

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 901 388**

51 Int. Cl.:

G06K 9/00 (2006.01)

G08B 13/196 (2006.01)

H04N 21/454 (2011.01)

H04N 7/18 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **06.11.2017** **PCT/EP2017/078286**

87 Fecha y número de publicación internacional: **07.06.2018** **WO18099689**

96 Fecha de presentación y número de la solicitud europea: **06.11.2017** **E 17797124 (9)**

97 Fecha y número de publicación de la concesión europea: **29.09.2021** **EP 3549115**

54 Título: **Cámara para vigilar una zona de vigilancia y dispositivo de vigilancia, así como procedimiento para vigilar una zona de vigilancia**

30 Prioridad:

30.11.2016 DE 102016223859

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2022

73 Titular/es:

ROBERT BOSCH GMBH (100.0%)
Postfach 30 02 20
70442 Stuttgart, DE

72 Inventor/es:

STRICKER, DIDIER;
WASENMUELLER, OLIVER;
GEILER, THOMAS y
ACKERMANN, JENS

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 901 388 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

Cámara para vigilar una zona de vigilancia y dispositivo de vigilancia, así como procedimiento para vigilar una zona de vigilancia

Estado de la técnica

5 La invención se refiere a una cámara para vigilar una zona de vigilancia con un sensor de cámara para crear al menos una imagen de vigilancia no enmascarada de la zona de vigilancia y/o de un sector de la zona de vigilancia, en donde el sensor de cámara está configurado para facilitar datos crudos, comprendiendo los datos crudos la al menos una imagen de vigilancia no enmascarada. La cámara comprende además una unidad de evaluación, en donde la unidad de evaluación comprende una interfaz de entrada para la recepción de los datos crudos y comprende una interfaz de salida para facilitar datos de imágenes. La unidad de evaluación comprende un módulo de verificación y un módulo de enmascaramiento, en donde el módulo de verificación está configurado para detectar una persona en la imagen de vigilancia no enmascarada basándose en los datos crudos, en donde el módulo de enmascaramiento está configurado para crear una imagen de vigilancia enmascarada, en donde la persona detectada está representada enmascarada en la imagen de vigilancia enmascarada.

15 Las cámaras se emplean con frecuencia para monitorizar zonas de vigilancia. Por ejemplo, en este sentido se vigilan fábricas, por lo que el derecho de los trabajadores en la planta de producción puede estar muy limitado a la protección de derechos de la personalidad. Por consiguiente, las aplicaciones sobre visión artificial se han desarrollado tanto que la vigilancia por cámara representa una solución asequible de la monitorización de procesos. Las instalaciones de videovigilancia recurren con frecuencia a sensores de barrera, como por ejemplo barreras fotoeléctricas e interruptores inductivos, con el fin de desconectar cámaras en la presencia de una persona en la zona de vigilancia.

20 El documento DE 10 2008 007 199 A1 que a decir verdad forma el estado de la técnica más cercano, describe un módulo de enmascaramiento para un sistema de vigilancia, en donde el sistema de vigilancia presenta al menos una cámara de vigilancia y es adecuada y/o está dispuesta para observar zonas de vigilancia con objetos móviles, con un equipo de selección para seleccionar objetos como objetos de selección, en donde el módulo de enmascaramiento está configurado para emitir enmascarados objetos de selección o sectores de estos.

25 El documento DE EP 2 429 182 A2 describe un procedimiento para desfigurar datos de una cámara relativos a personas. Mediante una unidad de procesamiento, la cámara desfigura datos referidos a personas de imágenes originales registradas en cada configuración ajustable por el usuario dentro de la cámara y almacena estas imágenes modificadas o derivadas de esta como imágenes de resultado en una memoria o las hace accesibles a través de una interfaz.

30 En el documento US 2006/0064384 A1 se describe un sistema de seguridad para proteger la esfera privada de una persona que se encuentra en un espacio. El sistema de seguridad comprende un sensor de localización para localizar a la persona y un sensor de vídeo para registrar datos visuales de la persona. Comprende también un subsistema informático que está acoplado con el sensor de localización y con el sensor de vídeo y que establece cómo se presentan, almacenan y se accede a los datos visuales de acuerdo con un nivel de protección de datos.

35 Un sistema de vigilancia con una unidad de imagen y una unidad de enmascaramiento se divulga en el documento JP 2005 286468 A. El sistema de vigilancia modifica una imagen original capturada y genera a partir de esta una imagen enmascarada. La imagen enmascarada se modifica y se guarda de acuerdo con una escala de autoridad establecida para varias personas encargadas de la vigilancia o se muestra en un monitor.

Divulgación de la invención

40 En el marco de la invención se divulga una cámara para vigilar una zona de vigilancia con las características de la reivindicación 1 y un dispositivo de vigilancia con las características de la reivindicación 12, así como un procedimiento para vigilar una zona de vigilancia con las características de la reivindicación 13. De las reivindicaciones dependientes, de la siguiente descripción, así como de las figuras adjuntas resultan formas de realización preferidas o ventajosas.

