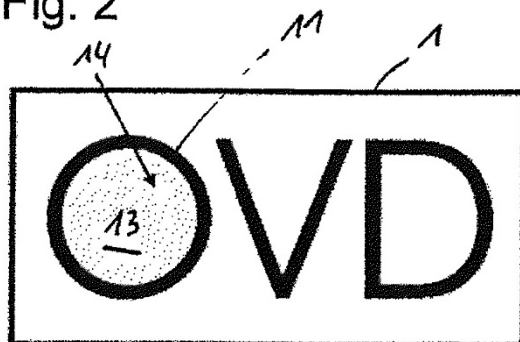


Fig. 3

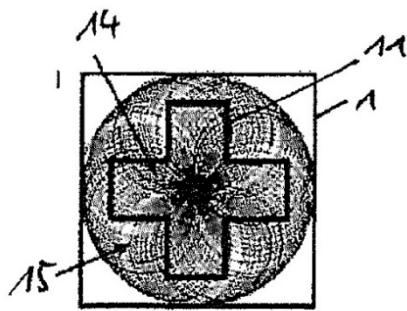


Fig. 4

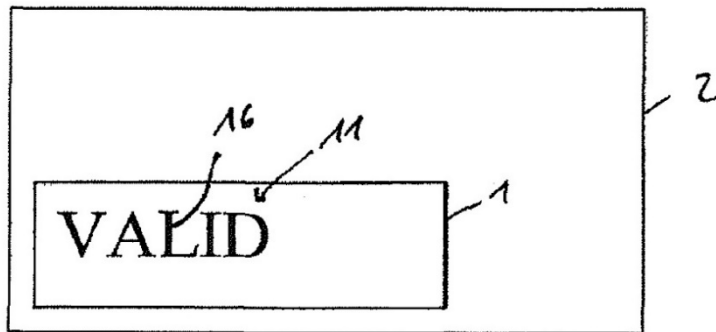


Fig. 5

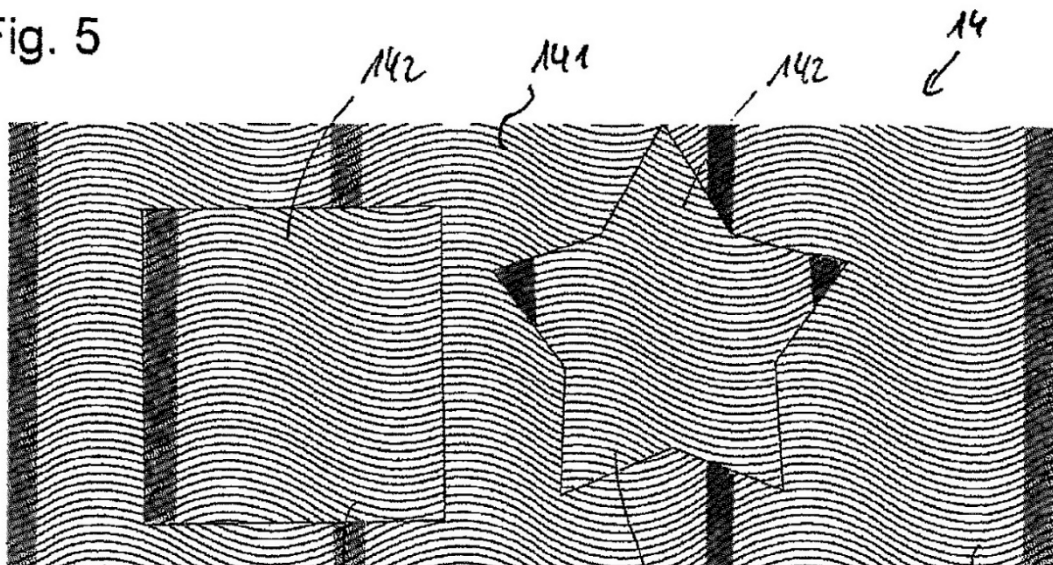


Fig. 6

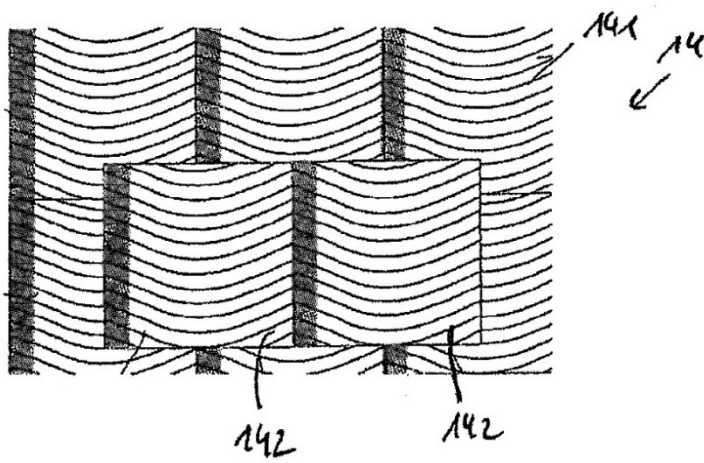


