

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 882 403**

51 Int. Cl.:

G06F 21/62

(2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **09.07.2018** **E 18182498 (8)**

97 Fecha y número de publicación de la concesión europea: **07.04.2021** **EP 3594842**

54 Título: **Dispositivo sensor para la anonimización de los datos de sensor, dispositivo de supervisión de imágenes y método de funcionamiento de un dispositivo sensor para la anonimización de los datos de sensor**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2021

73 Titular/es:

ARGO AI GMBH (100.0%)
Ungererstraße 69
80805 München, DE

72 Inventor/es:

FRIEDMANN, FELIX y
GOLAKIYA, NIRAV

74 Agente/Representante:

TOMAS GIL, Tesifonte Enrique

ES 2 882 403 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

Dispositivo sensor para la anonimización de los datos de sensor, dispositivo de supervisión de imágenes y método de funcionamiento de un dispositivo sensor para la anonimización de los datos de sensor

[0001] La invención se refiere a un dispositivo sensor para la anonimización de datos de sensor que se recopilan por medio de un sensor del dispositivo sensor. La anonimización de los datos de sensor recopilados se realiza por medio de una unidad de anonimización del propio dispositivo sensor. La invención también proporciona un dispositivo de supervisión de imágenes que comprende el dispositivo sensor. Finalmente, la invención también se refiere a un método para el funcionamiento del dispositivo sensor inventivo.

[0002] Los dispositivos de supervisión de imágenes, tales como cámaras con un sensor de imagen CCD, garantizan la seguridad y el orden públicos al proporcionar medios de vigilancia de su entorno. Dichos dispositivos de supervisión de imágenes se pueden incorporar en infraestructuras de tráfico, tales como postes de luz, farolas o carteles publicitarios, a lo largo de los bordes de las carreteras, para proporcionar vigilancia del tráfico. En los últimos años, sin embargo, los vehículos con tales sistemas de supervisión proporcionan un medio adicional de vigilancia del tráfico. Los vehículos se comunican entre sí y con la infraestructura de tráfico para transferir los datos recopilados para garantizar una mejor vigilancia. Recientemente, la interconexión cada vez mayor de vehículos entre sí o con la infraestructura de tráfico puede generar problemas en términos de privacidad de los datos. Generalmente, al menos un servidor procesa y distribuye datos recopilados por sensores a bordo de los vehículos. Los datos pueden contener permisos sensibles, tales como caras, matrículas o números de casa. Actualmente, esta información se transfiere al servidor y solo luego se hace anónima antes de su procesamiento posterior.

[0003] El documento US 2013/0108105 A1 divulga un método y un aparato para enmascarar la región de privacidad en base a una imagen de vídeo supervisada. Una unidad de detección de objetivos extrae un objeto objetivo del vídeo decodificado y detecta una región de enmascaramiento de privacidad del objeto objetivo extraído. Una unidad de enmascaramiento de la región de privacidad oculta la región de enmascaramiento de privacidad. La región de privacidad se puede detectar mediante aprendizaje automático. Sin embargo, el documento no revela la posibilidad de usar otros datos de sensor de los datos de la cámara, por ejemplo, datos LIDAR. Además, los datos de la cámara necesitan almacenarse como preparación de la anonimización. Si se interrumpe el funcionamiento del aparato, por ejemplo en caso de falla, estos datos almacenados con regiones desenmascaradas pueden ser extraídos de ese almacenamiento.

[0004] El documento DE 10 2012 002 390 A1 divulga un método y un dispositivo para una anonimización de matrículas. El dispositivo tiene una sección de control que recibe la imagen de una matrícula de un vehículo fotografiada por dos cámaras en dos puntos de control. La imagen que es tomada por las dos cámaras de la matrícula contiene solo partes de las matrículas, de modo que la matrícula está parcialmente anonimizada. La sección de control determina la velocidad media del vehículo entre los puntos de control. Un ordenador determina si la velocidad media excede el límite de velocidad predeterminado. Si este es el caso, una tercera cámara toma una fotografía completa de la matrícula y permite la asignación individual de la matrícula. Sin embargo, dicho documento no revela ningún método específico de anonimización de los datos de la cámara o los datos de sensor, además de no tomar ninguna imagen completa de la placa del sensor.

[0005] El documento US 2011/0161140 A1 divulga una unidad a bordo para un sistema de peaje de carretera que incluye al menos una cámara, que está dirigida hacia un pasajero de un vehículo que lleva la unidad a bordo y una unidad de evaluación, que cuenta a los pasajeros del vehículo en una imagen grabada por una cámara. En una forma de realización, la unidad de evaluación oculta a los pasajeros detectados en la imagen grabada. Sin embargo, no se revela ningún detalle sobre cómo se oscurecen las imágenes.

[0006] El documento US 2008/180538 A1 divulga un sistema que incluye un dispositivo de formación de imágenes operable para adquirir una imagen de un sujeto. El sistema también incluye un circuito anonimizador operable para generar una imagen anonimizada que incluye una menor fidelidad de una propiedad de un sujeto de la imagen adquirida en respuesta a una política de anonimización. El sistema incluye, además, una pantalla operable para proporcionar una indicación perceptible por humanos de la política de anonimización.

[0007] Un objeto de la presente invención es proporcionar un dispositivo sensor universalmente aplicable para la anonimización de los datos de sensor recopilados en un vehículo.

[0008] El objeto se logra mediante el objeto de las reivindicaciones independientes. Los desarrollos ventajosos con otras formas de realización convenientes y no triviales de la invención se especifican en la siguiente descripción, las reivindicaciones dependientes y las figuras.