45 De acuerdo con la invención se propone una cámara para vigilar una zona de vigilancia. La cámara es, por ejemplo, una cámara en color, una cámara en blanco y negro, una cámara de infrarrojos, una cámara 3D, una cámara de barrido, inclinación y zoom PTZ (*pan tilt zoom*) o similares. La cámara es, en particular, una videocámara y/o una cámara de imágenes individuales. La cámara puede disponerse y/o está dispuesta preferentemente en la zona de vigilancia. La zona de vigilancia es, en particular, una superficie al aire libre o una zona interior. Especialmente la zona de vigilancia es una empresa, una fábrica, un edificio, una planta de producción, un almacén, una nave, un aeropuerto, una calle y/o un parque.

50 La cámara comprende al menos un sensor de cámara para crear al menos una imagen de vigilancia no enmascarada de la zona de vigilancia y/o de un sector de la zona de vigilancia. La creación de la imagen de vigilancia es, en particular, una captura de una imagen que muestra y/o reproduce la zona de vigilancia. El sensor de cámara comprende y/o es, en particular, un chip CCD o un chip CMOS. El sensor de cámara está configurado preferentemente para crear una imagen individual, algunas imágenes y/o una corriente de datos de imágenes, especialmente una secuencia de

vídeo, como imagen de vigilancia no enmascarada. La cámara presenta en particular una dirección de captura, en donde la cámara puede orientarse con la dirección de captura hacia la zona de vigilancia y/o el sector. El sensor de cámara está configurado para facilitar datos crudos, en particular, datos de imagen crudos. Los datos crudos comprenden al menos una imagen de vigilancia no enmascarada. En particular, los datos de imagen crudos comprenden la corriente de datos de imágenes. Preferentemente los datos crudos comprenden datos adicionales, en donde los datos adicionales comprenden, por ejemplo, un cronosellador y/o datos de sensor de sensores en la cámara. Los datos crudos son, en particular, datos digitales y/o analógicos.

La cámara comprende una unidad de evaluación, en donde la unidad de evaluación está integrada en la cámara. La unidad de evaluación está configurada en particular en tecnología de hardware, y es, por ejemplo, un procesador, un bloque electrónico, una unidad de ordenador y/o un microcontrolador. La unidad de evaluación comprende una interfaz de entrada para la recepción de los datos crudos. La interfaz de entrada es preferentemente una interfaz de cable. En particular, el sensor de cámara comprende una salida de sensor de cámara para facilitar los datos crudos, en donde la salida de sensor de cámara está conectada en términos de procesamiento de datos, por ejemplo, mediante una conexión de cables, exclusivamente con la interfaz de entrada. La conexión de salida de sensor de cámara e interfaz de entrada preferentemente está libre de ramificaciones y/o derivaciones, en donde entre salida de sensor de cámara e interfaz de entrada no está dispuesto en particular ningún módulo adicional.

La unidad de evaluación integrada comprende una interfaz de salida para facilitar datos de imagen de salida. La interfaz de salida es una interfaz de cable o una interfaz de radio como, por ejemplo, una interfaz WLAN, interfaz de infrarrojos o una interfaz Bluetooth. Los datos de imagen de salida son preferentemente datos digitales, como alternativa los datos de imagen de salida son datos analógicos.

La unidad de evaluación integrada comprende un módulo de verificación. El módulo de verificación está configurado en particular como un componente de hardware y/o componente de software en la unidad de evaluación integrada. El módulo de verificación está configurado para detectar, basándose en los datos crudos, una persona, algunas y/o todas las personas en la imagen de vigilancia no enmascarada y/o en la zona de vigilancia. En la imagen de vigilancia no enmascarada y/o la zona de vigilancia puede encontrarse al menos una persona, en particular, en la zona de vigilancia puede permanecer temporalmente al menos una persona. El módulo de verificación está configurado preferentemente para detectar todas las personas que se encuentran en la zona de vigilancia en la imagen de vigilancia no enmascarada y/o las imágenes de vigilancia no enmascaradas. El módulo de verificación está configurado, en particular, para examinar los datos crudos basándose en reglas, por ejemplo, en parámetros y/o características predeterminadas, estando configurados los parámetros para encontrar personas y/o para diferenciar personas y fondo. Los parámetros y/o características comprenden, por ejemplo, formas, velocidades y/o modelos.

La unidad de evaluación integrada comprende un módulo de enmascaramiento. El módulo de enmascaramiento es en particular un componente de hardware y/o componente de software en la unidad de evaluación. El módulo de enmascaramiento está configurado una imagen de vigilancia enmascarada crear. Como alternativa y/o complemento el módulo de enmascaramiento está configurado para generar una multitud de imágenes de vigilancia enmascaradas. En la imagen de vigilancia enmascarada la persona detectada en la imagen de vigilancia no enmascarada y/o todas las personas detectadas en la imagen de vigilancia no enmascarada están representadas enmascaradas. Por ejemplo, la imagen de vigilancia enmascarada es la imagen de vigilancia no enmascarada con anonimización adicional de las personas mediante enmascaramiento. El enmascaramiento se realiza preferentemente mediante una superposición, distorsión u otra desfiguración de la persona. En particular, para la anonimización todo el cuerpo de la persona está enmascarado, como alternativa solo la cabeza y/o zona de los ojos de la persona está enmascarada.