Fig. 7

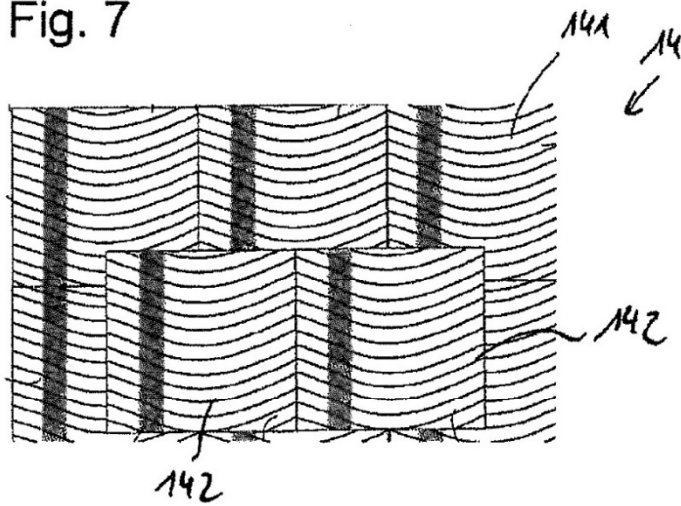


Fig. 8

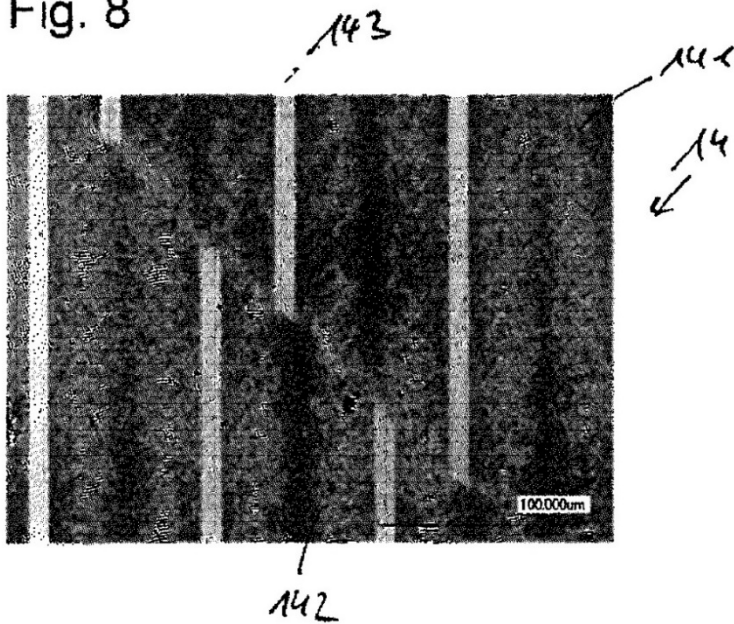


Fig. 9

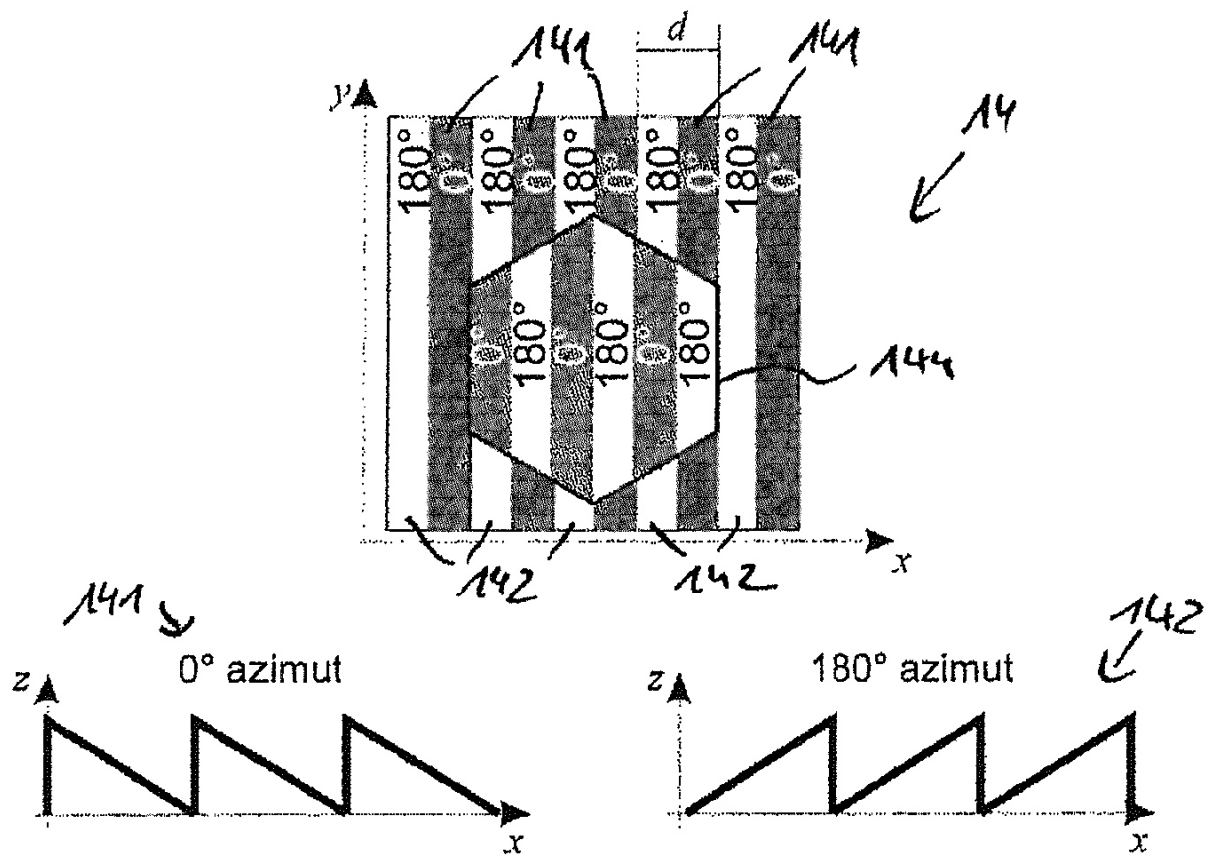


Fig. 10

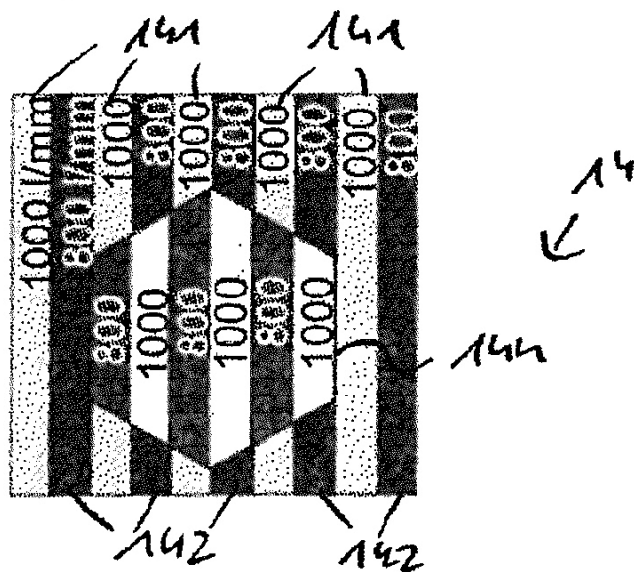
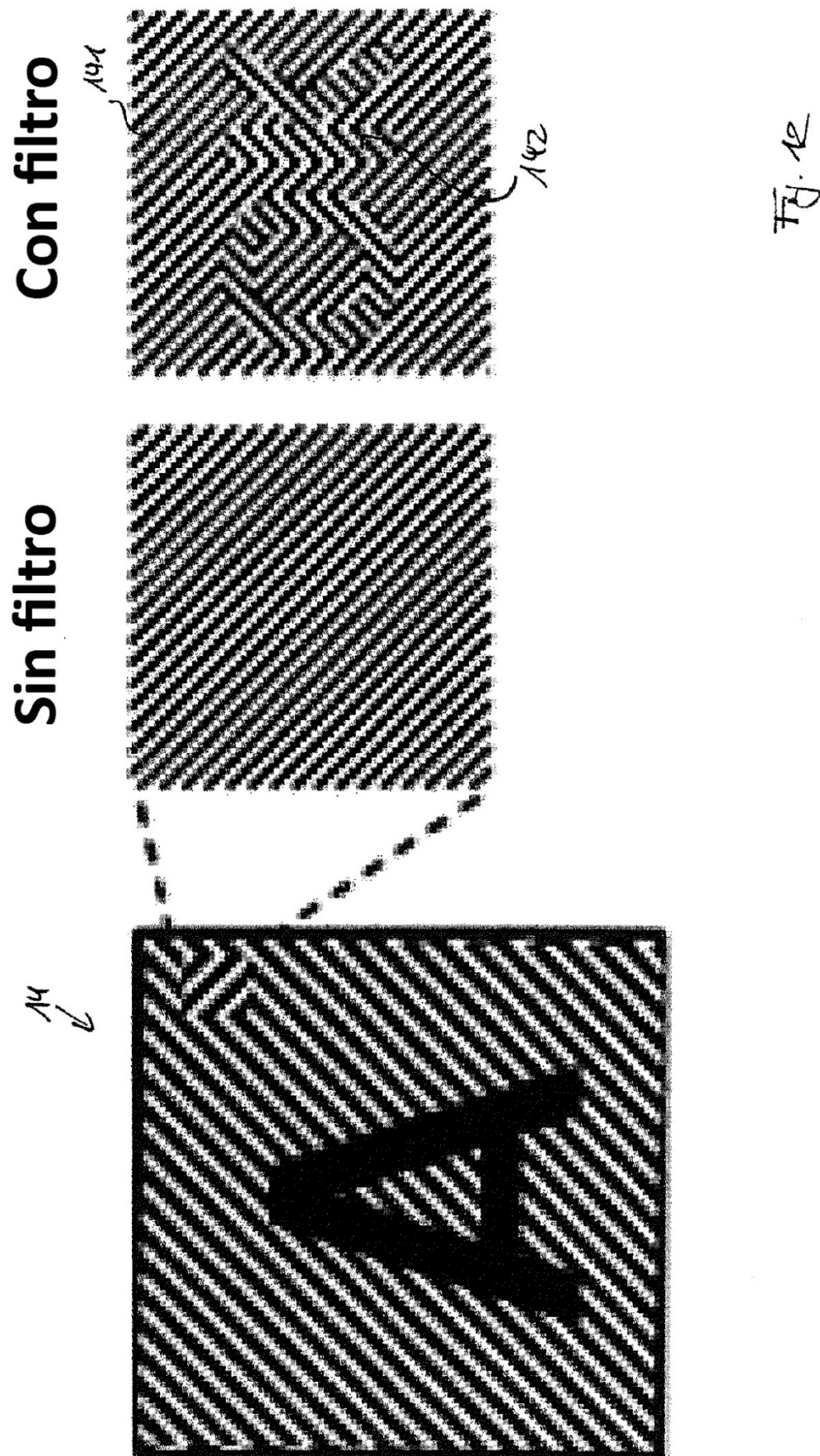