[0009] La invención proporciona un dispositivo sensor para recopilar los datos de sensor del entorno del dispositivo sensor y anonimizar los datos de sensor recopilados por medio de una unidad de anonimización, donde el sensor es un sensor LIDAR y/o un sensor de radar. Los datos recopilados describen el entorno del

dispositivo sensor. En otras palabras, los datos de sensor recopilados comprenden información o la información física del entorno dependiendo del tipo de sensor. Alternativamente, si el sensor es un sensor de imagen (por ejemplo, sensor CCD) de una cámara, entonces la información podría tener forma de píxeles de color y/o infrarrojos de la imagen de la cámara. Según la invención, el sensor puede tener la forma de un sensor LIDAR, donde, en este caso, la información del entorno tiene forma de representaciones en 3D del entorno. Un dispositivo sensor con dicho sensor plantea un problema, en el que la información sensible, como una privacidad personal y/o una cara y/o una matrícula de vehículo y/o un número de casa, se puede exponer fácilmente en una imagen generada por el sensor. Se debe evitar tal exposición de información sensible, por lo tanto, se debe realizar una anonimización de la información sensible. Esto se realiza por medio de la unidad de anonimización, que está incorporada en el dispositivo sensor. La incorporación se realiza de manera que se evita o hace imposible el almacenamiento permanente de cualquiera de los datos sensibles predefinidos (por ejemplo, caras).

[0010] El sensor del dispositivo sensor es un sensor LIDAR y/o un sensor de radar. En otras palabras, el uso del sensor LIDAR en el dispositivo sensor se puede usar para obtener la información del entorno del dispositivo sensor en forma de representación en 3D del entorno. Esto es, en particular, ventajoso en caso de ausencia de luz suficiente, como durante la noche, donde la representación en 3D del entorno por medio del sensor LIDAR se puede usar para obtener vigilancia. Además, en el caso de la presencia de una gran cantidad de luz, un sensor CCD proporciona un medio económico y eficiente de obtener vigilancia. Además, es posible pensar que una combinación de los sensores anteriormente mencionados, es decir, el sensor LIDAR y el sensor CCD, se puede usar al mismo tiempo para obtener un alto grado de vigilancia del entorno. Además, se puede pensar que en el dispositivo sensor se pueden usar otros sensores, tales como un sensor de imagen óptico y/o un sensor infrarrojo y/o un sensor ultrasónico. Los dos primeros sensores son ejemplos de sensor 2D, los sensores restantes son un ejemplo de un sensor 3D.

[0011] El sensor del dispositivo sensor está diseñado para generar un flujo de datos de sensor, es decir, una secuencia de imágenes, por ejemplo, en forma de un flujo MPEG. El sensor está acoplado a la unidad de anonimización por medio de una ruta de datos. La ruta de datos puede comprender un cable y/o un circuito electrónico y/o una fibra óptica. Dependiendo de la forma de transmisión del flujo de datos de sensor desde el sensor hasta la unidad de anonimización, la ruta de datos puede no contener ninguna memoria digital o solo una memoria volátil. La memoria volátil puede ocurrir en forma de un registro procesador o un búfer o RAM, solo para nombrar ejemplos. En los casos en los que la transmisión del flujo de datos de sensor desde el sensor hasta la unidad de anonimización se puede realizar a la velocidad a la que el sensor genera los datos, entonces no se requiere ninguna memoria digital en la ruta de datos. Como ejemplo para el uso de un registro de procesador, se podría considerar la transmisión del flujo de datos de sensor en serie, por ejemplo, por medio de una arquitectura de bus en serie. Entonces, es posible que se necesite una memoria volátil en la ruta de datos. En el caso de una memoria volátil, sin ninguna tensión de suministro, los datos almacenados se pierden o se borran en la memoria volátil. Esto es una ventaja, ya que el flujo de datos de sensor comprende los datos de sensor recopilados del sensor, que en sí mismo, comprende dichos datos sensibles, que son datos que contienen información sensible, y se envían a la unidad de anonimización para la anonimización de los datos de sensor recopilados del flujo de datos de sensor. Es necesario asegurarse de que los datos de sensor recopilados con la información sensible no se almacenen en una memoria.

[0012] En el caso de pérdida de tensión de suministro, es necesario asegurarse de que ninguno de los datos de sensor en la ruta de datos sea accesible para una segunda persona. En el caso de que no se necesite ninguna memoria digital en la ruta de datos, se asegura que ningún dato sea accesible para una segunda persona. Sin embargo, en el caso de que se necesite una memoria en la ruta de datos, la invención también tiene en cuenta el problema de la accesibilidad del flujo de datos de sensor, en el caso de una pérdida repentina de la tensión de suministro. Esto se garantiza usando la memoria solo en forma de memoria volátil que, debido a sus propiedades, pierde o elimina los datos de sensor almacenados en caso de pérdida de la tensión de suministro. Por lo tanto, se asegura que se realiza una transmisión de eliminación automática del flujo de datos de sensor desde el sensor hasta la unidad de anonimización.

[0013] Según la presente invención, la unidad de anonimización comprende un módulo de análisis para aplicar un criterio de privacidad predefinido en el flujo de datos de sensor para identificar datos sensibles predefinidos (por ejemplo, caras). El módulo de análisis puede tener la forma de un programa de *software* y/o un ASIC (circuito integrado de aplicación específica, por sus siglas en inglés) y/o un FPGA (matriz de puertas programables en campo, por sus siglas en inglés). Mientras que los datos sensibles en el flujo de datos de sensor pueden tener forma de, por ejemplo, datos de privacidad y/o caras y/o matrículas de vehículos y/o números de casa. El criterio de privacidad predefinido se puede definir por medio de al menos un método o algoritmo, como un algoritmo basado en al menos una información de borde e/o información de forma y/o distribución de color e/o información del vídeo original/flujo de datos de sensor e/o información de al menos un flujo de datos de referencia y/o datos de aprendizaje automático. En otras palabras, en un momento determinado, cuando el flujo de datos de sensor se transmite a la unidad de anonimización, el módulo de análisis lee los datos de sensor particulares proporcionados en el flujo de datos de sensor en ese momento y sobre la base de, por ejemplo, un algoritmo de red neuronal artificial, reconoce al menos una región en los datos de sensor correspondiente a la información sensible.

