(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 979 285**

(51) Int. Cl.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.03.2018 PCT/EP2018/057972**

(87) Fecha y número de publicación internacional: **18.10.2018 WO18188957**

(96) Fecha de presentación y número de la solicitud europea: **28.03.2018 E 18712915 (0)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2024 EP 3610466**

(54) Título: **Procedimiento de registro y control de entrada de visitantes**

(30) Prioridad:

10.04.2017 EP 17165817

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.09.2024

(73) Titular/es:

INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil, CH

(72) Inventor/es:

FRIEDLI, PAUL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de registro y control de entrada de visitantes

La presente invención se refiere a un procedimiento para operar un sistema de control de acceso para controlar un acceso a una zona de acceso restringido en un edificio o terreno, en el que el procedimiento comprende un procedimiento de registro para un visitante. La invención se define en las reivindicaciones 1 a 14.

La tecnología aquí descrita se refiere en general a un sistema de control de acceso que permite a un usuario autorizado acceder a una zona de acceso restringido en un edificio o recinto. Los ejemplos de realización de la tecnología se refieren, en particular, a un sistema de control de acceso para visitantes y a un procedimiento para operar dicho sistema de control de acceso.

Los sistemas de control de acceso pueden estar configurados de las más diversas maneras. Por ejemplo, el documento US 9.077.716 describe un sistema de control de acceso en el que un dispositivo electrónico móvil se comunica con una cerradura electrónica de puerta mediante una conexión inalámbrica Bluetooth o WLAN y con un servidor web mediante una conexión inalámbrica WAN (Wide Area Network) para abrir la cerradura electrónica. Para ello, el dispositivo electrónico móvil envía su identificador de dispositivo y un identificador de la cerradura electrónica introducido por un usuario al servidor web, que comprueba la autorización de acceso y envía al dispositivo móvil una respuesta compuesta por un comando de cerradura, el identificador de cerradura y un patrón de código. El dispositivo móvil envía el comando de cerradura y el patrón de código a la cerradura electrónica. Si la cerradura reconoce el comando de cerradura y el patrón de código como válidos, esta se abre.

El documento US 2016/0308859 revela un sistema de control de acceso con un dispositivo de control de acceso montado en una pared, que ofrece múltiples opciones para la autenticación de un usuario, incluido el reconocimiento facial. El usuario puede ser registrado por un administrador que introduce datos personales y derechos de acceso en el sistema de control de acceso.

El documento US2015221151 A1 describe un sistema de seguridad que determina y evalúa varios factores para la identificación de una persona. El sistema de seguridad tiene un sistema de validación para confirmar positivamente la identidad y ubicación física de una persona. El sistema de validación tiene un sensor de ubicación para detectar ubicaciones de dispositivos móviles, una cámara para monitorizar una zona, una memoria de datos faciales y un dispositivo de procesamiento. El dispositivo de procesamiento solicita desde la memoria de datos de reconocimiento facial un registro de datos faciales asociado a un usuario conectado a un dispositivo móvil detectado y compara ese registro de datos faciales con imágenes de imágenes faciales tomadas por la cámara. En el caso de una coincidencia, se concederá el acceso.

El documento WO 2010/112586 A1 describe un sistema de control de acceso en el que un teléfono móvil transportado por un usuario envía un código de identificación a un nodo de acceso. Si el código de identificación se detecta como válido, el nodo de acceso envía un código de acceso al teléfono móvil que muestra el nodo de acceso en una pantalla. Si el usuario sujeta el teléfono móvil junto a una cámara para que ésta pueda detectar el código de acceso representado, el sistema de control de acceso comprobará si el código de acceso detectado es válido. Si es válido, se concede el acceso al usuario.

Estos sistemas de control de acceso ofrecen una cierta facilidad de uso, ya que los usuarios no llevan consigo tarjetas de autorización o llaves convencionales y no tienen que recordar un código de acceso. En cambio, el dispositivo electrónico móvil, que muchos usuarios ya llevan con ellos para fines de comunicación, ofrece la función de una tarjeta de autorización o llave. A pesar del uso de dispositivos móviles, estos sistemas de control de acceso requieren que los usuarios manejen los dispositivos móviles. Por lo tanto, existe la necesidad de una tecnología diferente, aún más fácil de usar.