Fig. 11



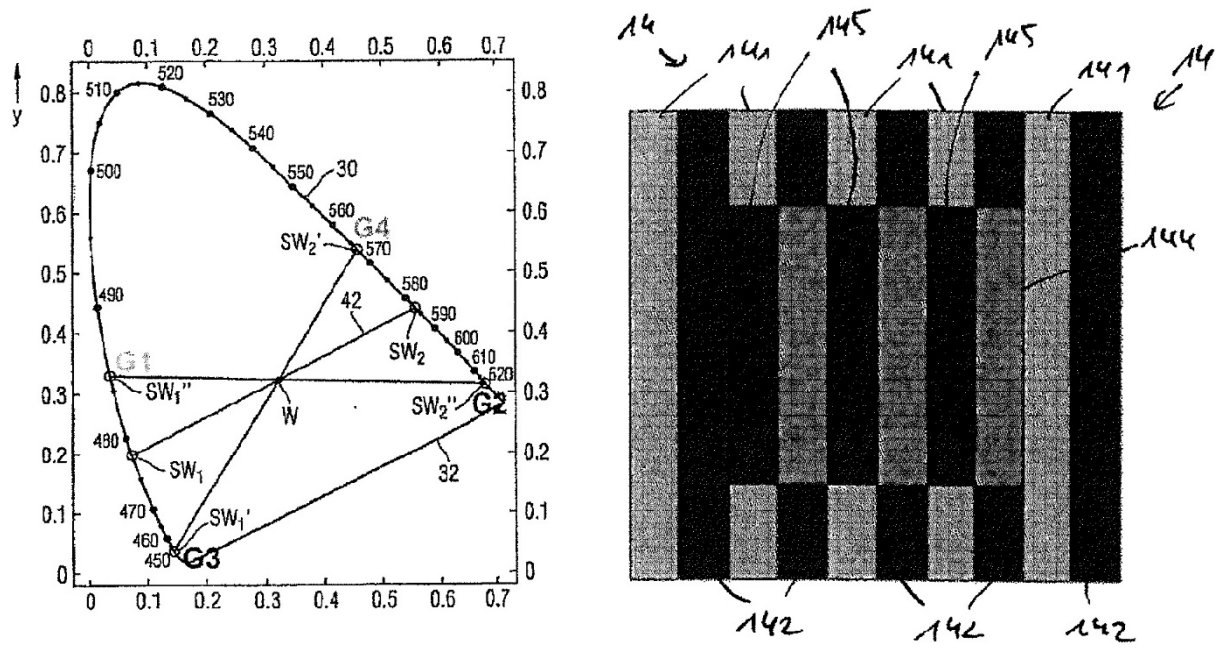


Fig. 13

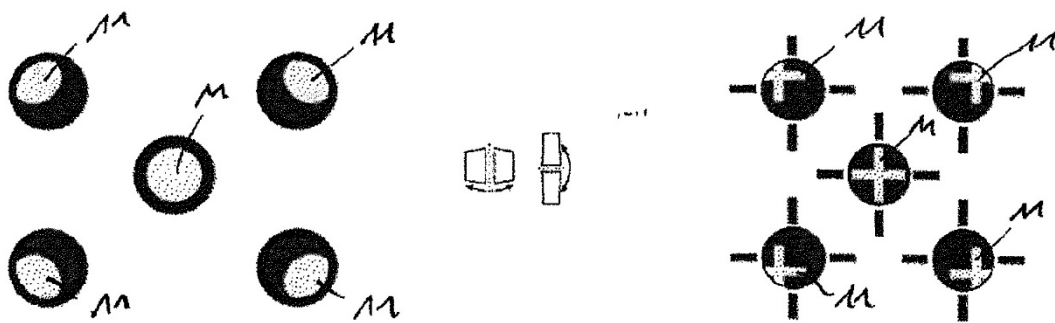


Fig. 14

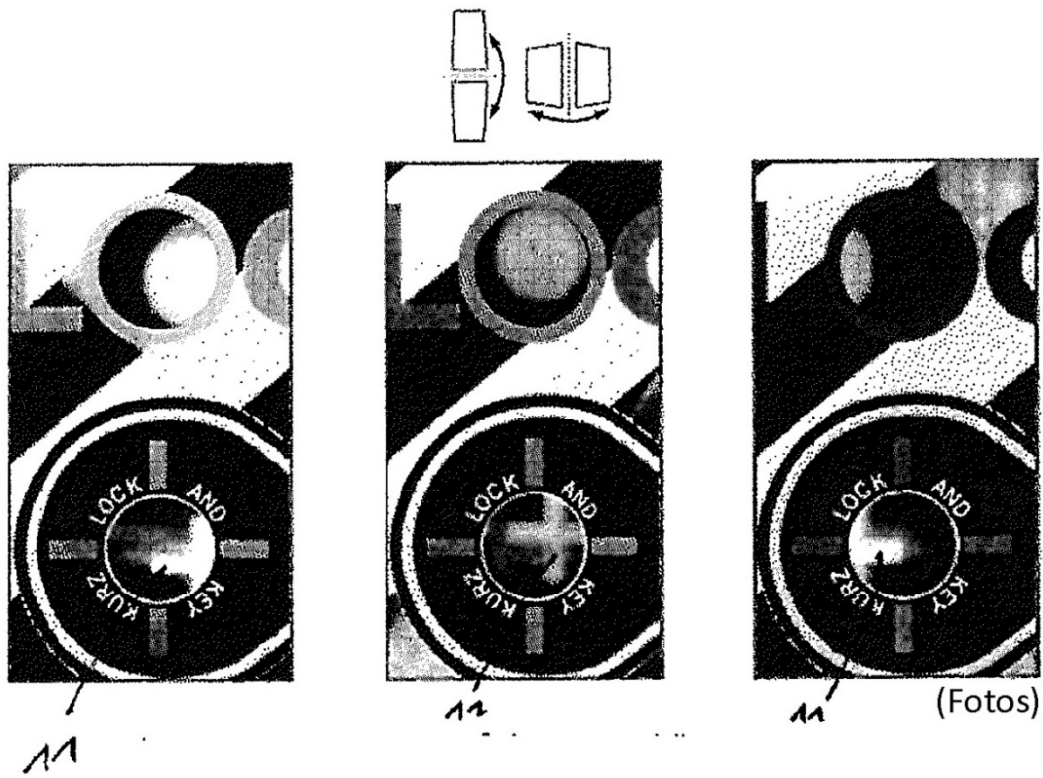


Fig. 15

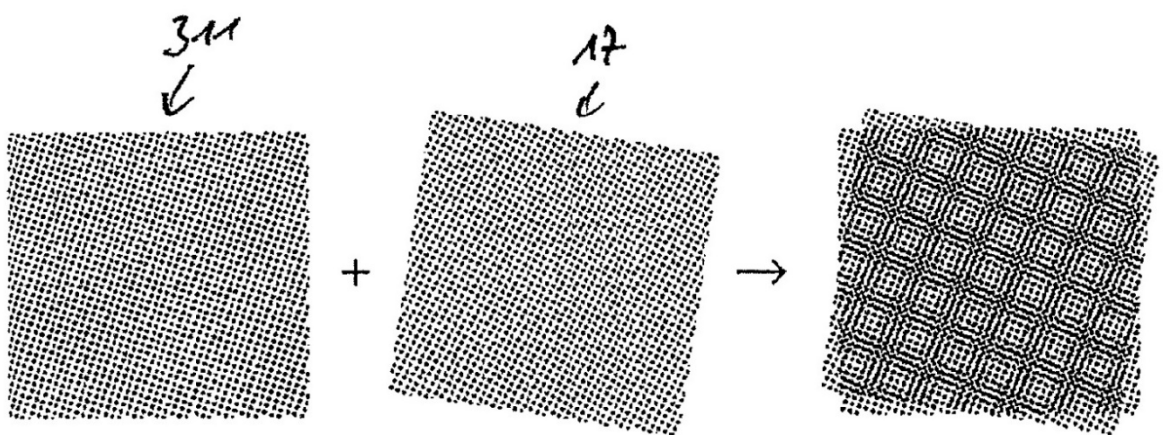


Fig. 16