[0014] Dicha región o dicho subconjunto de datos de sensor del flujo de datos de sensor se denominan datos sensibles. Es decir, el módulo de análisis es capaz de identificar y clasificar al menos una región o un subconjunto de datos de sensor en el flujo de datos de sensor como datos sensibles. El resto del flujo de datos de sensor se puede clasificar como las regiones de datos normales, es decir, datos que no necesitan anonimización. Por ejemplo, en el caso de un flujo de datos de sensor recopilado por un dispositivo sensor en un vehículo, este flujo de datos de sensor podría incluir imágenes de una escena de tráfico. En un momento determinado, el flujo de datos de sensor alcanza la unidad de anonimización. En este momento determinado, el módulo de análisis analiza el flujo de datos de sensor que puede comprender información de los vehículos del entorno en el entorno del vehículo. El módulo de análisis es capaz de identificar y clasificar dichos datos sensibles correspondientes a información sensible, como, por ejemplo, al menos una matrícula de vehículo, y puede marcar estos datos sensibles.

[0015] Según la presente invención, la unidad de anonimización comprende, además, un módulo de sustitución para sustituir los datos sensibles en el flujo de datos de sensor por datos de enmascaramiento predefinidos, de manera que los datos de sensor se anonimizan en el flujo de datos de sensor antes de cualquier almacenamiento en una memoria no volátil. En otras palabras, el módulo de sustitución puede comprender un programa de *software* y/o un ASIC y/o un FPGA, que está diseñado para sustituir los datos sensibles en el flujo de datos de sensor por datos de enmascaramiento predefinidos, como un desenfoque de los datos sensibles o sustituir una distribución de color en los datos sensibles por un color monocromático o un solo color (por ejemplo, píxeles blancos o píxeles negros). Esto es una ventaja porque la anonimización de los datos sensibles se realiza sin transformar la imagen original y/o dentro del flujo de datos de sensor.

[0016] Dicha memoria no volátil puede ser, por ejemplo, un disco duro y/o un USB (bus universal en serie, por sus siglas en inglés) y/o una nube de datos. Además, es posible que los datos de sensor recopilados se puedan transferir a un sistema de supervisión del tráfico, donde los datos de sensor recopilados de diferentes vehículos y/o infraestructuras estáticas, tales como una cámara en los postes de luz y/o un semáforo, se pueden almacenar en una memoria no volátil en el sistema de supervisión del tráfico. En general, esto permite que la anonimización de los datos de sensor tenga lugar en tiempo real en el camino del sensor, incluso antes de que se almacenen en la memoria no volátil. En otras palabras, el flujo de datos de sensor que es capturado por el dispositivo sensor se hace directamente anónimo antes de que el flujo de datos de sensor sea procesado y transmitido a otro dispositivo o sistema, especialmente fuera del dispositivo sensor. Por lo tanto, el flujo de datos de sensor que proviene del dispositivo sensor se anonimiza directamente antes de que los datos de sensor del flujo de datos de sensor se almacenen en una memoria no volátil.

[0017] La invención también comprende formas de realización que proporcionan características que ofrecen ventajas técnicas adicionales.

[0018] En una forma de realización, el dispositivo sensor puede contener un módulo de encriptación, que está diseñado para encriptar al menos una parte del flujo de datos de sensor antes de almacenarlo en la memoria no volátil. El módulo de encriptación puede tener la forma de un programa de *software* de encriptación y/o un ASIC y/o un FPGA que usa criptografía para evitar el acceso no autorizado a los datos de un sensor almacenados en la memoria no volátil. Por ejemplo, después de un accidente de un vehículo que lleva la memoria no volátil o después de un robo de la memoria no volátil, como un disco duro, los datos de sensor almacenados en el disco duro todavía están protegidos debido a la encriptación de los datos de sensor por medio del módulo de encriptación.

[0019] En una forma de realización, el módulo de análisis del dispositivo sensor comprende al menos una red neuronal artificial para analizar el flujo de datos de sensor y/o el módulo de sustitución comprende al menos una red neural artificial para sustituir los datos sensibles. La al menos una red neuronal artificial del módulo de análisis se puede entrenar mediante el método de aprendizaje automático para identificar los datos sensibles en el flujo de datos de sensor. De forma similar, al menos una red neuronal artificial del módulo de sustitución se puede entrenar mediante un método de aprendizaje automático para sustituir los datos sensibles sobre la base de un valor de datos predefinido (es decir, los datos de enmascaramiento), como un píxel monocromático y/o una visión borrosa de los datos sensibles del flujo de datos de sensor. Esto permite una operación eficiente del módulo de análisis y el módulo de sustitución del dispositivo sensor. Por lo tanto, se realiza una anonimización eficiente y fiable de los datos de sensor en tiempo real por medio del dispositivo sensor de la invención. El módulo de análisis y el módulo de sustitución puede compartir una red neuronal artificial común.

