

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 893 808**

51 Int. Cl.:

G07C 9/00

(2010.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **29.12.2015** **E 15202991 (4)**

97 Fecha y número de publicación de la concesión europea: **04.08.2021** **EP 3188134**

54 Título: **Método de control de los derechos de acceso mediante un sistema de control de acceso**

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
10.02.2022

73 Titular/es:

SKIDATA AG (100.0%)
Untersbergstrasse 40
5083 Grödig/Salzburg, AT

72 Inventor/es:

SURKAU, REINHARD;
HEIDER, MICHAEL;
SCHLECHTER, THOMAS;
LANG, CHRISTIAN y
DIAZ, JORGE JUAN CLEMENTE

74 Agente/Representante:

IZQUIERDO BLANCO, María Alicia

ES 2 893 808 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

Método de control de los derechos de acceso mediante un sistema de control de acceso

5 **[0001]** La presente invención se refiere a un método para el control de las autorizaciones de acceso por un sistema de control de acceso según el preámbulo de la reivindicación 1.

10 **[0002]** A partir de la técnica anterior se conocen dispositivos de acceso condicional para las personas, que comprenden medios para detectar preferiblemente sin contacto y evaluar los permisos de acceso, así como las cerraduras mecánicas o diseñadas de otro modo, por ejemplo, en forma de torniquetes o las llamadas puertas abatibles, activando las cerraduras automática o manualmente en la dirección de apertura solo después de que se haya obtenido una autorización de acceso válida.

15 **[0003]** Además, se conocen dispositivos de control de acceso para vehículos que también tienen medios para detectar y evaluar autorizaciones de acceso, así como barreras en forma de barreras para vehículos, que se accionan en la dirección de apertura después de que se dispone de una autorización de acceso válida.

20 **[0004]** De manera desventajosa, el acceso resulta ser inconveniente a través de la cerradura y el bloqueo de la entrada del acceso. En particular, en el caso de los dispositivos de control de acceso para personas, la presencia de las cerraduras se percibe como desagradable. Además, el control de acceso realizado en relación con las cerraduras produce estrés, como resultado de lo cual, por ejemplo, en las áreas de esquí, el disfrute del tiempo libre se ve perjudicado significativamente.

25 **[0005]** Además, este tipo de control de acceso también resulta ineficaz y costoso para los operadores de los medios de transporte o instalaciones de ocio en los que se realiza el control de acceso descrito anteriormente, ya que la mayoría de usuarios suelen disponer de una autorización de acceso válida. De acuerdo con el estado de la técnica, todos los usuarios son controlados para determinar una proporción generalmente muy pequeña de evasores de tarifas o usuarios con autorización de acceso no válida, lo que por un lado implica mucho esfuerzo y, por otro, conduce a retrasos en el acceso.

30 **[0006]** El documento DE 10 2009 000006 A1 da a conocer un método para controlar un objeto en un área de vigilancia conocida, y un dispositivo de identificación portátil es detectado por medio de un primer método que se generan datos de identificación por medio de cámaras, datos de imagen, que se asignan mediante una evaluación de un dispositivo de identificación. En este caso, se evitan los datos de imagen generados con una imagen de referencia, los datos de imagen se generan solo una vez y los datos se verifican sobre la base de este proceso de adquisición único.

40 **[0007]** El documento WO 2011/128408 A1 describe un dispositivo de control de acceso para vigilar y controlar el paso de personas a través de un pasillo o una apertura de la puerta entre una zona exterior y una parte interior que sobresale, comprendiendo un dispositivo de control de acceso de al menos un dispositivo para solicitar una autorización de paso que una persona activa que solicita autorización para atravesar el pasillo o la entrada. El dispositivo de control de acceso conocido comprende además un dispositivo de detección y seguimiento de presencia para detectar la presencia de una persona en las proximidades del pasillo o la abertura de la puerta y para rastrear el movimiento de una persona dentro del pasillo o la abertura de la puerta y una unidad de control con el al menos un dispositivo para solicitar una autorización de paso y el dispositivo de detección y seguimiento de presencia está conectado operativamente, la unidad de control está configurada para, tras la activación del dispositivo para solicitar una autorización de paso, controlar el dispositivo de detección y seguimiento de presencia de modo que, entre un grupo de personas que se encuentra en las inmediaciones del pasillo o se encuentran presentes en la abertura de la puerta, se reconoce y localiza a la persona que ha activado el dispositivo para solicitar una autorización de paso.

50 **[0008]** La presente invención se basa en el objeto de especificar un método para el control de las autorizaciones de acceso por un sistema de control de acceso, a través de cuya aplicación se omite cerradura omitida, y se aumenta la comodidad, sin reducir la calidad del control de las autorizaciones de acceso.