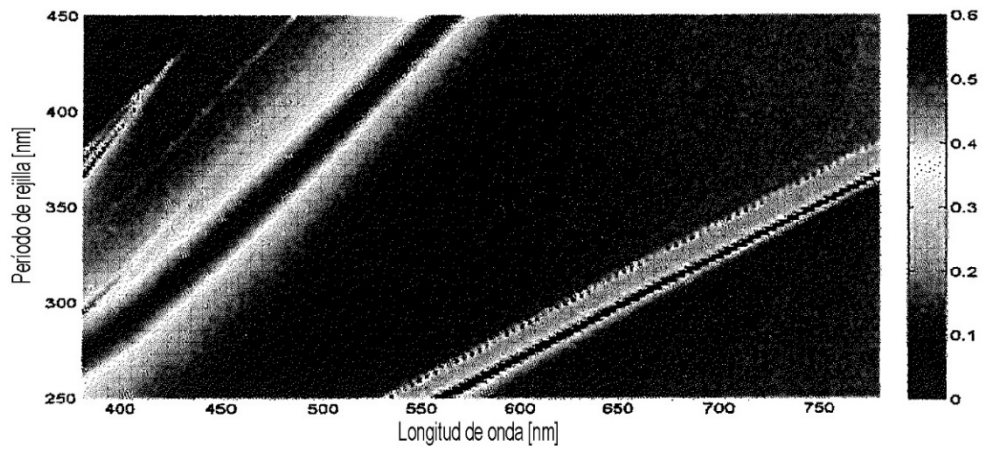


Fig. 17

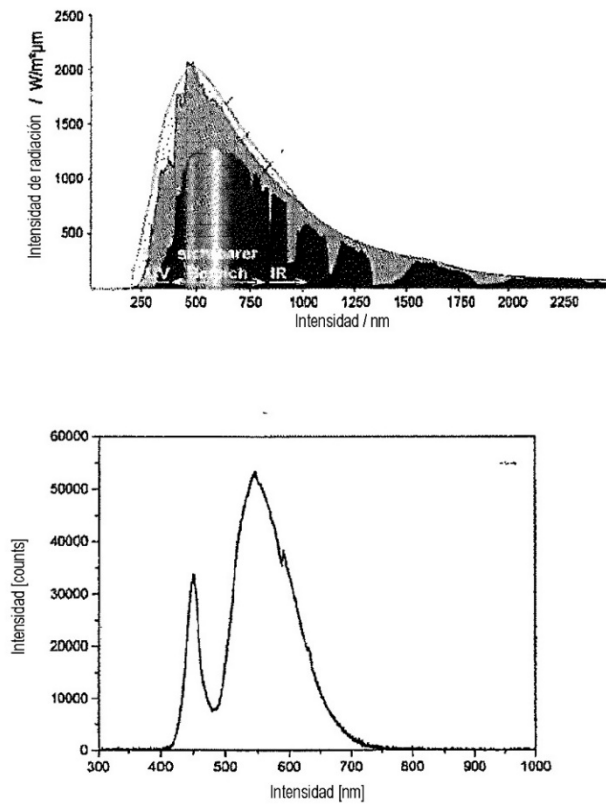


Fig. 18

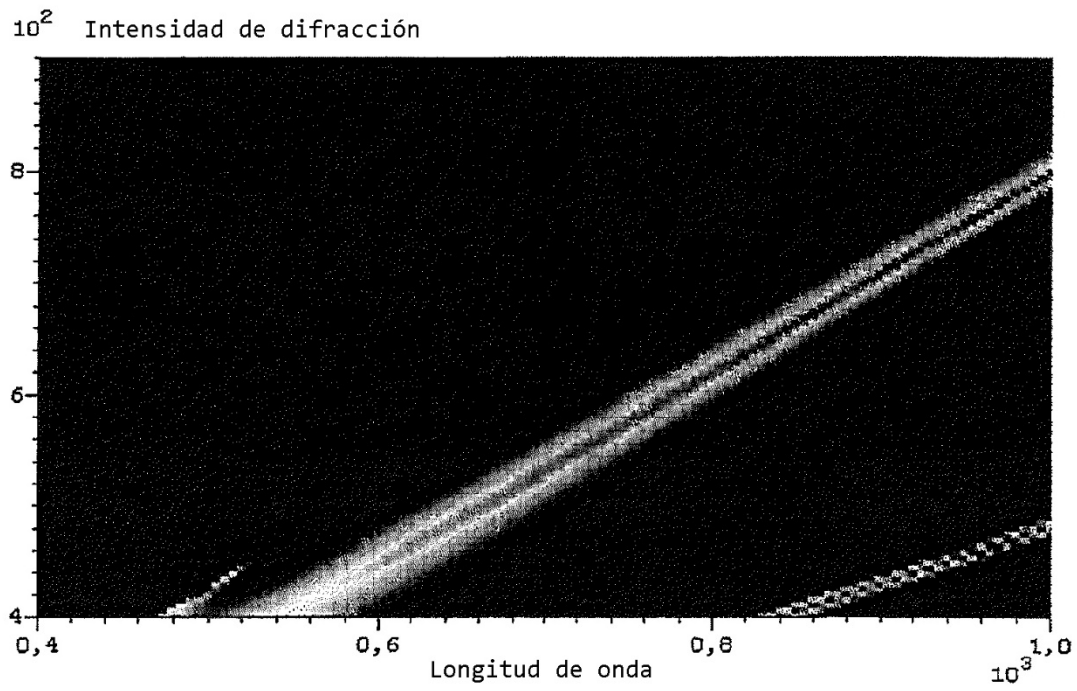


Fig. 19

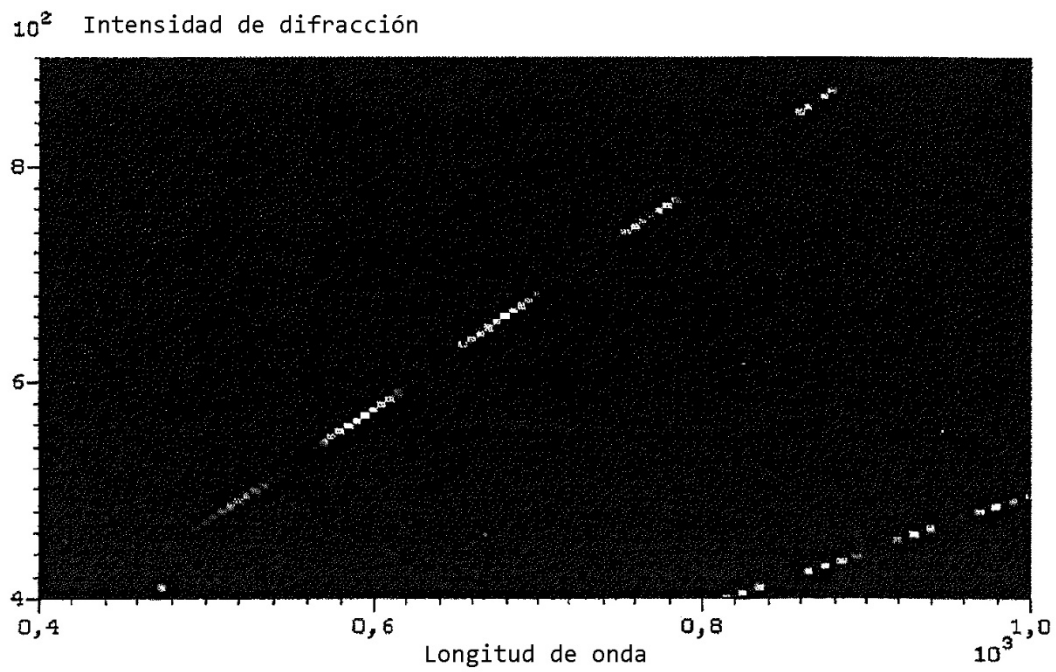
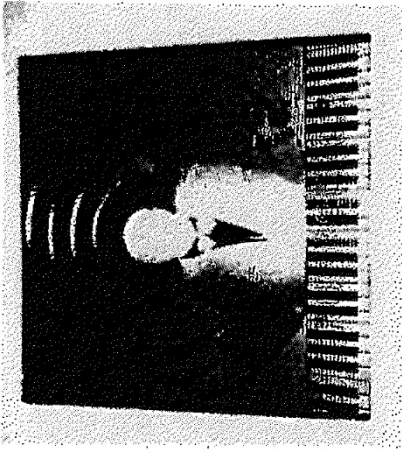