Los datos de imagen de salida comprenden exclusivamente imágenes de vigilancia enmascaradas. En particular, las imágenes de vigilancia enmascaradas y/o datos de imagen de salida no comprenden ninguna imagen de vigilancia enmascarada con personas y/o personas no enmascaradas. Los datos de imagen de salida no comprenden preferentemente ninguna información relativa a personas en la zona de vigilancia no enmascarada, en particular, los datos de imagen de salida no comprenden ninguna cara claramente reconocible. Las imágenes de vigilancia no enmascaradas sin personas son, en particular, imágenes de vigilancia enmascaradas.

Preferentemente la cámara comprende una interfaz de cámara, en donde la interfaz de cámara en términos de procesamiento de datos está conectada con la interfaz de salida. En particular, la interfaz de cámara coincide con la interfaz de salida y/o la forma. La interfaz de salida está configurada preferentemente para facilitar a un usuario de la cámara los datos de imagen de salida. Los datos de imagen de salida pueden comprender en particular datos adicionales como, por ejemplo, datos de sensor de sensores en la cámara, cronosellador y/o informaciones de ubicación.

Es una consideración de la invención facilitar una cámara asequible y fiable con cuya ayuda pueden vigilarse zonas de vigilancia, sin registrar, facilitar y/o almacenar datos referidos a personas. Ya no es necesaria una verificación de casos individuales costosa mediante un sistema de sensores adicional como, por ejemplo, con sensores de movimiento. La seguridad en términos de software contra ataques de terceros puede diseñarse ahora también de manera más sencilla, dado que la cámara está configurada para no poder emitir ninguna imagen de vigilancia con informaciones relativas a personas que pueden ser de interés para terceros. Para trabajadores y/o personas en la zona de vigilancia se logra una mejor transparencia real y/o percibida del proceso de anonimización de los datos de cámara de vigilancia.

- En un diseño especialmente preferido de la invención la cámara y/o la unidad de evaluación integrada comprende un módulo de segmentación. El módulo de segmentación está configurado para segmentar basándose en los datos crudos la imagen de vigilancia no enmascarada en una zona de persona y una zona de fondo. En particular, el módulo de segmentación está configurado para segmentar la imagen no enmascarada en varias zonas de persona y zonas de fondo, determinar por ejemplo para varias personas en una imagen de vigilancia varias zonas de persona. Las varias zonas de persona y/o zonas de fondo pueden estar unidas y/o fragmentadas. La zona de persona es, en particular, la zona que ocupa la persona en la imagen de vigilancia no enmascarada y/o enmascarada. Como alternativa y/o complemento la zona de persona es la zona de cabeza y/o de los ojos de la persona en la imagen de vigilancia enmascarada y/o no enmascarada. La zona de fondo es, en particular, la zona en la imagen de vigilancia enmascarada y/o no enmascarada que está libre de personas. Por segmentación se entiende, por ejemplo, la división, por ejemplo, distribución virtual y/o por zonas, de la imagen de vigilancia no enmascarada en dos zonas diferentes, concretamente las zonas de persona y las zonas de fondo. El diseño toma como base la consideración de facilitar una cámara que, por ejemplo, basándose en un reglamento, puede dividir una imagen de vigilancia en una zona con datos referidos a personas y una zona sin datos referidos a personas.
- Preferentemente el módulo de enmascaramiento está configurado para anonimizar en la imagen de vigilancia enmascarada la persona detectada coloreando y/o distorsionando de la zona de persona. En particular, el módulo de enmascaramiento está configurado para enmascarar todas las personas detectadas coloreando y/o distorsionando de las zonas de persona. Preferentemente la imagen de vigilancia enmascarada es la imagen de vigilancia no enmascarada con zona de persona teñida, en donde la zona de fondo permanece invariable. La coloración se realiza preferentemente con un contraste grande o pequeño con respecto al entorno de la zona de persona.
- En una configuración posible la cámara, en particular, la unidad de evaluación integrada comprende un módulo de estimación. El módulo de estimación está configurado para determinar un fondo estimado para la zona de persona, en donde el fondo estimado se determina o se estima preferentemente basándose en los datos crudos. Como alternativa y/o complemento el fondo estimado está almacenado de manera fija para la zona de vigilancia en el módulo de estimación. Además, es posible que el fondo estimado se determine nuevamente en cada momento mediante el módulo de estimación basándose en material de imagen y/o de sensor adicional. El fondo estimado es el fondo real de la zona en cuestión y/o una aproximación en la zona que la oculta/ocultan la persona y/o las personas en la imagen de vigilancia no enmascarada. El módulo de enmascaramiento está configurado en la imagen de vigilancia enmascarada para enmascarar la persona detectada llenando la zona de persona en la imagen de vigilancia no enmascarada con el fondo estimado. Preferentemente, la zona de persona llenada con el fondo estimado está enmarcada en la imagen de vigilancia enmascarada, en donde mediante el marco en la imagen de vigilancia enmascarada se remarca dónde se encuentra una persona enmascarada. Este diseño toma como base la consideración de crear imágenes de vigilancia enmascaradas con un enmascaramiento lo más desapercibido posible para personas y no perder informaciones de fondo.
- Es especialmente preferente que el módulo de verificación, el módulo de enmascaramiento, el módulo de segmentación y/o la unidad de evaluación esté configurado como una red neuronal. En particular, la red neuronal es una red de aprendizaje asociativo y que se mediante el modelo de aprendizaje ofrecido en conexión con el resultado esperado mediante retroalimentación. La red neuronal actúa preferentemente como filtro no lineal, en donde mediante entrenamiento de la red, mediante el cual se ajustan los parámetros disponibles de la red, se obtiene una función de filtro deseada. El diseño toma como base la consideración de facilitar una posibilidad especialmente efectiva, inteligente y/o rápida de la segmentación, verificación y enmascaramiento de imágenes de monitorización.
- En un diseño adicional de la invención y/o el módulo de verificación, el módulo de enmascaramiento, el módulo de segmentación y/o la unidad de evaluación comprende una matriz de puertas programables de campo, abreviado FPGA por sus siglas en inglés. Como alternativa el módulo de verificación, el módulo de enmascaramiento, el módulo de segmentación y/o la unidad de evaluación es y/o comprende otro subconjunto electrónico de programación y/o configuración fija. En particular la FGPA comprende elementos lógicos configurables, en donde la FPGA está configurada para la realización de lógica combinatoria entre distintas combinaciones booleanas. La ventaja de este diseño es obtener una cámara con unidad de evaluación integrada especialmente segura, rápida y a prueba frente a ataques.
- En particular está previsto que la detección de la persona mediante el módulo de verificación se base en una lógica difusa. Por ejemplo, el módulo de verificación está configurado para aplicar reglas difusas para la detección de una y/o varias personas en las imágenes de vigilancia no enmascaradas. El diseño toma como base la consideración de facilitar una cámara para la anonimización para lo cual es no es necesario ningún modelo matemático explícito para valorar los datos crudos.
- En un diseño especialmente preferido de la invención el módulo de verificación está configurado para llevar a cabo la detección de una persona y/o de todas las personas en la zona de vigilancia y/o la imagen de vigilancia no enmascarada basándose en un movimiento detectado. La detección de movimiento se realiza, por ejemplo, mediante evaluación de al menos dos imágenes de vigilancia capturadas con una distancia en el tiempo de un sector solapado y/o igual. Como alternativa y/o complemento, la detección de movimiento se realiza basándose en datos de sensor, de sensores integrados en la cámara y dirigidos hacia el sector. Preferentemente el módulo de verificación está configurado para seguir y/o hacer un seguimiento de una persona basándose en el movimiento detectado, en donde por ejemplo