55 **[0009]** Este objeto se resuelve mediante las características de la reivindicación 1.

60 **[0010]** En consecuencia, se propone un método para controlar las autorizaciones de acceso por un sistema de control de acceso cuyos permisos de acceso o identificaciones son almacenados en medios de almacenamiento de datos, o dispositivos electrónicos móviles a los que se asocia una autorización de acceso al menos de manera única, distante en el marco por medios de un local o central, posiblemente geográficamente, los dispositivos de lectura conectados al servidor se detectan y leen sin contacto, con al menos tres dispositivos de lectura en cada área de entrada del sistema de control de acceso, que cubren toda el área de entrada, con varias cámaras conectadas al servidor que se proporciona en cada zona de entrada del sistema de control de acceso, que cubre toda la zona de entrada, por lo que como parte de un primer método mediante la adquisición del soporte de datos o los dispositivos electrónicos móviles en los que se asigna una autorización de acceso o una identificación que indica una autorización de acceso válida, almacenadas por al menos tres dispositivos de lectura por trilateración o multilateración, se determina la posición actual del soporte de datos o de los dispositivos electrónicos móviles, y por medio de un segundo método de imagen,

que se realiza en paralelo al primero método, utilizando las cámaras se registra la posición actual de todas las personas presentes en la zona de entrada del sistema de control de acceso.

[0011] Las áreas de detección de los dispositivos de lectura y las cámaras son idénticas dentro del alcance de las tolerancias habituales.

[0012] El primer método puede ser preferiblemente un método en donde los soportes de datos o dispositivos electrónicos móviles utilizan el estándar Bluetooth Low Energy (BLE) como parte de "radiodifusión" a intervalos regulares para proporcionar una identificación que se asigna de forma única a al menos una autorización de acceso o datos de un envío de autorización de acceso, que es recibida por las unidades transceptoras BLE conectadas a un ordenador que comprende un medio de CPU y de almacenamiento dentro del alcance del dispositivo electrónico móvil o el soporte de datos.

[0013] Esto se realiza para localizar los dispositivos electrónicos móviles o el disco caracterizado porque en base a una intensidad de la señal de referencia, que por lo general corresponde a la intensidad de la señal a un metro y que está contenida como información en la señal del dispositivo electrónico móvil o el soporte de datos o en la dependencia desde el dispositivo electrónico móvil o desde el soporte de datos, por ejemplo del tipo de teléfono móvil, se almacenan en una tabla almacenada en el ordenador, la distancia entre el dispositivo electrónico móvil y el remitente BLE/unidades de recepción está decidida, seguido por la trilateración o si hay más de tres unidades transceptoras BLE, se lleva a cabo una multilateración.

[0014] El uso de estándares BLE de largo alcance para el ahorro de energía puede disponerse fácilmente por dispositivos móviles como teléfonos inteligentes, tabletas o relojes o soportes de datos inteligentes, como, por ejemplo, identificaciones enviadas por tarjetas RFID, cuyos derechos de acceso están claramente asignados, recibándose por unidades transceptoras BLE, sin aumentar significativamente el consumo de electricidad. Después de recibir una identificación de al menos una unidad transceptora BLE, se comprueba si a esta identificación se le asigna una autorización de acceso válida, esta evaluación se lleva a cabo en un ordenador conectado a la unidad transceptora BLE o en un servidor conectado al ordenador. La identificación puede ser, por ejemplo, un número de serie del dispositivo electrónico móvil o del soporte de datos. Cuando los soportes de datos o los dispositivos electrónicos móviles envían los datos de una autorización de acceso, se comprueba la validez de la autorización de acceso.

[0015] Alternativamente, para la aplicación del primer método por medio de los estándares BLE, pueden utilizarse las normas más adecuadas para llevar a cabo el primer método, tales como el estándar UWB (banda ultra ancha) para la comunicación de corto alcance que posibilita una localización del soporte de datos o los dispositivos electrónicos móviles análogos a la norma BLE con alta precisión.

[0016] El segundo método puede, en particular, ser a un método para la identificación de la persona por medio de cámaras 3D, tales como cámaras TOF, a saber, cámaras, que miden distancias por medio de un método de tiempo de tránsito (tiempo de vuelo, TOF), cámaras estéreo, o cámaras de PMD, a saber, las cámaras TOF que comprenden un mezclador fotónico, que permite una detección de la posición exacta de las personas por medio de análisis de imagen.