[0020] En una forma de realización, el flujo de datos de sensor contiene información de una observación del tráfico. En otras palabras, el dispositivo sensor se puede incorporar en una infraestructura de tráfico. La infraestructura de tráfico puede comprender una infraestructura estática, como un poste de luz y/o un semáforo y/o un edificio enfrente de una calle y/o un cartel publicitario de los bordes de las carreteras. Adicional o alternativamente, el dispositivo sensor se puede incorporar en una infraestructura móvil de la infraestructura de tráfico, como un vehículo, como un vehículo o una locomotora. Esto permite una vigilancia de toda la región de tráfico, que incluye al menos vehículo móvil en la calle, al menos un vehículo móvil, como una bicicleta y/o una

persona que camina por el lado de los peatones a lo largo de la calle y/o eventos y/o actividades que tienen lugar en una región a lo largo de la calle. Además, la incorporación del dispositivo sensor en la infraestructura estática de la infraestructura de tráfico puede permitir identificar el número de personas que se sienta en un vehículo, lo que podría ser importante en el caso de un sistema de peaje de carretera. Por lo tanto, se logra una vigilancia de toda la región de tráfico, lo que garantiza una seguridad y protección del transporte público. Al mismo tiempo, se puede realizar la anonimización de los datos sensibles pertinentes, tales como la matrícula del vehículo, las caras de las personas en el vehículo, así como en el lado de los peatones a lo largo de la calle.

[0021] En una forma de realización, el criterio de privacidad predefinido puede proporcionar una definición para la información que debe ser anonimizada en el flujo de datos de sensor como datos sensibles. En otras palabras, en base a la información, como información de al menos información de un borde y/o de una forma y/o distribución de color de datos de un sensor en el flujo de datos de sensor, un algoritmo basado en el reconocimiento de una región de la cara habilita el módulo de análisis del dispositivo sensor para identificar los datos sensibles de los datos de sensor.

[0022] En una forma de realización, la información que debe ser anonimizada en el flujo de datos de sensor puede ser una cara y/o una matrícula de vehículo y/o un número de casa. Esto es una ventaja, porque esta información son los datos sensibles más frecuentes que necesitan ser anonimizados en el flujo de datos de sensor.

[0023] En una forma de realización, la ruta de datos puede comprender al menos un cable y/o un circuito electrónico y/o una fibra óptica. Por lo tanto, pueden proporcionarse múltiples opciones para un usuario del dispositivo sensor para la transmisión de los datos de sensor desde el sensor hasta la unidad de anonimización.

[0024] En una forma de realización, el flujo de datos de sensor puede comprender datos brutos o datos codificados en MPEG. En otras palabras, el flujo de datos de sensor puede comprender puntos de coordenadas tridimensionales, por ejemplo, en el caso de un sensor LIDAR, o datos de un vídeo o audio dependiendo del tipo de sensor usado. Esto es una ventaja porque proporciona una flexibilidad para usar diferentes tipos de sensores para recopilar la información del entorno del dispositivo sensor, ya que el dispositivo sensor es capaz de procesar diferentes formas de datos brutos o datos codificados en MPEG. Además, se pueden detectar de forma fiable diferentes características del entorno, si se combinan diferentes formas de datos brutos o datos codificados en MPEG de diferentes sensores para obtener una vigilancia del entorno.

[0025] En una forma de realización, el módulo de sustitución está diseñado para generar datos de un enmascaramiento sobre la base de un valor de datos predefinidos (por ejemplo, píxeles blancos o píxeles negros) y/o difuminando una región de la imagen. En otras palabras, el módulo de sustitución sustituye los datos sensibles marcados por el módulo de análisis por valores de datos predefinidos, tales como el color monocromático o difuminando los datos sensibles. Por lo tanto, se realiza la anonimización de los datos de sensor.

[0026] La invención también comprende un dispositivo de supervisión de imágenes que comprende un dispositivo sensor para la anonimización de datos de sensor recopilados por el dispositivo sensor. El dispositivo de supervisión de imágenes se puede incorporar en al menos una infraestructura estática o fija, por ejemplo, una cámara en un poste de luz para la vigilancia del tráfico o en un túnel. Además, el dispositivo de supervisión de imágenes puede tener forma de un vehículo de motor. El vehículo de motor puede comprender varios sensores para generar respectivamente datos de sensor que contienen información sobre el entorno del vehículo de motor. El vehículo de motor puede ser un vehículo de pasajeros o una locomotora o un camión o una motocicleta. Esto es ventajoso porque permite incorporar el dispositivo de supervisión de imágenes en toda la infraestructura de un tráfico o de una ciudad, de modo que se asegura una vigilancia del entorno del tráfico o la ciudad.

[0027] La invención comprende, además, un método de funcionamiento de un dispositivo sensor para anonimizar un flujo de datos de sensor que es generado por un sensor del dispositivo sensor. El primer paso del método inventivo incluye identificar datos sensibles predefinidos en el flujo de datos de sensor por medio de un criterio de privacidad predefinido a través de un módulo de análisis. En otras palabras, el módulo de análisis puede ser un programa de *software* que comprende un algoritmo de red neuronal artificial que está diseñado para identificar datos sensibles, tales como una cara y/o una matrícula de vehículo y/o un número de casa. El módulo de *software* puede comprender, además, un algoritmo que está diseñado para rastrear al menos una región en movimiento en un fotograma de vídeo, como un filtro de Kalman o un filtro de partículas o un filtro bayesiano o una extracción de características para rastrear y detectar al menos una región en movimiento o los datos sensibles en el flujo de datos de sensor.

[0028] Después de la identificación de los datos sensibles por el módulo de análisis, el método inventivo comprende, además, un segundo paso, que incluye sustituir los datos sensibles en el flujo de datos de sensor a través de un módulo de sustitución por datos de enmascaramiento predefinidos, de manera que los datos de sensor se anonimizan en el flujo de datos de sensor antes de cualquier almacenamiento en una memoria no volátil. Por lo tanto, el método inventivo permite una anonimización de los datos de sensor en tiempo real.