están representadas enmascaradas zonas en la zona de vigilancia enmascarada, hacia la que se mueve la persona presumiblemente. El diseño toma como base la consideración de lograr una posibilidad de detección sencilla y un enmascaramiento de personas seguro, y reducir, por ejemplo, mediante enmascaramiento ampliado dirigido con seguridad elevada el peligro de zonas de persona no enmascaradas.

- 5 De acuerdo con la invención, la cámara y/o la unidad de evaluación integrada comprende un módulo de bloqueo. El módulo de bloqueo está diseñado con tecnología de hardware y/o de software. El módulo de bloqueo está dispuesto en términos de procesamiento de datos entre módulo de enmascaramiento e interfaz de salida y está conectado con estos en términos de procesamiento de datos. El módulo de bloqueo está configurado para bloquear y/o impedir una transmisión de datos crudos y/o una transmisión de imágenes de vigilancia no enmascaradas hacia los datos de imagen de salida. El módulo de bloqueo está configurado para examinar las imágenes de vigilancia enmascaradas en cuanto a personas y/o datos referidos a personas. El módulo de bloqueo está configurado para bloquear y/o interrumpir, en una detección de personas y/o datos referidos a personas en las imágenes de vigilancia enmascaradas, la emisión de datos de imagen de salida. El diseño toma como base la consideración de facilitar una cámara que impida de manera especialmente segura la emisión de imágenes de monitorización con datos referidos a personas hacia el exterior.
- 10
- 15 En un diseño adicional de la invención el módulo de bloqueo está configurado para impedir un flujo de datos de interfaz de salida en la dirección módulo de enmascaramiento y/o sensor de cámara. Por ejemplo, el módulo de bloqueo es una conexión en términos de procesamiento de datos que permite exclusivamente un flujo de datos de módulo de enmascaramiento a interfaz de salida. En particular, el módulo de bloqueo está configurado para impedir ataques desde el exterior y/o intentos de desconectar el módulo de enmascaramiento y/o acceder a imágenes de vigilancia no enmascaradas. El diseño toma como base la consideración de facilitar un nivel de seguridad para la cámara para que no pueda accederse a ninguna imagen de vigilancia no enmascarada.
- 20

Especialmente preferente es que el sensor de cámara y unidad de evaluación están dispuestos en una carcasa común. En particular, en la carcasa común puede disponerse una multitud de sensores de cámara, en donde la multitud de sensores de cámara está conectada con la unidad de evaluación. En la carcasa pueden disponerse, por ejemplo, otros sensores como, por ejemplo, sensores de movimiento, en donde los sensores facilitan datos de sensor que son preferentemente partes de los datos crudos. Preferentemente la cámara y/o la carcasa está remarcada hacia el exterior visualmente de manera llamativa, por ejemplo, con colores para que las personas en la zona de vigilancia reconozcan la cámara como cámara enmascarada. Este diseño se basa en la consideración de proponer una cámara y/o dispositivo de una sola pieza que tome imágenes de vigilancia anonimizadas y enmascaradas de una zona de vigilancia.