Un aspecto de dicha tecnología se refiere a un procedimiento para operar un sistema de control de acceso para controlar el acceso a una zona de acceso restringido en un edificio o terreno, en el que el procedimiento comprende un procedimiento de registro para el visitante. El sistema de control de acceso comprende un dispositivo de emisión y de recepción para la comunicación con un dispositivo electrónico móvil de un visitante mediante una conexión por radio, un dispositivo de almacenamiento, un procesador y un dispositivo de procesamiento de imágenes. Según el procedimiento de registro, los datos de invitación generados y enviados por un sistema de anfitrión electrónico se reciben a través del sistema de control de acceso, en el que los datos de invitación comprenden un número de identificación de una invitación y se refieren a una fecha en la que un anfitrión espera a un visitante en la zona de acceso restringido. Un perfil de visitante asociado a la invitación se crea en el dispositivo de almacenamiento y los datos de la invitación se almacenan en el perfil de visitante, en el que el dispositivo de almacenamiento contiene una base de datos proporcionada para almacenar perfiles de usuario de usuarios y visitantes autorizados. A través del sistema de control de acceso se reciben datos de imagen del visitante, el número de identificación de la invitación y un identificador específico del dispositivo, del dispositivo electrónico del visitante. Los datos de imagen y el identificador se almacenan en el dispositivo de almacenamiento, en el que los datos de imagen y el identificador se asocian al perfil del visitante mediante el número de identificación de la invitación. Los datos de imagen son procesados por el sistema de control de acceso para generar una plantilla de referencia, en la que la plantilla de referencia se almacena en el

perfil del visitante.

Otro aspecto se refiere a un sistema de control de acceso para el control de un acceso a una zona de acceso restringido en un edificio o un terreno, en el que el sistema de control de acceso comprende un dispositivo de emisión y de recepción, un dispositivo de almacenamiento, un procesador y un dispositivo de procesamiento de imágenes. Durante el funcionamiento, el procesador controla una recepción de datos de invitación generados y enviados por un sistema de anfitrión electrónico a través del sistema de control de acceso, en el que los datos de invitación comprenden un número de identificación de una invitación y se refieren a una fecha en la que un anfitrión espera un visitante en la zona de acceso restringido. El procesador también controla la creación de un perfil de visitante asociado a la invitación en el dispositivo de almacenamiento, y el almacenamiento de los datos de invitación en el perfil de visitante. El dispositivo de almacenamiento contiene una base de datos que está proporcionada para almacenar perfiles de usuario de usuarios y visitantes autorizados. Además, el procesador controla una recepción a través del sistema de control de acceso de los datos de imagen del visitante, el número de identificación de la invitación y un identificador específico del dispositivo del visitante. El procesador también controla un almacenamiento de los datos de imagen y el identificador en el dispositivo de almacenamiento, en el que los datos de imagen y el identificador se asocian al perfil de visitante por medio del número de identificación de la invitación, un procesamiento de los datos de imagen mediante el dispositivo de procesamiento de imágenes para generar una plantilla de referencia; y un almacenamiento de la plantilla de referencia en el perfil de visitante.

La tecnología aquí descrita permite un registro de un visitante, de manera que al visitante se le pueda conceder acceso a una zona de acceso restringido a través del sistema de control de acceso de la misma manera que un usuario que vive o trabaja en el edificio. Por lo tanto, no hay que tomar precauciones especiales para los visitantes en el edificio, por ejemplo, no se requieren personas o solo se requieren pocas personas para recibir a los visitantes.

En un ejemplo de realización, la validez de un registro del visitante está limitada en el tiempo, por ejemplo, durante la duración de una visita. A continuación, el registro se puede desactivar o eliminar. En otro ejemplo de realización, el registro puede ser ilimitado en el tiempo, por ejemplo, si el visitante desea acceder varias veces a la zona de acceso restringido durante un período de tiempo más largo. Un registro desactivado se puede reactivar en un momento posterior para una nueva visita del visitante con datos de invitación actualizados. Eventualmente, puede omitirse el envío de una imagen.

En el sistema de control de acceso puede establecerse una ventana de tiempo para una invitación que defina un periodo de tiempo antes y/o después de un horario especificado en la fecha, dentro del cual debe concederse el acceso al visitante. Esta ventana de tiempo se puede comunicar al visitante en la invitación. Esto reduce el riesgo de posibles confusiones que pueden surgir si el visitante llega tarde o demasiado pronto.

La tecnología aquí descrita ofrece flexibilidad en cuanto a cómo se reciben los datos de imagen, el número de identificación de la invitación y el identificador del sistema de control de acceso. En un ejemplo de realización, estos datos se reciben a través de un canal de comunicación, que se indica en la invitación generada por el sistema anfitrión. En un ejemplo de realización, como canal de comunicación se indica una dirección de Internet de un portal web. En otro ejemplo de realización, como canal de comunicación se indica una dirección de correo electrónico o un número de teléfono de una administración del edificio.