[0029] En otra forma de realización del método inventivo, el dispositivo sensor puede ser una parte de un vehículo, de manera que la anonimización de los datos de sensor a través del dispositivo sensor se realice a bordo del vehículo. El propio vehículo comprende varios sensores para generar datos de sensor sin procesar el entorno, como los sensores LIDAR y/o los sensores CCD. Esto es una ventaja porque el vehículo puede proporcionar vigilancia de su entorno durante su movimiento tanto durante el día como durante la noche, lo cual se puede realizar debido a la presencia de diferentes tipos de sensores. Además, es posible pensar que el dispositivo sensor incorporado en el vehículo se enciende incluso cuando el vehículo no está en marcha o el vehículo está estacionado en una ubicación particular. Los datos de sensor obtenidos se pueden almacenar en una memoria no volátil en el propio vehículo. Esto es beneficioso por motivos de seguridad, por ejemplo, en caso de daño a un vehículo, el dispositivo sensor encendido puede registrar el entorno del vehículo e identificar a la persona involucrada que comete la infracción.

[0030] En otra forma de realización del método inventivo, el flujo de datos de sensor anonimizado se puede transmitir a un sistema de supervisión del tráfico y/o a una nube de datos. Esto es una ventaja porque, en el caso de un robo de vehículo, los datos de sensor anonimizados obtenidos se guardan todavía en una ubicación segura diferente, como el sistema de supervisión del tráfico y/o la nube de datos. Esto permite a las fuerzas de seguridad identificar a la persona que comete la infracción y posibilitar la obtención del vehículo robado.

[0031] La invención también comprende las diversas combinaciones de las características de las formas de realización descritas, si no se indica lo contrario. A continuación, se describe una implementación ejemplar de la invención. Las figuras muestran:

Figura 1 una ilustración esquemática de una forma de realización de un dispositivo sensor; y

Figura 2 una ilustración esquemática de una forma de realización de un método de funcionamiento del dispositivo sensor.

La forma de realización explicada a continuación es una forma de realización preferida de la invención. Sin embargo, en la forma de realización, los componentes descritos de la forma de realización representan cada uno características individuales de la invención que deben considerarse independientes entre sí y que desarrollan cada uno la invención también independientemente entre sí y, por lo tanto, también deben considerarse como un componente de la invención de manera individual o en una combinación distinta a la mostrada. Además, la forma de realización descrita también se puede suplementar con otras características de la invención ya descritas.

[0032] En las figuras, los elementos que cumplen la misma función están marcados con idénticos signos de referencia.

[0033] La figura 1 muestra una ilustración esquemática de una forma de realización de un dispositivo sensor 10. El dispositivo sensor 10 está incorporado en un vehículo 11 que puede ser un vehículo de pasajeros. El vehículo 11 puede comprender un sistema de asistencia al conductor (no mostrado en la figura), que puede proporcionar, por ejemplo, una funcionalidad de piloto automático. En otras palabras, el sistema de asistencia al conductor puede conducir el vehículo 11 de forma autónoma o completamente automática. El dispositivo sensor 10 comprende un sensor 12 que es un sensor LIDAR y/o un sensor de radar. El dispositivo sensor 10 puede proporcionarse como una cámara o, más generalmente, como un dispositivo de supervisión de imágenes 30. Sin embargo, dado que el vehículo 11 puede comprender varios sensores, el dispositivo sensor 10 puede comprender una pluralidad de sensores o se pueden proporcionar varios dispositivos sensores con diferentes sensores.

[0034] En la forma de realización actual mostrada en la figura 1, en aras de la claridad, se supone que el dispositivo sensor 10 comprende solo un sensor 12. El dispositivo de supervisión de imágenes 30 que comprende el dispositivo sensor 10 puede tener forma de una videocámara o una cámara infrarroja, que se puede incorporar en el vehículo 11. El sensor 12 está diseñado para recopilar datos de un sensor y generar un flujo de datos de sensor 13 del entorno del vehículo 11 de los datos de sensor recopilados. El campo de visión del sensor 12, que está diseñado para recopilar los datos de sensor y generar el flujo de datos de sensor 13 del entorno del vehículo 11 de los datos de sensor recopilados, se muestra por medio de líneas discontinuas 32. El entorno del vehículo 11 puede comprender otro vehículo 31, que puede circular delante del vehículo 11. En el ejemplo mostrado, el vehículo 31 comprende una matrícula de vehículo 14, por ejemplo, "D NE U123". Al lado del vehículo 31 puede haber una calle peatonal 16, donde puede haber una persona 15 caminando en una dirección opuesta a la del vehículo 11. Además, al lado de la calle peatonal 16 puede estar situada una casa 17. La casa 17 tiene un número de casa 18, por ejemplo, "05".

[0035] El sensor 12 puede recopilar los datos de sensor del flujo de datos de sensor 13, que pueden tener forma de al menos un fotograma de vídeo, y pueden generar un primer flujo de datos de sensor T1 que puede tener forma de un flujo de datos de del sensor 13 codificado en MPEG.

[0036] El dispositivo sensor 10 puede comprender, además, una unidad de anonimización 19. El primer flujo de datos de sensor T1 puede transmitirse a la unidad de anonimización 19 por medio de una primera ruta de datos 20, que puede comprender un cable y/o un circuito electrónico y/o una fibra óptica. El primer flujo de datos de sensor T1 se puede transmitir directamente a la unidad de anonimización 19 a través de la primera ruta de datos 20 que no contiene ninguna memoria digital. Esto es útil cuando la transmisión del primer flujo de datos de sensor T1 desde el sensor 12 hasta la unidad de anonimización 19 se realiza a la velocidad a la que el sensor 12 genera los datos. Sin embargo, en casos en los que, por ejemplo, se usa un registro de procesador, se podría considerar la transmisión del primer flujo de datos de sensor T1 en serie, por ejemplo, por medio de una arquitectura de bus en serie. En este caso, puede ser necesaria una memoria volátil 22 en una segunda ruta de datos 21.