[0017] De acuerdo con una realización de la invención pueden usarse cámaras trinoculares que comprenden tres cámaras individuales a una diferente distancia entre sí, las cuales están dispuestas en una fila, en donde en cada caso dos de estas cámaras individuales actúan como una cámara estéreo. Ventajosamente, las diferentes combinaciones posibles de las cámaras individuales para formar una cámara estéreo permiten una amplia variación de las posibles longitudes focales del sistema general temporal y por lo tanto un análisis óptimo de la zona de interés (AOL), a saber, la zona de entrada del sistema de control de acceso.

[0018] Esto proporciona una evaluación adecuada, por ejemplo, utilizando la transformación del censo bien conocida en la técnica y la combinación de las imágenes de cada imagen estéreo de una cámara individual que incluye información de profundidad sobre sí mismas en las personas en el área de visualización y los objetos. La evaluación puede tener lugar en la propia cámara o en un equipo asignado a la cámara. Dependiendo del equipo de los componentes de la computadora, la optimización de la resolución parámetros/mono velocidad de fotogramas/frecuencia de imagen estéreo/algoritmo seleccionado/retardo (capacidad de tiempo real) permite diferentes demandas de rendimiento en el sistema, lo que permite una óptima y eficiente adaptación permitida del sistema en el campo de las circunstancias respectivas.

[0019] La información de profundidad obtenida puede utilizarse posteriormente en un siguiente paso para aislar a las personas en el marco y, por lo tanto, para detectar su presencia y, finalmente, llevar a cabo una determinación de la posición. La persona experta en la técnica está familiarizada con numerosos métodos diferentes de la literatura, tales como los métodos basados en el análisis y extracción de texturas en una imagen, los métodos basados en el análisis y la interpolación de movimiento durante varias imágenes sucesivas, y enfoques basados en modelos que en el contexto de reconocimiento de persona o bien se pueden implementar de forma monolítica, es decir, analizar el cuerpo humano como un todo, o basado en parte, es decir, el reconocimiento de las partes individuales del cuerpo humano y ensamblarlos en todo un cuerpo de acuerdo con las hipótesis adecuadas. Este último enfoque es particularmente

adecuado en el caso de que una persona está parcialmente oculta en la imagen.

[0020] De acuerdo con una forma de realización de la invención, en un siguiente paso en una fase de entrenamiento, los contornos típicos de la pieza del objeto examinado son derivados a partir de secuencias de imágenes y son almacenados en una base de datos. Para este propósito, las texturas de la imagen a ser examinada se pueden destacar de antemano, por ejemplo, con filtros anisótropas, que se utilizan típicamente en métodos de análisis de 3-D y son bien conocidos en la literatura. La ventaja del método de reconocimiento de la textura es que, dependiendo de la zona de aplicación, diferentes plantillas se pueden almacenar para optimizar los resultados; por ejemplo, las plantillas que contienen un casco se almacenan para un sistema de control de acceso de una estación de esquí. Esto significa que no es un conjunto óptimo de parámetros de detección para cada aplicación. Al ser las texturas generadas simples, también pueden fácilmente ser sometidas a transformaciones en tiempo real, tales como compresión, rotación o estiramiento. Esto significa que estas texturas también se pueden encontrar en la imagen cuando gira la persona o cambia la distancia entre las personas.

[0021] En un siguiente paso, otro conjunto de información puede generarse a partir de la imagen, obteniéndose por el denominado análisis "contexto de textura aproximada". Aquí, las estructuras 2D pequeñas y menos complejas se extraen de las imágenes. Las estructuras típicas de este tipo que se producen en los cuerpos humanos se almacenan en un libro de códigos. La información sobre la correlación mutua local también se puede almacenar en la imagen entre las estructuras individuales. Estas estructuras individuales se comprueban para su posición una contra la otra utilizando métodos estadísticos adecuados. Si esta comprobación muestra que, debido a la posición de las estructuras la una en relación a la otra y las propiedades individuales de las estructuras en detalle, es plausible que un número de estas estructuras describe una persona humana, este subconjunto se identifica como tal y la correspondiente área de imagen recibe un cuadro delimitador (virtual) para indicar la presencia de una persona humana.

[0022] En una etapa adicional, los enfoques anteriores se pueden combinar mediante el uso de un método de estimación máximo a posteriori, por ejemplo, que es bien conocido para los expertos en esta área. El resultado proporciona un estimador robusto para la posición individual y ubicación (por ejemplo, la postura, la rotación del cuerpo, la rotación de la cabeza, la alineación del brazo) de las personas en la imagen.

[0023] Esta información puede luego convertirse con conocimiento del entorno y la posición de la cámara en coordenadas absolutas x-y-(z) en el entorno real, utilizándose posteriormente como base para la localización, el recuento y el seguimiento (tracking) de las personas por medio del segundo método de formación de imágenes.