Una vez finalizado el registro del visitante, se podrá realizar un procedimiento de control de acceso si el visitante desea acceder según la invitación. El procedimiento de control de acceso comprende la recepción de un identificador específico del dispositivo enviado por el dispositivo electrónico móvil del visitante o de otro visitante a través del dispositivo de emisión y de recepción, cuando el dispositivo electrónico móvil se encuentra en una zona pública dentro del alcance de radio del dispositivo de emisión y de recepción. El identificador recibido del dispositivo electrónico móvil se almacena en el dispositivo de almacenamiento como perteneciente a un usuario o visitante presente. El procedimiento también comprende la creación de una plantilla en tiempo real para las características faciales del usuario o visitante presente a partir de una imagen de la cámara del usuario presente generada por una cámara del dispositivo de procesamiento de imágenes, si el usuario o visitante presente desea acceder a la zona de acceso restringido. Mediante el identificador almacenado del dispositivo electrónico móvil se determina si el identificador recibido del dispositivo electrónico móvil está asociado a una plantilla de referencia en la base de datos. Si existe una asociación de este tipo, el dispositivo de procesamiento de imágenes comprueba si la plantilla en tiempo real coincide con esa plantilla de referencia en un grado determinado. En el caso de una coincidencia, el sistema concede al usuario o visitante acceso a la zona de acceso restringido y en el caso de no coincidencia, el sistema niega el acceso.

En el procedimiento de control de acceso aquí descrito, no es necesario que el usuario manipule el dispositivo electrónico móvil, especialmente si el usuario ya está junto al acceso o cerca del mismo (por ejemplo, una puerta). Una primera fase de la verificación de si el usuario está autorizado para el acceso se realiza ya cuando el usuario todavía está relativamente lejos del acceso. El usuario, por ejemplo, puede moverse en la dirección del acceso a la zona de acceso restringido, mientras que en un ejemplo de realización el dispositivo electrónico móvil del usuario ya está o ya estaba en comunicación con el dispositivo de emisión y de recepción del sistema de control de acceso. El dispositivo de emisión y de recepción recibe el identificador del dispositivo electrónico móvil, que, si el usuario está registrado como autorizado para acceder, está asociado a un perfil de usuario almacenado. Si el usuario entra en una zona de detección de una cámara del sistema de control de acceso, en una segunda fase se determinan las

características faciales del usuario a partir de un registro digital de la cámara. Si las características faciales detectadas coinciden con las características faciales almacenadas en el perfil de usuario en un grado determinado, el usuario está autorizado al acceso y se le concede el acceso sin tener que manipular el dispositivo electrónico móvil. Por lo tanto, un usuario autorizado puede acceder casi de forma continua a la zona de acceso restringido.

Se puede autorizar el acceso a una zona de acceso restringido en un edificio o área a un gran número de usuarios (por ejemplo, varios cientos o miles); según este número, se crean perfiles de usuario. Sin embargo, la tecnología aquí descrita ofrece la ventaja de que la comprobación de la coincidencia se realiza rápidamente, porque no todos los perfiles de usuario de los usuarios autorizados para el acceso deben comprobarse para la coincidencia, sino solo los perfiles de usuario de los usuarios realmente presentes. Por lo tanto, un usuario presente puede acceder a la zona de acceso restringido sin una detención o un retraso significativos. Esto reduce el riesgo de que se forme una cola de espera antes del acceso, especialmente en caso de tráfico intenso.

La tecnología no solo ofrece una verificación más rápida, sino que también se puede utilizar con altos requisitos de seguridad, ya que, por ejemplo, se realiza una doble autenticación. Por un lado, se utilizan dos canales diferentes: Radio para la transmisión de un identificador y la detección óptica de un rostro de un usuario. El identificador debe pertenecer a un usuario registrado en el sistema y la evaluación de los parámetros faciales debe indicar un usuario registrado. Por otro lado, se deben buscar o verificar menos perfiles de usuario, lo que reduce la frecuencia de errores (es decir, se niega erróneamente el acceso a un usuario autorizado o se concede erróneamente el acceso a un usuario que no está autorizado).

Dependiendo del volumen de tráfico, en la zona pública puede encontrarse una pluralidad de dispositivos electrónicos móviles. En tal situación, el dispositivo de emisión y de recepción recibe una pluralidad de identificadores que se almacenan en el dispositivo de almacenamiento, y para cada identificador almacenado se determina si el identificador recibido está asociado a una plantilla de referencia en la base de datos. Si existen asociaciones de esa clase, se comprueba si la plantilla en tiempo real coincide con una de estas plantillas de referencia; en caso de coincidencia, el sistema concede al usuario acceso a la zona de acceso restringido y, en caso de no coincidencia, le niega el acceso. Por lo tanto, la ventaja mencionada de la verificación rápida está garantizada incluso con un alto volumen de tráfico, ya que la verificación está limitada a la coincidencia con una cantidad limitada de perfiles de usuario.