Fig. 20

14 ↗



14 ↗



Fig. 21



14 ↗



14 ↗

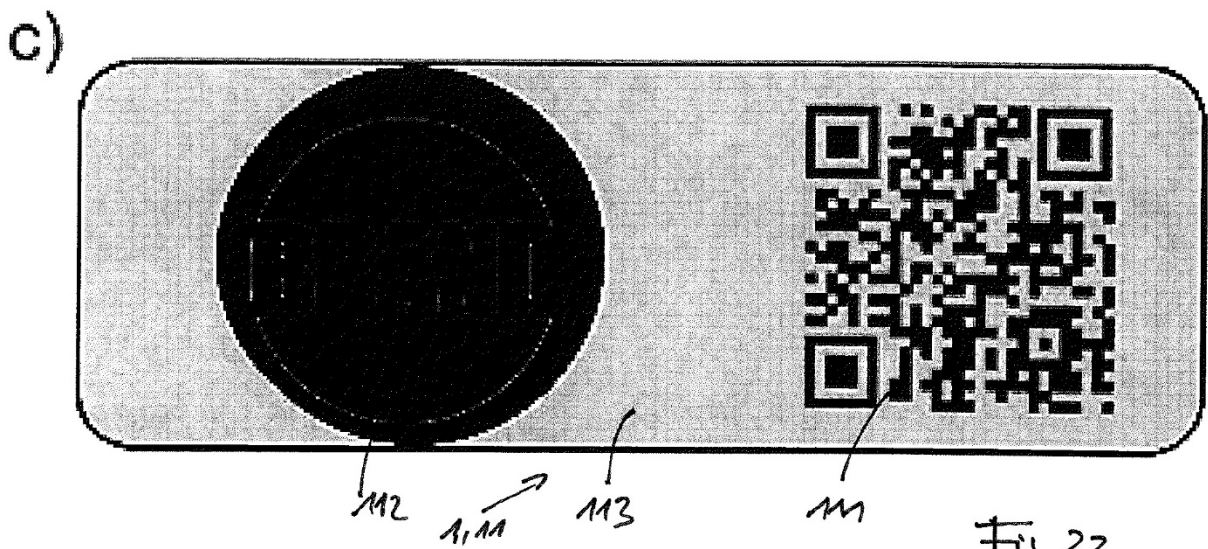
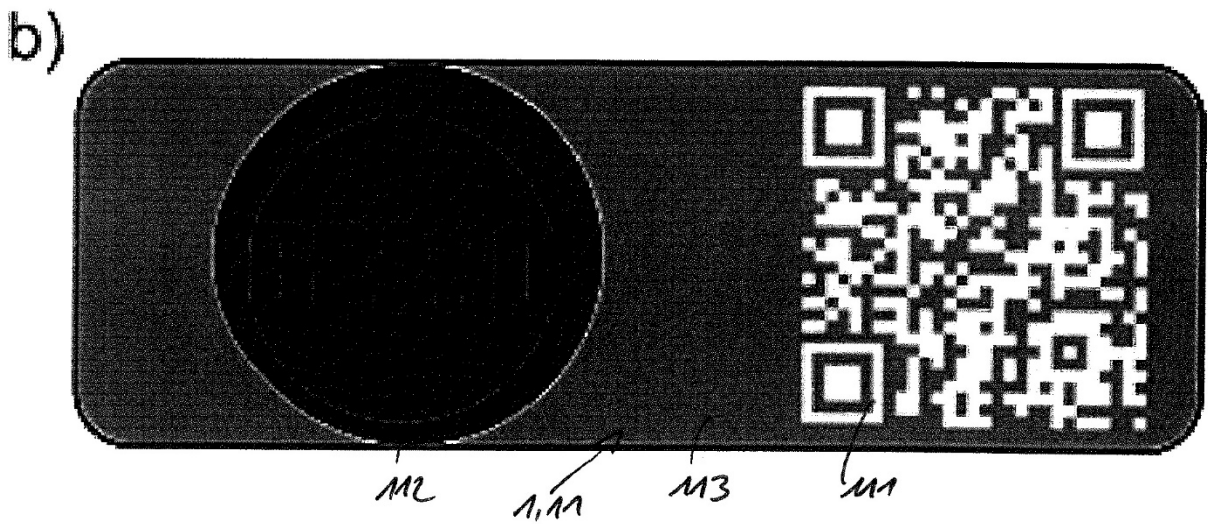
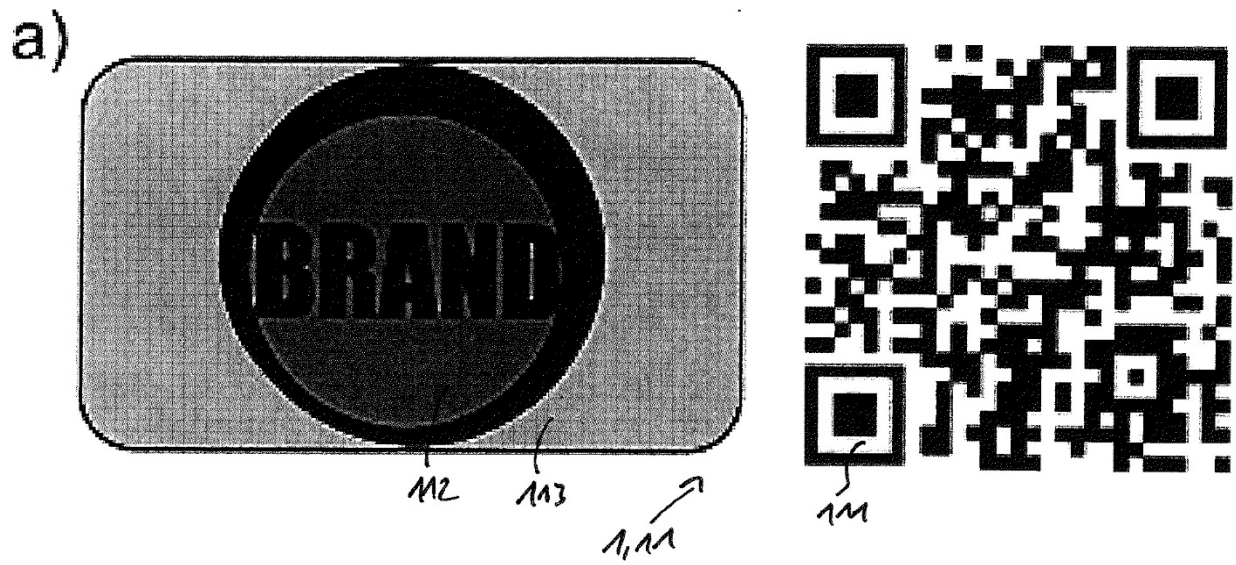