[0024] En una forma de realización adicional del método se puede utilizar la infraestructura existente del mismo modo para la detección objetos que no son personas en la imagen, es decir, objetos tales como equipaje, piedras, acumulaciones de nieve. Esto permite que el operador del sistema de control de acceso sea avisado automáticamente de peligros tales como los riesgos de caídas, los riesgos de congestión, la colocación no autorizada de objetos, etc., en la zona de entrada y, posteriormente, para advertir al usuario.

[0025] Debido al concepto de la invención, el soporte de datos o los dispositivos electrónicos móviles en los que se almacenan una autorización de acceso válida o una identificación que está asociado de forma única con autorización de acceso y por lo tanto las personas que llevan al menos una autorización de acceso válida en la forma de un soporte de datos o puede ser un dispositivo electrónico móvil en donde se almacena una autorización de acceso válida o una identificación, a la que se asigna claramente una autorización de acceso, e incluye todas las personas presentes espacialmente en la zona de entrada en tiempo real, de modo que un mapa de identificación y un mapa de personas pueden ser creados.

[0026] El mapa de identificación corresponde a la distribución espacial de las personas, las cuales llevan al menos una autorización de acceso válida en la forma de un soporte de datos o de un dispositivo electrónico móvil en donde se almacena una autorización de acceso válida, o una identificación que se asigna de forma única a una autorización de acceso, con lo que el mapa de personas corresponde a la distribución espacial de todas las personas en la zona de entrada del sistema de control de acceso.

[0027] En un paso siguiente se comparan en el servidor los datos suministrados por los dos procedimientos, para que, en el contexto de una "coincidencia" del mapa de identificación con el mapa de personas, se puede identificar las personas que llevan al menos una autorización de acceso válida en la forma de un disco o un dispositivo electrónico móvil, en donde se almacena una autorización de acceso válida o un documento de identidad, a la que se asigna claramente una autorización de acceso. Aquí se determina si corresponde la posición determinada de una persona registrada por medio del segundo método de formación de imágenes con una posición de un soporte de datos o un dispositivo electrónico móvil determinado mediante el primer método, en donde se almacena una autorización de acceso válida o una identificación que claramente tiene al menos una autorización de acceso válida asignada. Si este no es el caso, se reconoce y localiza una persona que no tiene autorización de acceso o no tiene una autorización de acceso válida.

[0028] Debido a la coincidencia, es decir, la asignación de las autorizaciones de acceso válidas registradas por medio del primer método a las personas registradas por medio del segundo método, se genera un denominado mapa de

superposición que representa la distribución espacial de la asignación y las personas sin asignar y/o autorizaciones de acceso.

[0029] Se llevan a cabo de forma permanente la aplicación paralela de la detección del soporte de datos o los dispositivos electrónicos móviles, en los que se ha dispuesto una autorización de acceso válida, o una identificación que se asigna de forma única a una autorización de acceso y que se almacena por el primer método y las personas presentes por medio del segundo método y la posterior adaptación, por lo que esta información está disponible en tiempo real, y se crea un perfil de movimiento de las personas que son identificadas como personas que no tienen una autorización de acceso válida y de las personas que llevan una autorización de acceso válida en la forma de un soporte de datos o de un dispositivo electrónico móvil, en donde se almacena una autorización de acceso válida o una identificación, a la que se asigna claramente una autorización de acceso.

[0030] Según la invención, se evalúan en tiempo real los perfiles de movimiento en el servidor de acuerdo con el mapa de superposición, en donde, cuando en un sistema de control de acceso que no tiene cerraduras que comprenden dispositivos de control de acceso, personas que, de acuerdo con el mapa de superposición, llevan una autorización de acceso válida en la forma de un soporte de datos o un dispositivo electrónico móvil en donde se almacena una autorización de acceso válida o una identificación, a la que se asigna claramente una autorización de acceso, pasan una línea virtual predeterminada, que corresponde a la de acceso a la zona de vigilancia por el sistema de control de acceso, se crea una entrada correspondiente en un servidor del sistema de control de acceso.

[0031] Si, de acuerdo con el mapa de superposición, personas no identificadas como personas con una autorización de acceso válida sobrepasan la línea virtual predeterminada, en el sistema se detecta un acceso no autorizado. De esta manera, se consigue un sistema de control de acceso sin bloqueos. Además, también se omiten los dispositivos de control de acceso correspondientes.