En la tecnología aquí descrita, por un lado, la verificación de la coincidencia está limitada a una cantidad limitada de perfiles de usuario. Por otro lado, esta cantidad limitada solo comprende a los usuarios autorizados, ya que solo en el caso de un usuario autorizado, el identificador del dispositivo móvil está asociado a un perfil de usuario almacenado. Para el dispositivo de procesamiento de imágenes, esto significa que se imponen requisitos relativamente bajos a un algoritmo de procesamiento de imágenes implementado en el mismo, por ejemplo con respecto a la precisión de reconocimiento. En comparación con un algoritmo de procesamiento de imágenes, cuya tarea es identificar a una persona en base a un número relativamente grande de características faciales con una alta precisión de reconocimiento (es decir, el grado de coincidencia debe ser relativamente alto, por ejemplo, mayor que aproximadamente el 90 %), con la tecnología descrita aquí es suficiente con asociar relativamente pocas características faciales a uno de los usuarios autorizados. Además, el grado de coincidencia se puede establecer, por ejemplo, entre aproximadamente el 60 % y aproximadamente el 90 %. Por lo tanto, se puede utilizar un algoritmo de procesamiento de imágenes económico; sin embargo, se pueden garantizar los requisitos de seguridad.

En un ejemplo de realización, la comprobación de la coincidencia comprende una generación de una señal de resultado. En caso de una coincidencia, esto indica que el usuario tiene acceso a la zona de acceso restringido, mientras que en caso de no coincidencia, indica que el usuario no tiene acceso a la zona de acceso restringido. Como función de la señal de resultado, en un ejemplo de realización se puede generar una señal de control para liberar o bloquear una barrera (física) (por ejemplo, una barrera, una puerta o un molinete). En otro ejemplo de realización, la señal de control activa un dispositivo de información en caso de negarse el acceso. El dispositivo de información se puede utilizar, por ejemplo, en combinación con un acceso sin una barrera física. Si se detecta un usuario no autorizado en el acceso, en un caso el dispositivo de información puede generar una alarma que perceptible en el acceso (acústica y/o visualmente). En otro caso, la señal de control puede alertar a un servicio de seguridad, que controla al usuario reconocido como no autorizado.

En un ejemplo de realización, la conexión por radio entre el dispositivo de emisión y de recepción y un dispositivo electrónico móvil de un usuario se realiza según un estándar Bluetooth. Esto es ventajoso porque los teléfonos móviles o teléfonos inteligentes disponibles en el mercado ya están equipados con tecnología Bluetooth y, por lo tanto, no se necesitan dispositivos especiales.

La tecnología aquí descrita también permite flexibilidad con respecto al identificador de un dispositivo móvil. El identificador de un dispositivo móvil puede comprender, por ejemplo, un número de identificación de dispositivo asociado de forma fija al dispositivo o un número de teléfono asociado al dispositivo móvil. En un ejemplo de realización, cada dispositivo móvil está equipado con un software específico de la aplicación que genera un identificador único e invariable en el tiempo para el dispositivo móvil. El identificador (independientemente de que incluya un número de identificación del dispositivo, un número de teléfono o sea generado por software) permite la identificación única de un dispositivo móvil.

En un ejemplo de realización, el dispositivo de procesamiento de imágenes está estructurado de forma modular; un módulo de procesamiento de imágenes, a partir de una imagen digital, genera la plantilla en tiempo real, y un módulo de evaluación, que está conectado con el módulo de procesamiento de imágenes y el dispositivo de almacenamiento, genera una señal de resultado, que indica si la plantilla en tiempo real coincide con esa plantilla de referencia. Esta modularidad permite una adaptación eficiente de los módulos a diferentes requisitos (por ejemplo, la implementación de un algoritmo de procesamiento de imágenes económico en el módulo de evaluación).

En el caso de la tecnología aquí descrita, es una ventaja que su aplicación no se limite a la forma en que está configurado el acceso a la zona de acceso restringido. El acceso puede incluir una barrera física, por ejemplo una barrera, una puerta, una puerta giratoria o un molinete, que se desbloquea o se bloquea. Alternativamente, el acceso puede estar diseñado sin una barrera física de esa clase (es decir, como un acceso esencialmente sin barreras). Si se detecta un usuario no autorizado en el acceso (con o sin barrera física) con la ayuda de la tecnología aquí descrita, se puede generar una alarma y/o se puede alertar a un servicio de seguridad.

En un ejemplo de realización, la tecnología aquí descrita se puede utilizar en combinación con un sistema de ascensor. Para cada usuario autorizado se puede establecer, por ejemplo, una planta de destino en la que se encuentra, por ejemplo, su lugar de trabajo o su domicilio. Con cada concesión de acceso, se puede generar una llamada de destino para el usuario en cuestión, tras lo cual un control de ascensor del sistema de ascensor desplaza una cabina de ascensor primero a un piso de entrada y, a continuación, a un piso de destino. De este modo, se mejora la facilidad de uso, ya que el usuario puede dirigirse directamente a una cabina de ascensor asignada sin tener que introducir una llamada de ascensor.