[0037] La unidad de anonimización 19 comprende un módulo de análisis 23 que puede tener forma de un programa de *software* o un ASIC o un FPGA. El módulo de análisis 23 está diseñado para identificar datos sensibles predefinidos, por ejemplo, una cara de la persona 15 y/o las matrículas de vehículos 14 y/o el número de casa 18, en el primer flujo de datos de sensor T1 por medio de un criterio de privacidad predefinido. El criterio de privacidad puede enumerar o definir aquellas características en el primer flujo de datos de sensor T1 que se identifican y/o se clasifican como datos sensibles. Por lo tanto, la persona experta puede definir los datos sensibles según las necesidades actuales proporcionando un criterio de privacidad predefinido en consecuencia.

[0038] Como se muestra en la figura 2, el módulo de análisis 23 puede leer en el primer flujo de datos de sensor T1 e identificar y/o clasificar los datos sensibles, tales como la cara de la persona 15, la matrícula de vehículo 14 y el número de casa 18, en base a un criterio de privacidad predefinido. El criterio de privacidad predefinido puede incluir un algoritmo, como un primer algoritmo de red neuronal artificial 28 basado en datos de susceptibilidad de aprendizaje automático.

[0039] El módulo de análisis 23 puede generar a partir del primer flujo de datos de sensor T1 un segundo flujo de datos de sensor T2, donde se marcan los datos sensibles. Por ejemplo, la cara de la persona 15, la matrícula de vehículo 14 y el número de casa 18 se marcan como datos sensibles a través de una región cuadrática o rectangular respectiva (cuadro delimitador), como se muestra con líneas discontinuas. Sin embargo, es posible pensar que las regiones que describen los datos sensibles se pueden ajustar según la forma de los datos sensibles. Por ejemplo, la cara de la persona 15 se puede marcar mediante una región circular o una región ovalada, cuya área es suficiente para marcar la cara de la persona 15. Esto se puede hacer para incorporar una máxima información admisible posible en el segundo flujo de datos de sensor T2. Alternativamente, los píxeles individuales en el segundo flujo de datos T2 se pueden marcar como datos sensibles o datos no sensibles. Esto evita el uso de una forma estándar, como un rectángulo o un óvalo.

[0040] Por lo tanto, el primer flujo de datos de sensor T1 se transmite desde el sensor 12 hasta el módulo de análisis 23 de la unidad de anonimización 19. Aquí, el primer flujo de datos de sensor T1 se convierte en el segundo flujo de datos de sensor T2, que incluye los datos sensibles, tales como la cara de la persona 15, la matrícula de vehículo 14 y el número de casa 18, que se marcan como datos sensibles. En lugar de convertir el primer flujo de datos de sensor T1 en un segundo flujo de datos de sensor T2, el primer flujo de datos de sensor T1 se puede reenviar sin cambios y la información que identifica los datos sensibles puede proporcionarse por separado, por ejemplo, por medio de coordenadas de regiones que se identifican como datos sensibles en el primer flujo de datos de sensor T1. En aras de la simplicidad, la siguiente descripción asume que se proporciona un segundo flujo de datos de sensor T2, aunque el primer flujo de datos de sensor T1 se puede usar en su lugar con la información relativa a las regiones marcadas proporcionadas por separado.

[0041] La unidad de anonimización 19 comprende, además, un módulo de sustitución 24, que está diseñado para sustituir los datos sensibles del segundo flujo de datos de sensor T2 por datos de enmascaramiento predefinidos, de manera que el segundo flujo de datos de sensor T2 se anonimiza antes de almacenarse en cualquier memoria no volátil, como un disco duro 25 y/o una nube de datos 26. El módulo de sustitución 24 puede recibir el segundo flujo de datos de sensor T2 con regiones marcadas de los datos sensibles y enmascarar los datos sensibles en el segundo flujo de datos de sensor T2, por ejemplo, por medio de un algoritmo de red neuronal artificial 27, como regiones borrosas o como regiones con un color predefinido que pueden ser diferentes del color dado por los datos sensibles. Por lo tanto, el módulo de sustitución 24 convierte el segundo flujo de datos de sensor T2 en un tercer flujo de datos de sensor T3. Por lo tanto, se consigue la anonimización del primer flujo de datos de sensor T1 al tercer flujo de datos de sensor T3. En otras palabras, el proceso de anonimización del primer flujo de datos de sensor T1 al tercer flujo de datos de sensor T3 se puede hacer en tiempo real de todo el flujo de datos de sensor 13.

[0042] El módulo de análisis 23 y el módulo de sustitución 24 pueden proporcionarse alternativamente como una única unidad, por ejemplo, una única red neuronal que se puede preparar para sustituir directamente cualquiera de los datos sensibles identificados en base al criterio de privacidad predefinido.

[0043] El dispositivo sensor 10 que se puede incorporar en el vehículo 11 forma una parte del vehículo 11, de manera que la anonimización del flujo de datos de sensor 13 a través de la unidad de anonimización 19 se realiza a bordo del vehículo 11.