[0032] En caso de acceso no autorizado por una persona, esta persona puede ser seguida por medio de al menos una cámara adicional, con lo que preferiblemente se realiza un control de acceso manual utilizando la información de seguimiento. Dentro del ámbito de nuevas mejoras, esta persona puede estar marcada por medio de un láser o haz de luz con el fin de que sea más fácil para el personal encontrar a la persona. De acuerdo con una realización adicional, si se detecta el acceso no autorizado, un grupo de personas, incluyendo la persona sin autorización de acceso válida, se puede desviar por medio de activación para las personas de desviación, por ejemplo de puertas de seguridad, siendo el grupo de personas desviado de tal manera que pasan por los medios para controlar las autorizaciones de acceso que comprenden un dispositivo de control de acceso con un bloqueo mecánico, en donde los derechos de acceso se pueden leer sin contacto. Los medios para el desvío de las personas pueden ser activados de forma automática o manualmente mediante un interruptor o un dispositivo mecánico.

[0033] De acuerdo con ello, el sistema de control de acceso comprende al menos tres dispositivos de lectura, colocados en la zona de entrada y conectados a un servidor, que cubren toda la zona de entrada, para la detección y lectura sin contacto de autorizaciones de acceso o identificaciones almacenadas en soportes de datos, o dispositivos electrónicos móviles, en los que se asigna al menos una autorización de acceso, y varias cámaras conectadas al servidor en la zona de entrada del sistema de control de acceso, que cubre toda la zona de entrada. En el caso de que se proporcionan varias zonas de entrada, el sistema de control de acceso comprende al menos dispositivos de lectura y varias cámaras para cada zona de entrada. Con el fin de evitar el acceso no autorizado a través de un área de salida, las áreas de salida son las áreas de entrada en el sentido de la invención.

[0034] En un desarrollo de la invención, en el caso de las autorizaciones de acceso personales que son detectadas por medio del primer método, se puede determinar por medio del segundo método de formación de imágenes si las autorizaciones de acceso se han utilizado indebidamente por otros. Esto se hace mediante la comparación de una foto de la persona autorizada almacenada en una base de datos con una imagen de la persona creada usando el segundo método, la cual lleva una autorización de acceso personal o identificación almacenada en un soporte de datos o un dispositivo electrónico móvil que tiene asignado al menos una autorización de acceso personal. Análogamente a este procedimiento, se puede determinar si un adulto con una autorización de acceso para un niño está usando indebidamente esta autorización de acceso.

[0035] En un desarrollo adicional de la invención, la "correspondencia" del mapa de identificación con el mapa de personas puede optimizarse por medio de un enfoque de máxima verosimilitud (ML) y, opcionalmente, además, por medio de la combinación de un enfoque de máxima verosimilitud (ML) con la lógica difusa (FL).

[0036] Con ello, se generan tarjetas a partir del mapa de personas y del mapa de identificación, que, además de las posiciones de las personas detectadas o de los soportes de datos o dispositivos electrónicos móviles detectados en donde se asigna una autorización de acceso válida o una identificación, incluyen una fiabilidad estadística de estas posiciones. La fiabilidad estadística se puede calcular, por ejemplo, basándose en la experiencia de las desviaciones estándar conocidas y/o errores sistemáticos del método que se pueden derivar del entorno.

[0037] Posteriormente, se traen las dos tarjetas que utilizan un enfoque de máxima verosimilitud de la mejor forma posible en términos de probabilidad estadística como parte de una coincidencia para la cubierta, en donde las

probabilidades de la coincidencia de los resultados de la localización son calculadas de las dos tarjetas, en donde primero se vinculan entre sí los puntos con las probabilidades más altas.

[0038] De acuerdo con un desarrollo del proceso puede haber información adicional sobre la relación de identificaciones individuales o autorizaciones de acceso, por ejemplo, un grupo de identificaciones representa una familia, que se produce preferentemente en común. Otros factores "blandos" de este tipo pueden ayudar a aumentar la precisión del enfoque utilizando la lógica difusa. De manera adecuada, se puede unir entre sí datos diferentes. Por ejemplo, la información de "padre e hijo tienen cada uno identificaciones válidas y están preferiblemente cerca uno del otro" puede ser asignada junto con la información "hay una persona pequeña con una identificación coincidente en la zona de entrada" en probabilidades de asignación, con lo que dichos enlaces en combinación con la coincidencia de acuerdo con el enfoque de máxima verosimilitud posibilitan una coincidencia más fiable del mapa de personas con el mapa de identificación.

[0039] Además, de acuerdo con la invención, para optimizar la coincidencia del mapa de personas con el mapa de identificaciones, se puede utilizar no sólo la posición actual, sino también el desarrollo temporal del mapa de personas y del mapa de identificaciones. Si en el período temporal se mueven las personas registradas y los soportes de datos registrados o dispositivos electrónicos móviles en un patrón comparable, pueden ser unidos entre sí de forma más fiable. El uso de los períodos de tiempo del mapa de personas y el mapa de identificación también puede ser optimizado de acuerdo con el enfoque de máxima verosimilitud a fin de evitar desviaciones estadísticas con el tiempo, por ejemplo sombras en la imagen del método de formación de imágenes y/o vigilancia en la frecuencia del primer procedimiento, para ser capaz de compensar las perturbaciones del entorno inalámbrico por dispositivos de terceros, condiciones ópticas desfavorables relacionadas con el entorno, tales como nevadas, sobre la base de la probabilidad de ocurrencia.