Fig. 22

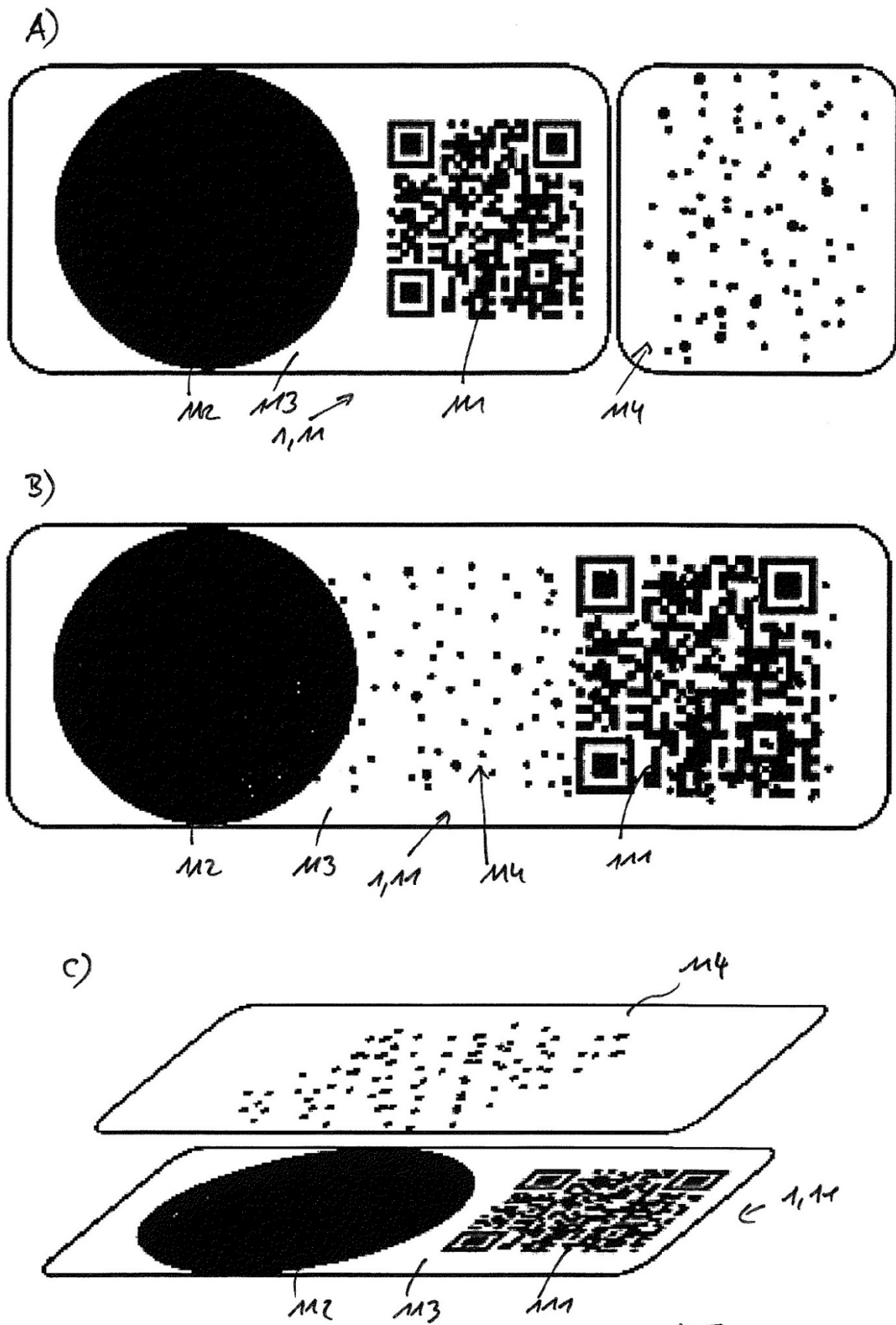
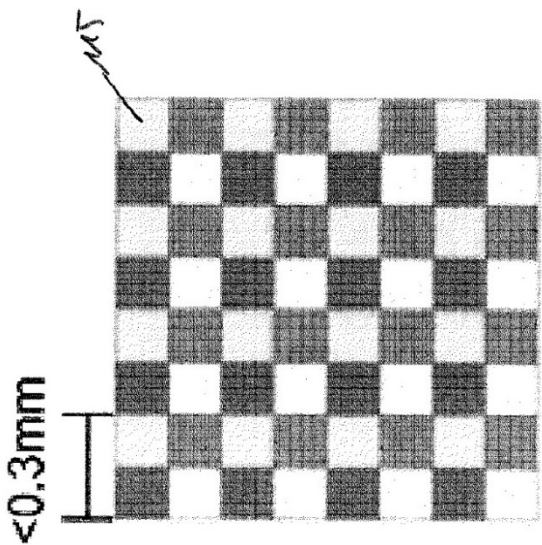
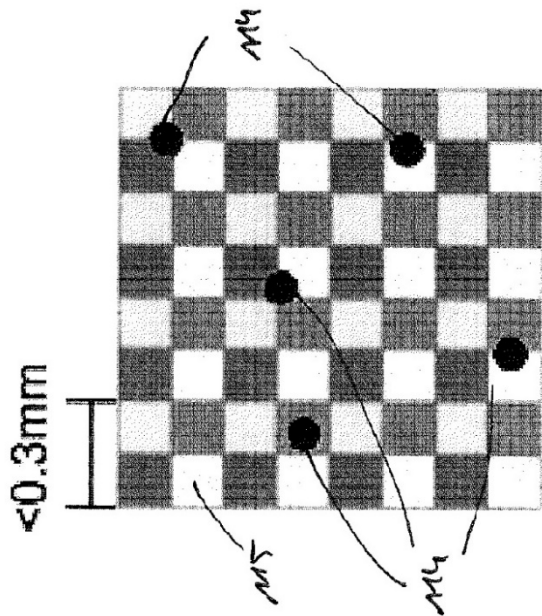
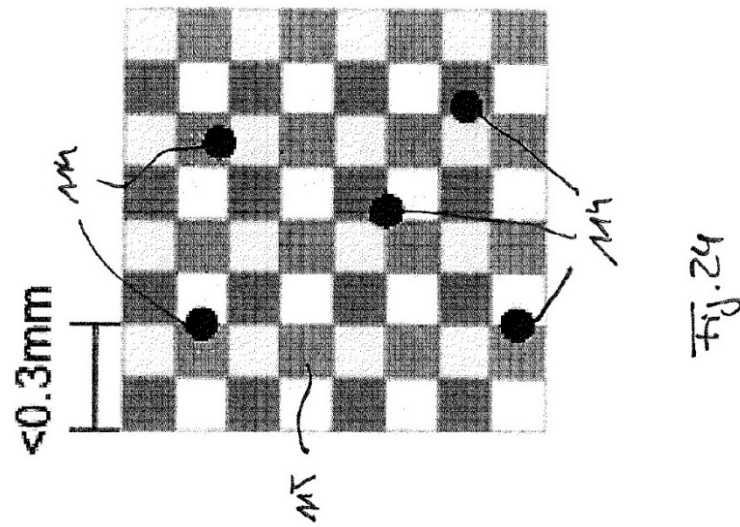