- 25
- 30 Otro objeto de la invención lo forma un dispositivo de vigilancia para vigilar una zona de vigilancia con una multitud de cámaras, en donde las cámaras comprenden un sensor de cámara para crear al menos una imagen de vigilancia no enmascarada de la zona de vigilancia y/o de un sector de la zona de vigilancia, en donde el sensor de cámara está configurado para facilitar datos crudos, en donde los datos crudos comprenden la al menos una imagen de vigilancia no enmascarada, con una unidad de evaluación integrada, en donde la unidad de evaluación comprende una interfaz de entrada para la recepción de los datos crudos y comprende una interfaz de salida para facilitar datos de imagen de salida, en donde la unidad de evaluación comprende un módulo de verificación y un módulo de enmascaramiento, en donde el módulo de verificación está configurado para detectar basándose en los datos crudos una persona en la imagen de vigilancia no enmascarada, en donde el módulo de enmascaramiento está configurado para crear una imagen de vigilancia enmascarada, en donde la persona detectada en la imagen de vigilancia está representada enmascarada, en donde los datos de imagen de salida comprenden exclusivamente imágenes de vigilancia enmascaradas. El dispositivo de vigilancia está configurado, en particular, para monitorizar zonas públicas, como parques o calles, o zonas no públicas, como fábricas.
- 35
- 40

Otras características, ventajas y efectos de la invención resultan de la siguiente descripción de un ejemplo de realización preferido de la invención, así como de las figuras adjuntas. A este respecto muestran:

- 45 figura 1 una vista esquemática de una cámara;
 figura 2 una imagen de vigilancia no enmascarada;
 figura 3 una imagen de vigilancia enmascarada.

La figura 1 muestra una cámara 1 en una vista esquemática. La cámara 1 es una cámara en color y está configurada para la videovigilancia de una zona de vigilancia 2. La zona de vigilancia 2 es, en este sentido, una zona de edificio, como por ejemplo una planta de producción en una fábrica. La cámara 1 presenta una carcasa 3. La carcasa 3 forma un encapsulamiento de los componentes de cámara con respecto al entorno. La carcasa 3 puede presentar medios de fijación para fijar la cámara 1 en la zona de vigilancia 2.

- 50 En la carcasa 3 están dispuestos un sensor de cámara 4 y una unidad de evaluación integrada 5. El sensor de cámara 4 es un chip semiconductor pixelado fotosensible que indica con dirección de captura hacia la zona de vigilancia 2. El sensor de cámara 4 está configurado para capturar imágenes de vigilancia no enmascaradas 6 (figura 2) de la zona de vigilancia 2. El sensor de cámara 4 presenta como interfaz de procesamiento de datos una salida de sensor de cámara 7, en donde la salida de sensor de cámara 7 está configurada para facilitar datos crudos, comprendiendo los datos crudos la imagen de vigilancia no enmascarada 6.
- 55

La unidad de evaluación integrada 5 es, por ejemplo, un bloque electrónico y presenta una interfaz de entrada 8 que está conectada en términos de procesamiento de datos, por ejemplo, mediante una línea conectada por cable, con la salida de sensor de cámara 7. A la interfaz de entrada 8 se facilitan de este modo los datos crudos y la imagen de vigilancia no enmascarada 6.

5 La unidad de evaluación integrada 5 presenta un módulo de verificación 9. El módulo de verificación 9 está conectado en términos de procesamiento de datos con la interfaz de entrada 8 y obtiene de este modo los datos crudos facilitados. El módulo de verificación 9 está configurado para verificar los datos crudos y/o las imágenes de vigilancia no enmascaradas 6 en cuanto a las personas 10 (figura 2) y detectar las personas encontradas 10 como tales. El módulo de verificación 9 analiza las imágenes de vigilancia no enmascaradas 6 en cuanto a determinadas características y
10 basándose en un reglamento evalúa si algo es una persona 10 o un objeto 11 (figura 2).

La unidad de evaluación integrada 5 comprende un módulo de segmentación 12 que está configurado para dividir la imagen de vigilancia no enmascarada 6 en zona de fondo y zona de persona 14 (figura 2). A este respecto, mediante el módulo de segmentación 12 se definen zonas en la imagen de vigilancia no enmascarada 6, que comprenden una persona 10 como zona de persona 14 y, por ejemplo, se representa como un rectángulo superpuesto por completo o
15 como una circunferencia. Las zonas sin personas 10 se establecen mediante el módulo de segmentación 12 como zona de fondo.