[0040] La invención se ilustra a modo de ejemplo con referencia a la figura adjunta, que ilustra un diagrama de flujo de una posible forma de realización del método.

[0041] Al comienzo del proceso, el sistema en donde se implementa el método está en el modo inactivo (modo de reposo), y, cuando de un aparato para llevar a cabo el segundo método de formación de imágenes, es decir, de una cámara en el intervalo de detección de la cámara, que corresponde a una parte de la zona de entrada del sistema de control de acceso, se detecta un objeto que se clasifica como una persona, que puede realizarse por ejemplo por medio del análisis descrito y la extracción de texturas, se registra la posición actual de la persona y se utiliza un algoritmo para generar el mapa de personas. Estos pasos se repiten hasta que todos los objetos actualmente clasificados como personas que se han detectado en el área de detección de la cámara y su posición actual han sido transferidos al algoritmo para generar el mapa de personas.

[0042] Inmediatamente después de este paso, o, como se ilustra con referencia a la figura adjunta, simultáneamente con la detección de personas a través del método de formación de imágenes por medio de al menos tres medios de lectura que se proporcionan en la entrada del sistema de control de acceso y para cubrir toda el área de entrada, el soporte de datos o los dispositivos electrónicos móviles en donde una autorización de acceso válida o una identificación para que una autorización de acceso se asigna claramente se almacenan, se registran sin contacto (sin cable) y se transfiere su posición actual, determinada por la trilateración o multilateración, a un algoritmo para generar el mapa de personas. Mediante la captura de los soportes de datos o dispositivos electrónicos móviles en los que se almacenan una autorización de acceso válida o una identificación a la que se asigna claramente una autorización de acceso, se registran implícitamente las personas que llevan al menos una autorización de acceso válida en la forma de un soporte de datos o un dispositivo móvil electrónico, en el que está incluida una autorización de acceso válida o una identificación que tiene una autorización de acceso asignada.

[0043] En un siguiente paso en el servidor, se compararon entre sí los datos suministrados por los dos métodos, para identificar las personas que llevan una autorización de acceso válida en la forma de un soporte de datos o un dispositivo electrónico móvil en donde se almacena una autorización de acceso válida o una identificación, a la que se asigna claramente una autorización de acceso, como parte de una "coincidencia" del mapa de identificación con el mapa de personas. Aquí se determina si corresponde la posición determinada de una persona registrada por medio del segundo método de formación de imágenes es una posición de un soporte de datos o un dispositivo electrónico móvil determinado mediante el primer método, en donde una autorización de acceso válida o una identificación que claramente tiene por lo menos una autorización de acceso válida asignada. Si esto no es el caso, se reconoce y se localiza una persona que no tiene una autorización de acceso o no tiene una autorización de acceso válida.

[0044] Debido a la coincidencia, es decir, la asignación de la autorización de acceso válida registrada por medio del primer método a las personas registradas mediante el segundo método, se genera un mapa de superposición que representa en tiempo real la distribución espacial de la asignación y de las personas y/o autorizaciones de acceso sin asignar.

[0045] La realización paralela de la detección del soporte de datos o los dispositivos electrónicos móviles a los que una autorización de acceso válida, o una identificación, en la que se almacena de forma única una autorización de acceso por el primer método y las personas presentes por medio del segundo método y la posterior coincidencia se

llevan a cabo de forma permanente para que esta información esté disponible en tiempo real y se genera un perfil de movimiento de las personas que han sido identificadas como personas sin autorización de acceso válida y aquellas que tienen autorización de acceso válida.

5 **[0046]** En el servidor, se evalúan los perfiles de movimiento de acuerdo con el mapa de superposición en tiempo real, con lo que, cuando en un sistema de control de acceso que no tiene dispositivos de control de acceso que incluyan
 10 cerraduras, personas que, según el mapa de superposición, tienen una autorización de acceso válida en la forma de un soporte de datos o un dispositivo electrónico móvil en donde una autorización de acceso válida o una identificación con una autorización de acceso asignada, sobrepasan una línea virtual predeterminada, la cual corresponde al acceso a la zona supervisada por el sistema de control de acceso, de acuerdo con un procedimiento de acceso, que se activa
 cuando, de acuerdo con el mapa de superposición, las personas con autorización de acceso válida están cerca de la zona de acceso, es decir, la línea virtual, una entrada correspondiente para esta autorización de acceso se crea en
 15 una servidor del sistema de control de acceso. Después pasarse la línea virtual, el procedimiento de acceso para esta autorización de acceso es bloqueado por un período de tiempo predefinido, de modo que si se pasa a través de la línea virtual de nuevo con esta autorización de acceso se clasifica como uso indebido.