A continuación se explican con más detalle distintos aspectos de la tecnología mejorada mediante ejemplos de realización, en relación con las figuras. En las figuras, los mismos elementos tienen los mismos símbolos de referencia. Muestran:

Fig. 1 una representación esquemática de un ejemplo de aplicación de un sistema de control de acceso en combinación con un edificio;

Fig. 2 una representación esquemática de un ejemplo de realización de un sistema de control de acceso;

Fig. 3 un diagrama de operaciones de un ejemplo de realización de un procedimiento de control de acceso como un aspecto de un procedimiento para operar el sistema de control de acceso; y

Fig. 4 un diagrama de señal ilustrativo para la representación de un ejemplo de realización de un procedimiento de registro de visitantes como un aspecto de un procedimiento para operar el sistema de control de acceso.

La fig. 1 es una representación esquemática de un ejemplo de aplicación de un sistema de control de acceso 1 en combinación con una situación en un edificio del que solo se muestran algunas paredes, habitaciones 4 y zonas 8, 10 por razones de representación. Las habitaciones 4 pueden ser, por ejemplo, oficinas, apartamentos, naves y/o cabinas de ascensor de un sistema de ascensor. En la aplicación del sistema de control de acceso 1 mostrado en la fig. 1 se encuentran en la zona 10 varios usuarios 2, que llevan consigo dispositivos electrónicos móviles 6 (en lo sucesivo también denominados dispositivo móvil 6). En este ejemplo, la zona 10 no está sujeta a ninguna restricción de acceso y en lo sucesivo también se denomina como zona pública 10. La zona pública 10 puede ser un área dentro o fuera del edificio. Un acceso 12 separa la zona pública 10 de la zona 8, que está sujeta a una restricción de acceso y es adyacente a las habitaciones 4. El experto reconoce que el sistema de control de acceso 1 no está limitado a aplicaciones dentro de un edificio, sino que también se puede utilizar de forma análoga para controlar el acceso a una zona de acceso restringido en un terreno. En esta descripción, por el término "edificio" se deben entender, por ejemplo, edificios residenciales, edificios comerciales, estadios deportivos, centros comerciales, pero también buques.

El sistema de control de acceso 1 supervisa el acceso 12, de modo que solo los usuarios autorizados 2 pueden acceder a la zona 8, por ejemplo, bloqueando o desbloqueando una puerta, una barrera, un molinete u otra barrera física, activando un dispositivo de información 38 en el caso de un acceso sin barrera física, si se detecta un usuario no autorizado 2, o combinando estas medidas. El dispositivo de información 38 puede activar, por ejemplo, una alarma óptica y/o acústica, o puede iniciar una notificación de un servicio de seguridad. En la fig. 1 está representado el sistema de control de acceso 1 a modo de ilustración como dispuesto en el acceso 12; además está indicado un molinete 36 como barrera física a modo de ejemplo. Sin embargo, el experto en la materia reconoce que en una implementación concreta el sistema de control de acceso 1 o sus componentes pueden estar dispuestos de diferentes formas.

En otro ejemplo de realización, el sistema de control de acceso 1 está dispuesto en un acceso 18 hacia al menos un espacio 4, eventualmente en cada acceso 18. Dependiendo del tipo de habitación 4, el acceso 18 incluye, por ejemplo, una puerta de oficina, una puerta de piso, una puerta de apartamento o una puerta de ascensor, que luego respectivamente representan una barrera física. En este ejemplo de realización, cada habitación 4 corresponde a una zona de acceso restringido 8, y la zona delante de un acceso 18 corresponde a la zona pública 10. El sistema de control de acceso 1 desbloquea, por ejemplo, una cerradura electrónica de una puerta de oficina o de una vivienda. En una aplicación en combinación con un ascensor, el sistema de control de acceso 1 puede evitar, por ejemplo, la salida de una cabina de ascensor cuando un usuario no autorizado 2 sube o quiere subir a la cabina.

Como se indica en la Fig. 1, el sistema de control de acceso 1 comprende un dispositivo de emisión y de recepción 14 (representado en la Fig. 1 como TX/RX) y una cámara 16 como parte de un dispositivo de procesamiento de imágenes; otros componentes del sistema de control de acceso 1 se muestran en la Fig. 2. En un ejemplo de realización descrito aquí, el dispositivo de emisión y de recepción está diseñado para recibir señales de radio, por lo que en lo sucesivo también se denomina transceptor 14. El transceptor 14 se comunica con los dispositivos electrónicos móviles 6 cuando están dentro del alcance de radio hacia el transceptor 14, es decir, una señal de radio emitida por un dispositivo móvil 6 tiene una intensidad de señal (expresada mediante un valor RSSI (Received Signal Strength Indicator)) en la ubicación del transceptor 14 que es mayor que un umbral establecido para una recepción segura. La comunicación se realiza, por ejemplo, a través de una red inalámbrica de campo cercano, como una red inalámbrica Bluetooth, WLAN/WiFi o una red inalámbrica ZigBee. Bluetooth es un estándar según IEEE 802.15.1, WLAN/WiFi es un estándar según IEEE 802.11, Zig-Bee es un estándar según IEEE 802.15.4; las redes inalámbricas de esa clase, según estos estándares sirven para la interconexión inalámbrica de dispositivos sobre una distancia corta desde aproximadamente unos pocos metros hasta aproximadamente unos cien metros. La red inalámbrica forma la interfaz a través de la que el dispositivo electrónico móvil 6 y el transceptor 14 pueden comunicarse entre sí.