La unidad de evaluación integrada 5 comprende un módulo de enmascaramiento 15. El módulo de enmascaramiento 15 está configurado para generar una imagen de vigilancia enmascarada 16, en donde la imagen de vigilancia enmascarada 16 se corresponde con la imagen de vigilancia no enmascarada 6 con zonas de persona 14 rellenas con color y/o almacenadas. Las zonas de persona 14 almacenadas a color anonimizan personas 10 de modo que en la
20 imagen de vigilancia enmascarada 16 no están contenidas informaciones relativas a personas. El módulo de enmascaramiento 15 está conectado en términos de procesamiento de datos con una interfaz de salida 17 de la unidad de evaluación integrada 5, en donde a la interfaz de salida 17 se facilitan datos de imagen de salida desde el módulo de enmascaramiento 15. Los datos de imagen de salida comprenden la imagen de vigilancia enmascarada 16. Las
25 imágenes de vigilancia no enmascaradas 6 sin personas 10 y/o sin informaciones relativas a las personas son imágenes de vigilancia enmascaradas 16 generales.

La carcasa de cámara 3 presenta una interfaz de cámara 18, en donde mediante la interfaz de cámara 18 se facilitan a un usuario los datos de imagen de salida.

Entre interfaz de salida 17 y módulo de enmascaramiento 15 en la conexión por procesamiento de datos está dispuesto un módulo de bloqueo 19. El módulo de bloqueo 19 está configurado para defenderse de ataques de hackers desde el exterior. A este respecto, el módulo de bloqueo 19 está configurado para impedir una corriente de datos de interfaz de salida 17 al módulo de enmascaramiento 15, de modo que el módulo de enmascaramiento 15, por ejemplo, no pueda desconectarse y/o de modo que no pueda accederse a imágenes de vigilancia no enmascaradas 6.

La figura 2 muestra esquemáticamente una imagen de vigilancia no enmascarada 6. La imagen de vigilancia no enmascarada 6 presenta una pluralidad de objetos 11a, 11b y 11c y dos personas 10a y 10b. El módulo de verificación 9 está configurado para reconocer las personas 10a y 10b como personas y diferenciarlas de los objetos 11a, 11b y 11c.

El módulo de segmentación 12 ha distribuido la imagen de vigilancia no enmascarada 6 en una zona de fondo y dos zonas de persona 14a y 14b. La zona de persona 14a se crea mediante el módulo de segmentación 12 al delimitar la persona detectada 10a con un rectángulo, de modo que toda la persona 10a está solapada por la zona de persona 14a.
40 La zona de persona 14b se crea mediante el módulo de segmentación 12 al delimitar la cabeza de la persona detectada 10b con un rectángulo, de modo que solo la cabeza de la persona 10b está solapada por la zona de persona 14b.

La figura 3 muestra la imagen de vigilancia enmascarada 16 basada en la imagen de vigilancia no enmascarada 6. La imagen de vigilancia enmascarada 16 muestra los objetos 11a, 11b, 11c y 11d de la imagen de vigilancia no enmascarada 6. La imagen de vigilancia enmascarada 16 no muestra la persona 10a de la imagen de vigilancia no enmascarada 6. La imagen de vigilancia enmascarada 16 tampoco muestra la cabeza de la persona 10b de la imagen de vigilancia no enmascarada 6.

La unidad de evaluación integrada 5 de la cámara 1 presenta un módulo de estimación. El módulo de estimación está configurado para estimar, basándose en la imagen de vigilancia no enmascarada 6 y/u otras imágenes de la zona de vigilancia 2, un fondo para la zona de persona 14a. El fondo es, en particular, la zona de la zona de vigilancia que está oculta en la imagen de vigilancia no enmascarada 6 por la persona 10a. El fondo para la zona de persona 14a representa en este caso el objeto 11a. El módulo de enmascaramiento 15 está configurado para representar la zona de persona 14a en la imagen de vigilancia enmascarada 16 llenada con el fondo. La persona 10 está representada por lo tanto enmascarada y se anonimiza. Un tipo de enmascaramiento adicional muestra la zona de persona enmascarada 14b. El módulo de enmascaramiento 15 está configurado a este respecto para representar la zona de persona 14b mediante relleno de color. La cabeza de la persona 10b ya no puede reconocerse mediante el relleno de color en la
50 imagen de vigilancia enmascarada y la persona 10b se anonimiza de este modo.
55