[0047] Si, de acuerdo con el mapa de superposición, sucede que personas identificadas como personas sin una
 autorización de acceso válida sobrepasan la línea virtual predeterminada, se detecta en el sistema una entrada no
 20 autorizada. De esta manera, se consigue un sistema de control de acceso sin bloqueos. Los datos se transmiten a un algoritmo adicional externo para el análisis de uso indebido.

REIVINDICACIONES

1. Un método para controlar los derechos de acceso por medio de un sistema de control de acceso, en donde los derechos de acceso o identificación, a los que se asigna de manera única al menos un derecho de acceso, que se almacenan en soportes de datos o dispositivos electrónicos móviles, se detectan y leen sin contacto por medio de dispositivos de lectura que están conectados a un servidor, donde al menos tres dispositivos de lectura están provistos en cada área de entrada del sistema de control de acceso, dispositivos de lectura que cubren toda la zona de entrada, en donde una pluralidad de cámaras que están conectadas al servidor en cada zona de entrada del sistema de control de acceso, cuyas cámaras cubren toda la zona de entrada, en donde, en el contexto de un primer método, se detecta la posición actual de los soportes de datos o dispositivos electrónicos móviles mediante la detección de los soportes de datos o los dispositivos electrónicos móviles, en los que se almacena un derecho de acceso válido o una identificación, a la que se asigna un derecho de acceso válido, mediante al menos tres dispositivos de lectura por trilateración o multilateración, y donde, mediante un segundo método de imagen que se realiza en paralelo con el primer método, se detecta la posición actual de todas las personas presentes en la zona de entrada del sistema de control de accesos por medio de las cámaras, como resultado de lo cual las personas que llevan consigo al menos un derecho de acceso en forma de soporte de datos o un dispositivo electrónico móvil, sobre el cual un derecho de acceso válido o una identificación, al cual un acceso derecho se asigna de forma única, se almacena y todas las personas presentes en el área de entrada se detectan espacialmente en tiempo real, de modo que se crea un mapa de identificación y un mapa de personas en el servidor, donde el mapa de identificación corresponde a la distribución espacial de las personas que llevan consigo al menos un derecho de acceso válido en forma de soporte de datos o dispositivo electrónico móvil, en donde se almacena un derecho de acceso válido o una identificación, al que se asigna un derecho de acceso de forma exclusiva, y el mapa de personas corresponde a la distribución espacial de todas las personas en el área de entrada del sistema de control de acceso, donde los datos entregados por los dos métodos se comparan entre sí en el servidor, para crear un mapa superpuesto en el contexto de una "coincidencia" del mapa de identificación con el mapa de personas, en donde se superponen las personas que llevan consigo al menos un derecho de acceso válido en forma de soporte de datos o un dispositivo electrónico móvil, en donde un derecho de acceso válido o se almacena una identificación, a la que se asigna un derecho de acceso de manera única, y se identifica a las personas sin un derecho de acceso válido, en donde se determina si la posición determinada de una persona detectada mediante el segundo método de imagen corresponde a una posición, determinado por medio del primer método, de un soporte de datos o un dispositivo electrónico móvil, en donde se almacena un derecho de acceso válido o una identificación, al que se asigna de manera única al menos un derecho de acceso válido, en donde, si este no es el caso, una persona es detectada y localizada, que no tiene un derecho de acceso válido, en donde los perfiles de movimiento se evalúan según el mapa superpuesto en tiempo real, en donde, si las personas, que llevan consigo un derecho de acceso válido según el mapa superpuesto, pasan una línea virtual predeterminada, que corresponde al acceso a la zona monitoreada por el sistema de control de acceso, se crea una entrada correspondiente en un servidor del sistema de control de acceso, y en donde si las personas, que se identifican como personas sin un derecho de acceso válido de acuerdo con el mapa de superposición, pasa la línea virtual predeterminada, se detecta un acceso no autorizado, como resultado de lo cual se realiza un sistema de control de acceso sin barreras.

2. El método para controlar los derechos de acceso mediante un sistema de control de acceso según la reivindicación 1, en donde, para el caso de un acceso no autorizado, el seguimiento de la persona sin un derecho de acceso válido se realiza mediante al menos una cámara adicional, donde se realiza un control de acceso manual en base a la información de seguimiento o si se detecta un acceso no autorizado de una persona, se realiza un desvío de un grupo de personas que contiene a la persona sin derecho de acceso válido mediante la activación de medios de desvío de personas, donde el grupo de personas se desvía de tal manera que se pasan los medios de control de los derechos de acceso, que comprenden un dispositivo de control de acceso con barrera mecánica, donde los derechos de acceso se pueden leer sin contacto.