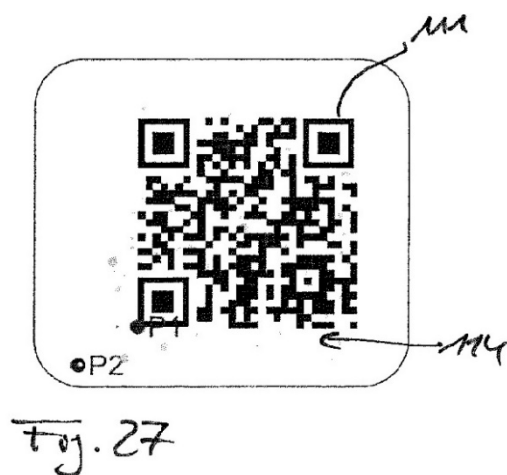
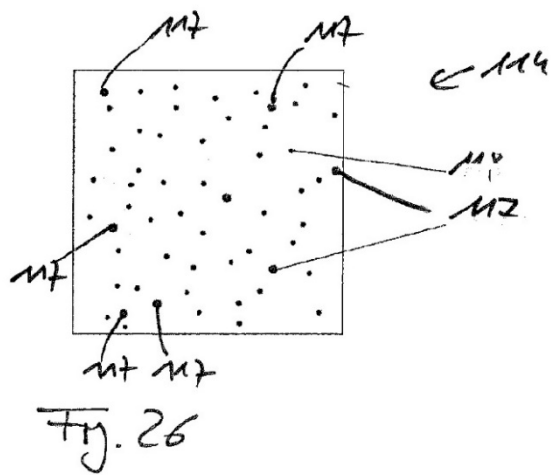
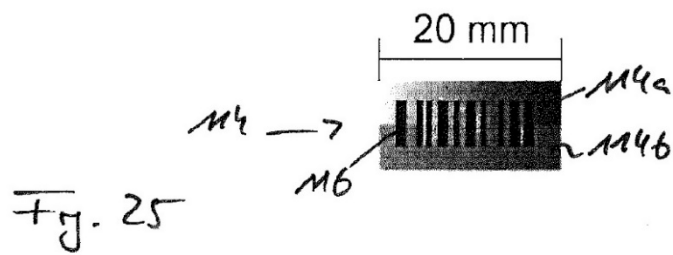
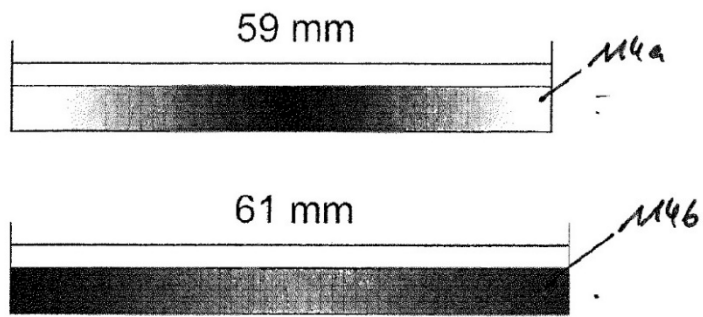