REIVINDICACIONES

1. Cámara (1) para vigilar una zona de vigilancia (2)
con un sensor de cámara (4) para crear al menos una imagen de vigilancia no enmascarada (6) de la zona de vigilancia (2) y/o de un sector de la zona de vigilancia (2), en donde el sensor de cámara (4) está configurado para facilitar datos
5 crudos, en donde los datos crudos comprenden la al menos una imagen de vigilancia no enmascarada (6),
con una unidad de evaluación (5), en donde la unidad de evaluación (5) comprende una interfaz de entrada (8) para la recepción de los datos crudos y comprende una interfaz de salida (17) para facilitar datos de imagen de salida,
en donde la unidad de evaluación (5) comprende un módulo de verificación (9) y un módulo de enmascaramiento (15),
10 en donde el módulo de verificación (9) está configurado para detectar basándose en los datos crudos una persona (10, 10a, 10b) en la imagen de vigilancia no enmascarada (6),
en donde el módulo de enmascaramiento (15) está configurado para crear una imagen de vigilancia enmascarada (16), en donde la persona detectada (10, 10a, 10b) en la imagen de vigilancia enmascarada (16) está representada enmascarada,
15 en donde la unidad de evaluación (5) es una unidad de evaluación (5) integrada en la cámara (1), en donde los datos de imagen de salida comprenden exclusivamente imágenes de vigilancia enmascaradas (16)
caracterizada por
un módulo de bloqueo (19), en donde el módulo de bloqueo (19) está dispuesto en términos de procesamiento de datos entre módulo de enmascaramiento (15) e interfaz de salida (17), en donde el módulo de bloqueo (19) está configurado
20 para examinar las imágenes de vigilancia enmascaradas en cuanto a personas y/o datos referidos a personas y en una detección de personas y/o datos referidos a personas en las imágenes de vigilancia enmascaradas bloquear y/o interrumpir la emisión de datos de imagen de salida.
2. Cámara (1) según la reivindicación 1, caracterizada por un módulo de segmentación (12), en donde el módulo de segmentación (12) está configurado para segmentar basándose en los datos crudos la imagen de vigilancia no enmascarada (6) en una zona de persona (10, 10a, 10b) y una zona de fondo.
- 25 3. Cámara (1) según la reivindicación 2, caracterizada porque el módulo de enmascaramiento (15) está configurado para anonimizar en la imagen de vigilancia enmascarada (16) la persona detectada (10, 10a, 10b) coloreando la zona de persona (14, 14a, 14b) en la imagen de vigilancia no enmascarada (6).
4. Cámara (1) según la reivindicación 2, caracterizada por un módulo de estimación, en donde el módulo de estimación está configurado para determinar un fondo estimado para la zona de persona (14, 14a, 14b), en donde el módulo de enmascaramiento está configurado para enmascarar en la imagen de vigilancia enmascarada (16) la persona detectada
30 (10, 10a, 10b) llenando la zona de persona (14, 14a, 14b) en la imagen de vigilancia no enmascarada (6) con el fondo estimado.
5. Cámara (1) según una de las reivindicaciones precedentes, caracterizada porque el módulo de verificación (9), el módulo de enmascaramiento (15), el módulo de estimación y/o la unidad de evaluación integrada (5) está configurado
35 como una red neuronal.
6. Cámara (1) según una de las reivindicaciones precedentes, caracterizada porque el módulo de verificación (9), el módulo de enmascaramiento (15), el módulo de estimación y/o la unidad de evaluación integrada (5) están configurados como una matriz de puertas programables de campo.
7. Cámara (1) según una de las reivindicaciones precedentes, caracterizada porque la detección de la persona mediante
40 el módulo de verificación (9) se basa en una lógica difusa.
8. Cámara (1) según una de las reivindicaciones precedentes, caracterizada porque la detección de la persona mediante el módulo de verificación (9) se basa en una detección de movimiento.
9. Cámara según una de las reivindicaciones precedentes, caracterizada porque el módulo de bloqueo (19) está configurado para impedir un flujo de datos de la interfaz de salida (17) en la dirección del módulo de enmascaramiento
45 (15) y/o sensor de cámara (4).
10. Cámara (1) según una de las reivindicaciones precedentes, caracterizada porque sensor de cámara (4) y unidad de evaluación (4) están dispuestos en una carcasa común (3).
11. Dispositivo de vigilancia para vigilar una zona de vigilancia (2) con una multitud de cámaras (1) según una de las reivindicaciones 1-10.
- 50 12. Procedimiento para vigilar una zona de vigilancia (2) con las siguientes etapas:

- crear al menos una imagen de vigilancia no enmascarada (6) de la zona de vigilancia (2) y/o de un sector de la zona de vigilancia (2) mediante un sensor de cámara (4);
 - facilitar datos crudos mediante el sensor de cámara (4), en donde los datos crudos comprenden la al menos una imagen de vigilancia no enmascarada (6);
- 5 - facilitar una unidad de evaluación (5), en donde la unidad de evaluación (5) comprende una interfaz de entrada (8) para la recepción de los datos crudos y comprende una interfaz de salida (17) para facilitar datos de imagen de salida, en donde la unidad de evaluación (5) comprende un módulo de verificación (9) y un módulo de enmascaramiento (15);
- detectar a una persona (10, 10a, 10b) en la imagen de vigilancia no enmascarada (6) basándose en los datos crudos mediante el módulo de verificación (9);
- 10 - crear una imagen de monitorización enmascarada (16) mediante el módulo de enmascaramiento (15), en donde la persona detectada (10, 10a, 10b) está representada enmascarada en la imagen de vigilancia enmascarada (16),
- facilitar datos de imagen de salida que comprenden exclusivamente imágenes de vigilancia enmascaradas (16), mediante la unidad de evaluación (5), en donde la unidad de evaluación (5) es una unidad de evaluación (5) integrada en la cámara (1)
- 15 caracterizado por
- la facilitación de un módulo de bloqueo (19) dispuesto en términos de procesamiento de datos entre módulo de enmascaramiento (15) e interfaz de salida (17), en donde el módulo de bloqueo (19) examina las imágenes de vigilancia enmascaradas en cuanto a personas y/o datos referidos a personas, y en una detección de personas y/o datos referidos a personas en las imágenes de vigilancia enmascaradas bloquea y/o interrumpe la emisión de datos de imagen de salida.
- 20