[0044] El dispositivo sensor 10 puede comprender, además, un módulo de encriptación 29, que puede estar diseñado para encriptar el tercer flujo de datos de sensor T3 antes de almacenar el tercer flujo de datos de sensor T3, por ejemplo, en dicha memoria no volátil, como el disco duro 25 y/o la nube de datos 26. El módulo de encriptación 29 pueden ser un programa de *software* que comprende un algoritmo de encriptación basado en, por ejemplo, un cifrado de datos transparente (TDE) o un cifrado de nivel celular (CLE). En otras palabras, el módulo de encriptación 29 puede recibir el tercer flujo de datos de sensor T3 y procesar el tercer flujo de datos de sensor T3 por medio del algoritmo de encriptación y convertir el tercer flujo de datos de sensor T3 en un cuarto flujo de datos de sensor T4. Este cuarto flujo de datos de sensor T4 tiene forma de un flujo de datos encriptado. El cuarto flujo de datos de sensor T4 se puede almacenar en la memoria no volátil, como un disco duro 25, en el vehículo 11 y/o se puede transmitir de forma inalámbrica a un sistema de supervisión del tráfico, no mostrado en la figura, y/o se puede transmitir de forma inalámbrica a la nube de datos 26. Esto es una ventaja, porque permite una protección del flujo de datos de sensor 13 en caso de robo o daño al vehículo 11. Por lo tanto, el dispositivo sensor 10 permite la anonimización de los datos de sensor en tiempo real a bordo del vehículo 11. Cabe señalar que el primer flujo de datos de sensor T1, el segundo flujo de datos de sensor T2, el tercer flujo de datos de sensor T3 y el cuarto flujo de datos de sensor T4 indican las diferentes formas del flujo de datos de sensor 13.

[0045] En general, el ejemplo muestra cómo se puede lograr la anonimización de datos de sensor antes de que se genere cualquier dato no volátil o reconstruible.

REIVINDICACIONES

- 5 1. Dispositivo sensor (10) que comprende un sensor (12) y una unidad de anonimización (19), donde el sensor (12) está diseñado para generar un flujo de datos de sensor (13) y donde el sensor (12) está acoplado a la unidad de anonimización (19) mediante una ruta de datos (20, 21) que no contiene ninguna memoria digital o solo una memoria volátil (22), donde la unidad de anonimización comprende:
 - 10 – un análisis de módulo (23) para identificar datos sensibles (14, 18) predefinidos en el flujo de datos de sensor (13) en base a un criterio de privacidad predefinido; y
 - un módulo de sustitución (24) para sustituir los datos sensibles (14, 18) en el flujo de datos de sensor (13) con datos de enmascaramiento predefinidos, de manera que los datos de sensor se anonimizan en el flujo de datos de sensor (13) antes de cualquier almacenamiento en una memoria no volátil (25, 26),
- 15 **caracterizado por el hecho de que** el sensor (12) es un sensor LIDAR y/o un sensor de radar.
- 20 2. Dispositivo sensor (10) según la reivindicación 1, que contiene un módulo de encriptación (29), que está diseñado para encriptar al menos una parte del flujo de datos de sensor (13) antes de cualquier almacenamiento en una memoria no volátil (25, 26).
- 25 3. Dispositivo sensor (10) según la reivindicación 1 o 2, donde el módulo de análisis (23) comprende al menos una red neural artificial (28) para analizar el flujo de datos de sensor (13) y/o el módulo de sustitución (24) comprende al menos una red neural artificial (27) para sustituir los datos sensibles (14, 18).
- 30 4. Dispositivo sensor (10) según cualquiera de las reivindicaciones precedentes, donde el flujo de datos de sensor (13) contiene información a partir de una observación del tráfico.
- 35 5. Dispositivo sensor (10) según cualquiera de las reivindicaciones precedentes, donde el criterio de privacidad predefinido proporciona una definición para la información que se debe anonimizar en el flujo de datos de sensor (13) como datos sensibles (14, 18).
6. Dispositivo sensor (10) según la reivindicación 5, donde la información que se debe anonimizar en el flujo de datos de sensor (13) son caras y/o matrículas de vehículos (14) y/o números de casa (18).
7. Dispositivo sensor (10) según cualquiera de las reivindicaciones precedentes, donde la ruta de datos (20, 21) se basa en al menos un cable y/o circuito electrónico y/o una fibra óptica.
- 40 8. Dispositivo sensor (10) según cualquiera de las reivindicaciones precedentes, donde el flujo de datos de sensor (13) comprende datos brutos o datos codificados en MPEG.
9. Dispositivo sensor (10) según cualquiera de las reivindicaciones precedentes, donde el módulo de sustitución (24) está diseñado para generar los datos de enmascaramiento en base a un valor de datos predefinido (píxeles blancos o píxeles negros) y/o mediante el desenfoque de una región de imagen.
- 45 10. Dispositivo de supervisión de imágenes (30) que comprende un dispositivo sensor (10) según cualquiera de las reivindicaciones anteriores.
- 50 11. Método de funcionamiento de un dispositivo sensor (10) según cualquiera de las reivindicaciones anteriores para anonimizar un flujo de datos de sensor (13) que es generado por un sensor (12) del dispositivo sensor (10), que incluye los pasos de:
 - 55 – identificar datos sensibles (14, 18) predefinidos en el flujo de datos de sensor (13) por medio de un criterio de privacidad predefinido a través de un módulo de análisis (23); y
 - sustituir los datos sensibles (14, 18) en el flujo de datos de sensor (13) a través de un módulo de sustitución (24) por datos de enmascaramiento predefinidos, de manera que los datos de sensor se anonimizan en el flujo de datos de sensor (13) antes de cualquier almacenamiento en una memoria no volátil (25, 26),
- 60 **caracterizado por el hecho de que** el sensor es un sensor LIDAR y/o un sensor de radar.
12. Método según la reivindicación 11, donde el dispositivo sensor (10) forma parte de un vehículo (11), de manera que la anonimización de los datos de sensor a través del dispositivo sensor (10) se realiza a bordo del vehículo (11).
- 65 13. Método según la reivindicación 11 o 12, donde el flujo de datos de sensor (13) anonimizado se transmite a un sistema de supervisión del tráfico y/o a una nube de datos (26).