En otro ejemplo de realización, el dispositivo de emisión y de recepción 14 está acoplado comunicativamente a una red de comunicación 38. En este ejemplo de realización, el dispositivo de emisión y de recepción 14 puede recibir el identificador específico del dispositivo de un dispositivo móvil 6 a través de la red de comunicación 38. El dispositivo móvil 6 puede determinar su ubicación actual con la ayuda de una función instalada en el mismo para determinar la posición, por ejemplo, en base a GPS (Sistema de Posicionamiento Global). Mediante una conexión de Internet (incluida la red de comunicación 38) a través de un sistema de telefonía móvil (por ejemplo, 4G) y, en algunos casos, un software específico de la aplicación, el dispositivo móvil 6 puede transmitir la ubicación junto con su identificador al dispositivo de emisión y de recepción 14.

A continuación, se describen ejemplos de realización de la tecnología con ayuda del transceptor 14. Como se describió anteriormente, el transceptor 14 recibe un identificador enviado por un dispositivo electrónico móvil 6 por medio de una radiocomunicación (de campo cercano).

La cámara 16 genera un registro de cámara de un usuario 2 (en particular, su rostro), que se encuentra en el área de detección de la cámara 16, si el usuario 2 desea entrar en la zona de acceso restringido 8 en el acceso 12. En un ejemplo de realización, la cámara 16 genera un registro de cámara digital (también denominada imagen digital). El transceptor 14 y la cámara 16 (incluyendo otros componentes del dispositivo de procesamiento de imágenes) pueden estar dispuestos en una carcasa, que está dispuesta, por ejemplo, como se muestra en la fig. 1 en el acceso 12. Alternativamente, el transceptor 14 y la cámara 16 (incluidos otros componentes del dispositivo de procesamiento de imágenes) también pueden estar dispuestos por separado como unidades separadas, por ejemplo, espacialmente separadas entre sí en un área alrededor del acceso 12, en el que la cámara 16 debe disponerse de tal manera que esencialmente solo se detecte aquel usuario 2 que realmente desee acceder.

En la situación mostrada en la fig. 1, la tecnología aquí descrita es aplicable de manera ventajosa para operar el sistema de control de acceso 1 con la menor complejidad posible y para conceder al usuario 2 un acceso cómodo a la zona de acceso restringido 8. En resumen y a modo de ejemplo, el funcionamiento del sistema de control de acceso 1 se realiza según un ejemplo de realización, del siguiente modo: Tan pronto como un usuario 2 está dentro del alcance de radio del transceptor 14, su dispositivo móvil 6 se comunica automáticamente con el transceptor 14 y el dispositivo móvil 6 envía su identificador al transceptor 14. En la situación según la fig. 1, el transceptor 14 recibe una pluralidad de identificadores. Por lo tanto, el sistema de acceso 1 "sabe" cuántos dispositivos móviles 6 se encuentran en un momento determinado en el alcance de radio y, si sus usuarios 2 son usuarios registrados 2, a qué usuario 2 pertenecen los dispositivos móviles 6. Estos usuarios 2 se pueden agrupar en un grupo de usuarios presentes 2. Si ahora uno de los usuarios presentes 2 desea acceder a la zona de acceso restringido 8, el sistema de control de acceso 1, en el marco de un procedimiento de procesamiento de imágenes o de reconocimiento facial, determina un conjunto de datos con características faciales de este usuario 2 y compara este conjunto de datos determinado con los conjuntos de datos (características faciales) almacenados asociados al usuario presente 2. Con ello, esta comparación se limita al grupo de los usuarios presentes 2; por lo tanto, solo se buscan los registros de datos de este grupo en cuanto a si el registro de datos determinado encaja con uno de los registros de datos almacenados. Debido a que no es necesario buscar todos los registros de datos creados en el sistema de control de acceso 1, el procedimiento de reconocimiento facial se lleva a cabo más rápido y se puede decidir más rápidamente si el usuario 2 tiene derecho de acceso o no.

La fig. 1 muestra además la red de comunicación 38, que en un ejemplo de realización está conectada comunicativamente a un sistema anfitrión 36 y al sistema de control de acceso 1. Además, se indica que un usuario 2 puede comunicarse a través de la red de comunicación 38 mediante una conexión de comunicación 40, por ejemplo, con el sistema anfitrión 36 o con un portal web. Las funciones ilustrativas de la red de comunicación 38 y del sistema anfitrión 36 se describen con relación a la fig. 4.