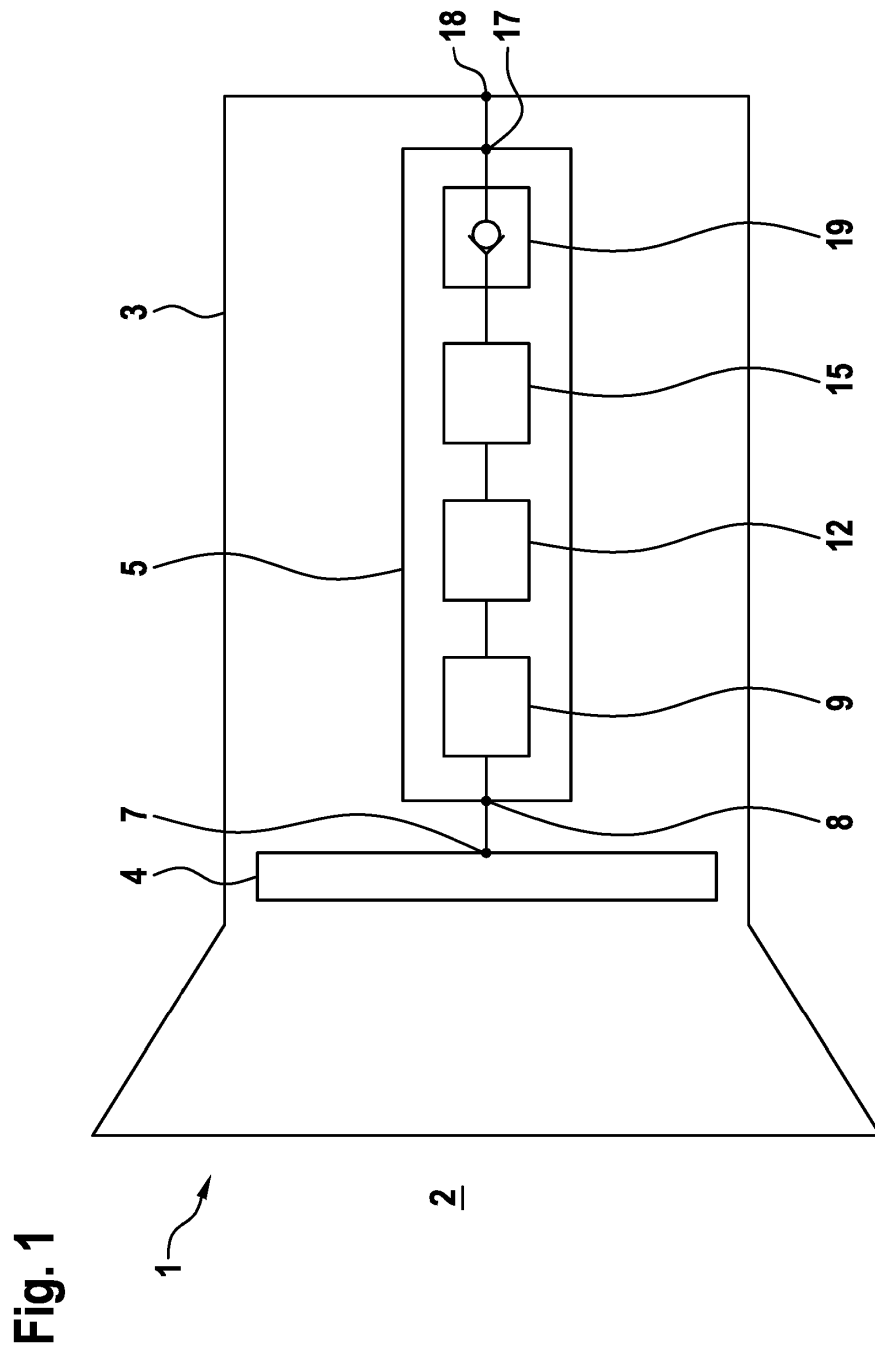


Fig. 2

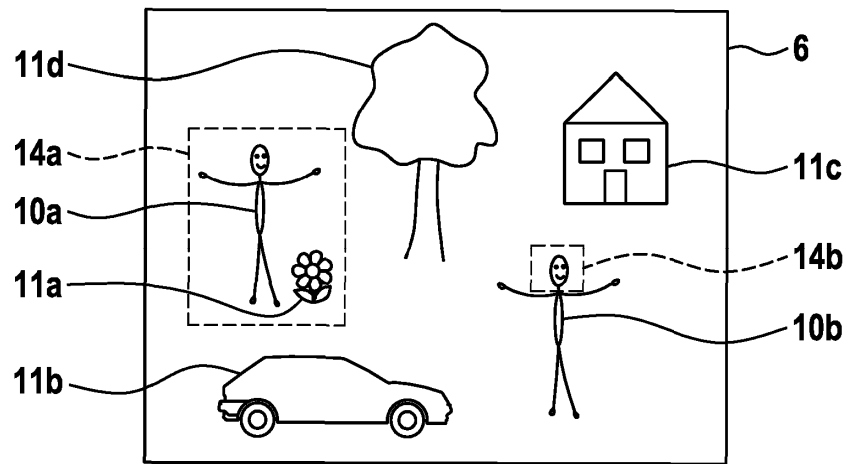


Fig. 3