3. El método para controlar los derechos de acceso mediante un sistema de control de acceso según la reivindicación 1 o 2, en donde para el caso de los derechos de acceso personal que se detectan mediante el primer método, se determina mediante el segundo método de imagen, si estos derechos de acceso están siendo abusados sin autorización por parte de otras personas, lo cual se realiza mediante la comparación de una foto de la persona autorizada, que se almacena en una base de datos, con una imagen, creada mediante el segundo método, de la persona que lleva consigo el derecho de acceso personal o DNI, al que se le asigna de forma exclusiva al menos un derecho de acceso personal válido, que se almacena en un soporte de datos o en un dispositivo electrónico móvil.

4. El método para controlar los derechos de acceso mediante un sistema de control de acceso según la reivindicación 1 o 2, en donde la "correspondencia" del mapa de identificación con el mapa de personas se optimiza mediante una combinación de aproximaciones de máxima verosimilitud (ML) y lógica difusa (FL), donde se generan mapas a partir del mapa de personas y el mapa de identificación, que, además de las posiciones de las personas detectadas o de los portadores de datos detectados o de los dispositivos electrónicos móviles detectados, sobre los cuales un derecho de acceso válido o una identificación, a los que se les asigna un derecho de acceso de forma única, se almacenan, contienen una fiabilidad estadística de estas posiciones derivadas de las mismas, donde el mapa de identificación y el mapa de personas se ponen en congruencia mediante un enfoque de máxima verosimilitud de la mejor manera posible en términos de probabilidad estadística en el contexto de emparejamiento, en donde se calculan las probabilidades de emparejamiento de los resultados de localización de ambos mapas, y en donde los puntos con las

probabilidades mutuas más altas están vinculados entre sí.

5. El método para controlar los derechos de acceso mediante un sistema de control de acceso según la reivindicación 4, en donde el curso temporal del mapa de personas y el mapa de identificación se utilizan para optimizar la coincidencia del mapa de personas con el mapa de identificación, en donde, si las personas detectadas y los soportes de datos o los dispositivos electrónicos móviles detectados en el curso temporal se mueven en un patrón comparable, estos se vinculan de manera más confiable entre sí.

6. El método para controlar los derechos de acceso mediante un sistema de control de acceso según una de las reivindicaciones anteriores, donde el primer método es un método, en el contexto del cual los soportes de datos o dispositivos electrónicos móviles transmiten una identificación, a la que al menos se asigna un derecho de acceso de forma única, o datos de un derecho de acceso a través del estándar de baja energía de Bluetooth (BLE) en el contexto de "transmisión" a intervalos regulares, que son recibidos por unidades transceptoras BLE en el alcance del dispositivo electrónico móvil o los portadores de datos, cuyas unidades transceptoras están conectadas a un ordenador que comprende una CPU y medios de almacenamiento, en donde la localización de los dispositivos electrónicos móviles o de los portadores de datos se realiza en base a una intensidad de la señal de referencia, que generalmente corresponde a la intensidad de la señal a una distancia de un metro y que está contenida como información en la señal del dispositivo electrónico móvil o el soporte de datos o se almacena en una tabla guardada en la computadora como una función del dispositivo electrónico móvil o del soporte de datos, se determina la distancia entre el dispositivo electrónico móvil y las unidades transceptoras BLE, realizándose posteriormente una trilateración, o en el caso de más de tres unidades transceptoras BLE, una multilateración.

7. El método para controlar los derechos de acceso por medio de un sistema de control de acceso según una de las reivindicaciones 1-5 precedentes, donde el segundo método de imagen es un método para el reconocimiento de personas por medio de cámaras 3D, cámaras estéreo o cámaras PMD, que permite una detección precisa de la posición de las personas mediante análisis de imágenes.

8. El método para controlar los derechos de acceso mediante un sistema de control de acceso según una de las reivindicaciones 1-5 anteriores, en donde se utilizan cámaras trinoculares para realizar el segundo método de imagen, que en cada caso comprende tres cámaras individuales a una distancia diferente entre sí, que están dispuestas en fila, donde en cada caso, dos de estas cámaras individuales actúan como una cámara estéreo, donde las diferentes posibilidades de combinación de las cámaras individuales para formar una cámara estéreo permiten una amplia variación de las posibles distancias focales y así un análisis óptimo de la zona de entrada del sistema de control de accesos.