La figura 2 muestra una representación esquemática de un ejemplo de realización del sistema de control de acceso 1. El sistema de control de acceso 1, en un ejemplo de realización, está construido modularmente y comprende un dispositivo de procesamiento de imágenes que, además de la cámara 16, comprende un módulo de procesamiento de imágenes 22 (procesamiento de imágenes en la fig. 2) y un módulo de evaluación 24 (evaluación en la fig. 2).

Adicionalmente, el sistema de control de acceso 1, además del transceptor 14, comprende un procesador 20, un dispositivo de almacenamiento 26 (memoria en la fig. 2) y un dispositivo de almacenamiento intermedio 28 (memoria intermedia en la fig. 2). El experto en la materia reconoce que al menos uno de los dispositivos de almacenamiento 26, 28 también se puede asociar al dispositivo de procesamiento de imágenes o que la función del dispositivo de almacenamiento intermedio 28 puede ser realizada por el dispositivo de almacenamiento 26 y, por lo tanto, el dispositivo de almacenamiento intermedio 28 puede omitirse en un ejemplo de realización. El procesador 20 tiene una salida 32 para una señal de control y una entrada 30 para una señal de resultado generada por el módulo de evaluación 24. Dependiendo de la señal de resultado, el procesador 20 controla el sistema de control de acceso 1 de tal manera que al usuario 2 se le conceda o se le niegue el acceso. Por ejemplo, si una barrera física (por ejemplo, un molinete 36 en la fig. 1) separa las zonas 8, 10, la señal de control libera la barrera o la bloquea. Por el contrario, si la separación de zonas se realiza sin una barrera física, la señal de control, en el caso de un usuario no autorizado 2, por ejemplo, activa el dispositivo de información 38 para generar una alarma o alerta a un servicio de seguridad. El dispositivo de información 38, en combinación con una barrera, también se puede activar para indicar al usuario 2 o a un servicio de seguridad que la barrera se ha desbloqueado o bloqueado.

En un ejemplo de realización, la cámara 16 comprende una cámara digital con propiedades que pueden seleccionarse y/o ajustarse; por lo tanto, en este ejemplo de realización, los registros de la cámara están disponibles como conjuntos de datos digitales. Las propiedades de la cámara digital, por ejemplo, la resolución (por ejemplo, indicada en megapíxeles), la exposición y la distancia focal, se seleccionan o ajustan de tal manera que se puede evaluar un registro de cámara (imagen digital) y el rostro del usuario 2 se puede reconocer en calidad evaluable en la imagen digital. Por ejemplo, la imagen digital está disponible en formato JPEG, pero también puede estar en otro formato, por ejemplo, en formato BMP o JPEG2000. La cámara 16 puede estar equipada con un módulo de sensor o estar conectada con un módulo de sensor separado, que activa la cámara 16 cuando detecta la presencia de un usuario 2 en el área de detección de la cámara 16. El módulo de sensor puede comprender, por ejemplo, un sensor de proximidad, que puede estar diseñado como un sensor ultrasónico, un sensor infrarrojo o un sensor óptico (por ejemplo, una barrera fotoeléctrica, un sensor de luminosidad). Alternativamente, en un ejemplo de realización, la presencia de un usuario 2 en el área de detección de la cámara 16 puede identificarse detectando cambios en el área de detección. Si el usuario 2, por ejemplo, entra en el área de detección y la cámara 16 está continuamente en un estado activo, la cámara 16 registra los cambios delante de un fondo esencialmente estático; estos cambios se interpretan como una presencia.

El módulo de evaluación 24 se muestra a modo de ilustración como una unidad separada que está conectada con el módulo de procesamiento de imágenes 22, el procesador 20 y el dispositivo de almacenamiento intermedio 28. En un ejemplo de realización, el módulo de evaluación 24 y el módulo de procesamiento de imágenes forman una unidad. Los dispositivos de almacenamiento 26, 28 también se muestran como unidades separadas para fines ilustrativos; dependiendo de la configuración, pueden estar agrupados en un dispositivo de almacenamiento, en el que, por ejemplo, ocupan áreas de almacenamiento separadas. Independientemente de esto, los dispositivos de almacenamiento 26, 28 pueden comprender, por ejemplo, una unidad de disco duro (HDD) o una unidad de CD/DVD, una unidad de semiconductor/disco de estado sólido (SSD), o combinaciones de las mismas, u otros dispositivos de almacenamiento para datos digitales.