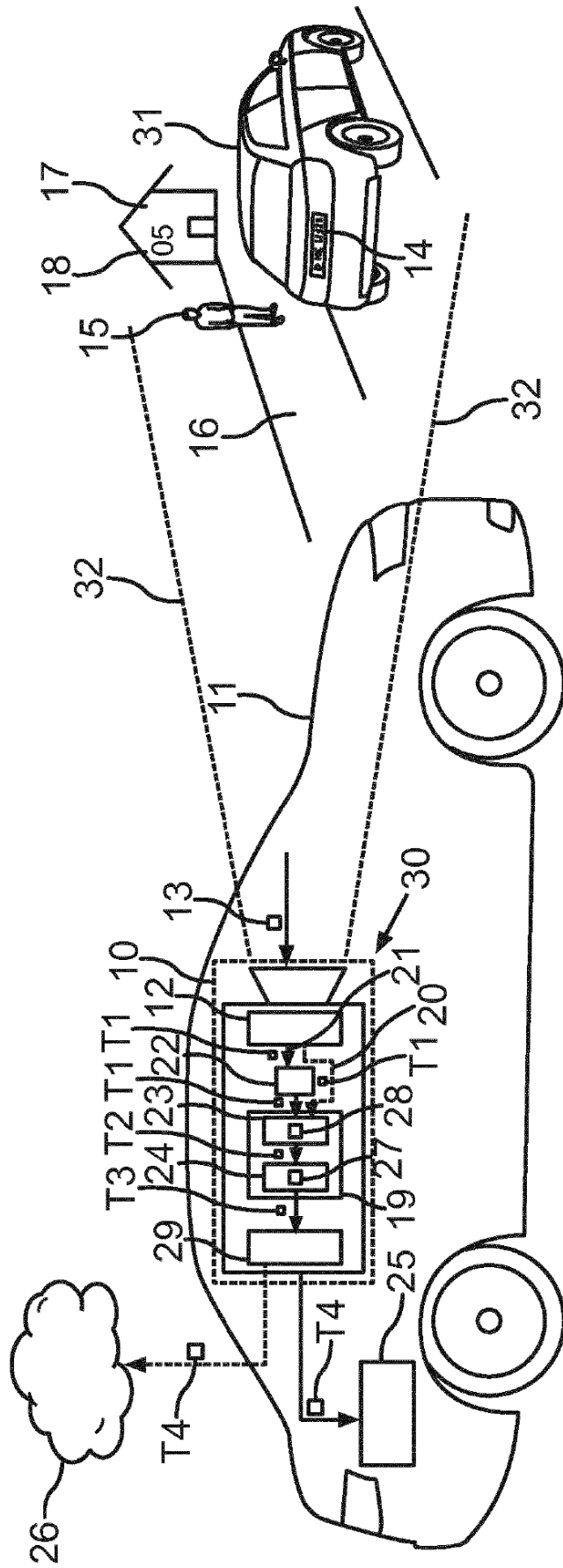


Fig.1

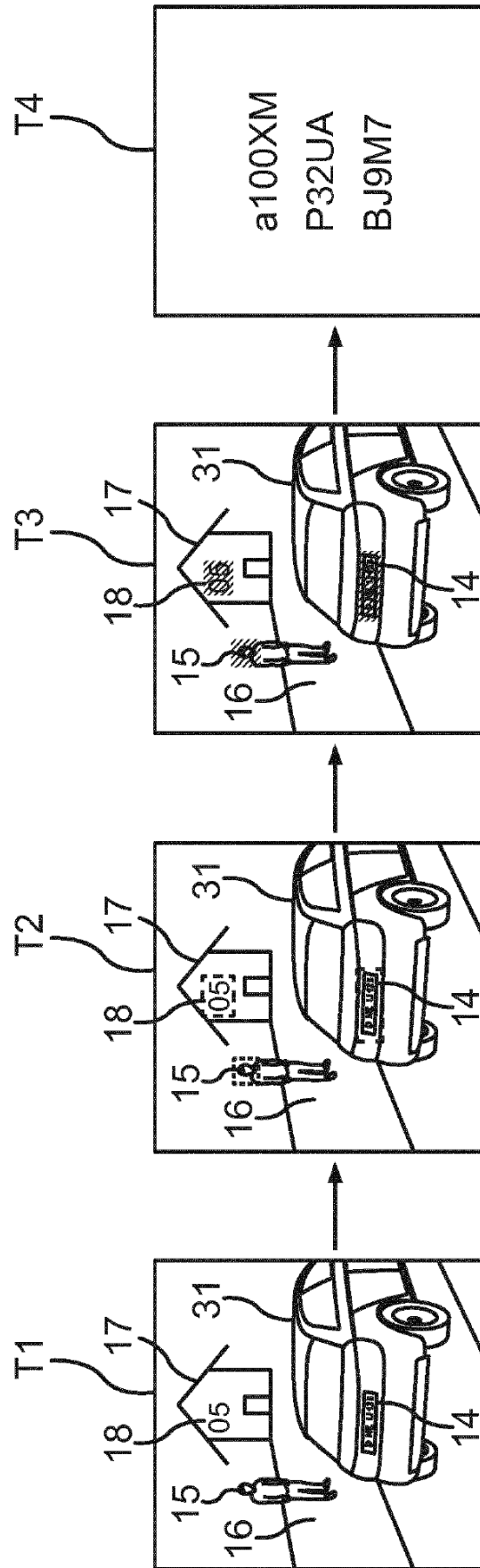


Fig.2