Fig. 23





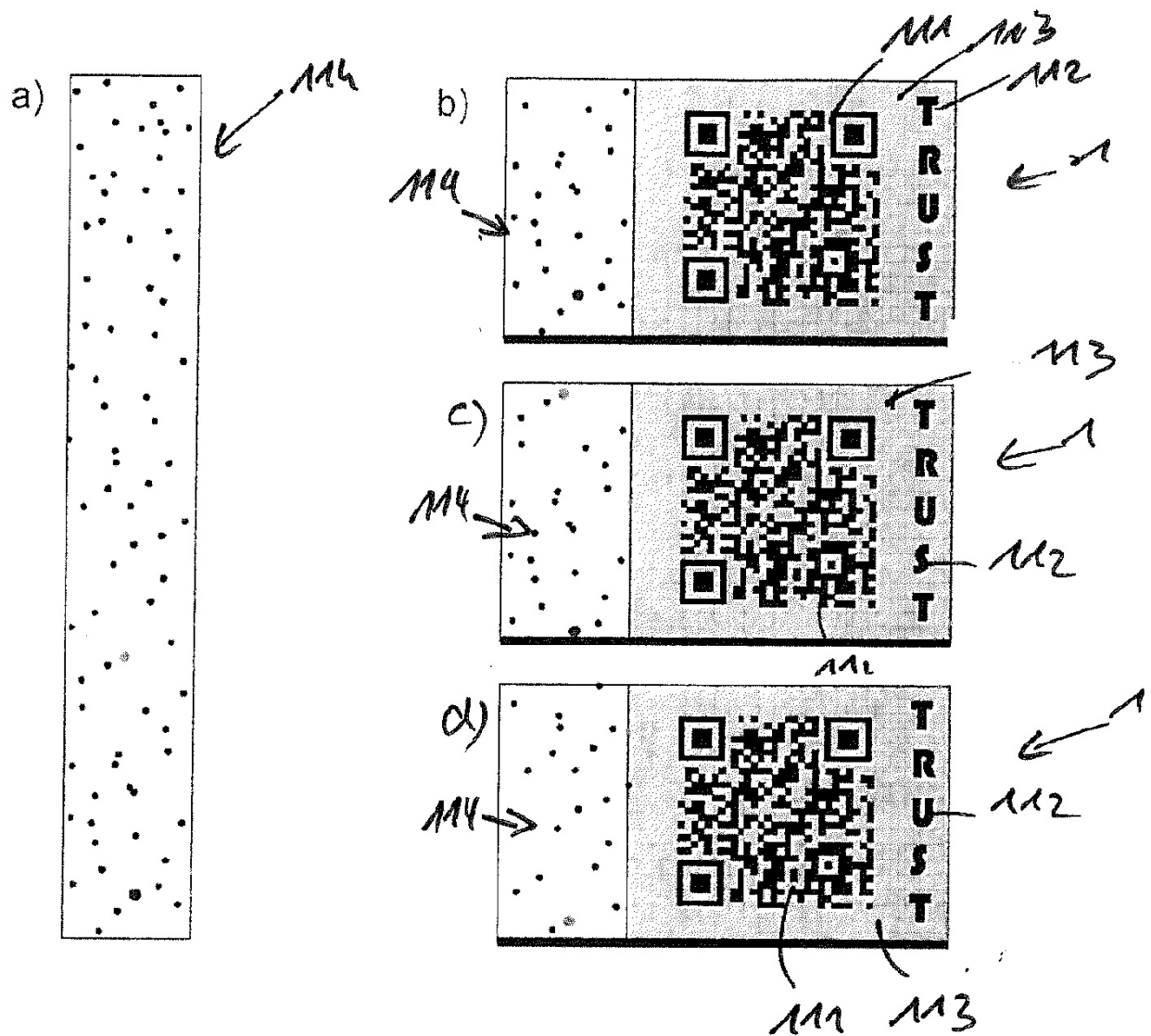


Fig. 28