La unidad mencionada formada por el módulo de evaluación 24 y el módulo de procesamiento de imágenes 22 comprende al menos una unidad de procesador que realiza un procedimiento asistido por ordenador para el procesamiento de imágenes. Se conocen procedimientos de procesamiento de imágenes, por ejemplo, por el documento US 8,494,231 B2. Una presentación básica del procesamiento de imágenes con el fin del reconocimiento facial se describe en la publicación "Reconocimiento facial" de la Oficina Federal Alemana de Seguridad de la Información (bajo el tema Biometría, disponible en la dirección www.bsi.bund.de). Esta publicación distingue entre las tres etapas principales de trabajo "Crear plantilla", "Crear conjunto de datos de referencia" y "Comparar imágenes faciales". Para que la comparación de dos imágenes faciales sea lo más sencilla y rápida posible, se determinan las características de un rostro y se almacenan en forma de un conjunto de datos de características denominado como "plantilla". Si en una imagen se encontró el rostro de un usuario y fue normalizado, además de los ojos, la nariz y la zona de la boca /barbilla, se buscan, miden y relacionan otras características. Estas características extraídas se codifican, comprimen y almacenan como un registro de datos de características (plantilla). Para determinar la similitud de las plantillas de dos imágenes faciales, estas se combinan mediante un algoritmo matemático. Esto da como resultado un grado de similitud de las plantillas. Si el resultado se encuentra dentro de ciertos límites de tolerancia, las dos plantillas y, por lo tanto, las imágenes faciales que se toma como base se clasifican como idénticas.

Según la tecnología aquí descrita, al registrarse como usuario autorizado, se crea una plantilla para cada usuario 2 y se almacena en un perfil de usuario del usuario 2. La plantilla se puede generar a partir de una imagen digital que muestra el rostro del usuario 2. Esta plantilla se denomina en lo sucesivo plantilla de referencia. Es ventajoso que durante el registro el rostro del usuario 2 está expuesto a condiciones de luz similares a las del lugar en el entorno de la cámara 16. Esto favorece la comparación de plantillas, es decir, la comparación de la plantilla de referencia con una plantilla en tiempo real, que se genera cuando un usuario 2 desea acceder a la zona de acceso restringido 8.

En la situación mostrada en la fig. 1, varios usuarios 2 se encuentran en la zona pública 10; algunos de ellos pueden desear el acceso a la zona de acceso restringido 8, algunos pueden estar de camino a una salida del edificio desde la zona 8 y, a su vez, otros pueden estar de camino a otra parte del edificio. En la situación mostrada, esto significa que no todos los usuarios 2 que se encuentran en la zona pública 10 realmente quieren entrar en la zona 8. Sin embargo, desde el punto de vista del sistema de control de acceso 1, todos los usuarios presentes son 2 usuarios potenciales 2 que tarde o temprano podrían querer acceder.

El sistema de control de acceso 1 determina los usuarios 2 presentes con la ayuda de la comunicación entre los dispositivos móviles 6 y el transceptor 14. En cada dispositivo móvil 6 se activa un módulo de radio, por ejemplo, un módulo Bluetooth, para poder comunicarse con el transceptor 14 tan pronto como este se encuentre dentro del alcance de radio del transceptor 14. Dependiendo de la configuración del dispositivo móvil 6 y de su módulo de radio, se puede activar adicionalmente una aplicación de software específica de la aplicación (también denominada como App, aplicación). La aplicación de software específica de la aplicación, en un ejemplo de realización, se utiliza junto con el control de acceso y el uso de ascensores. En un ejemplo de realización, el software específico de la aplicación también genera un identificador único e invariable en el tiempo para el dispositivo móvil. Un identificador de esa clase, generado por el software, constituye una alternativa al número de identificación del dispositivo mencionado anteriormente y a un número de teléfono.

Durante la comunicación, el dispositivo móvil 6 envía su identificador al transceptor 14; el sistema de control de acceso 1 actualiza así una base de datos en la que se almacenan los identificadores de todos los dispositivos móviles 6 presentes en ese momento. Puede tratarse tanto de dispositivos móviles 6, cuyos usuarios 2 están registrados como usuarios autorizados 2 en el sistema de control de acceso 1, como de dispositivos móviles 6, cuyos usuarios 2 no están registrados. En un ejemplo de realización, la base de datos que almacena los identificadores de los usuarios presentes 2 se encuentra en la memoria intermedia 28.

Para cada usuario registrado 2 se ha creado un perfil de usuario en el sistema de control de acceso 1, es decir, se almacena como un registro de datos en una base de datos 34. En un ejemplo de realización, la base de datos 34 está configurada en el dispositivo de almacenamiento 26. El perfil de usuario comprende datos personales del usuario 2 (por ejemplo, nombre, motivo de la autorización (residente, empleados, proveedor de servicios externos) y características faciales en forma de una plantilla), autorizaciones de acceso (por ejemplo, ciertas habitaciones 4 y pisos) y, posiblemente, restricciones de tiempo de acceso (por ejemplo, acceso de lunes a viernes, de 7:00 a 20:00). En el perfil de usuario, al usuario 2 también se asocia al menos un dispositivo móvil 6. Como alternativa a la creación del perfil de usuario en el sistema de control de acceso 1, el perfil de usuario puede estar creado en una base de datos de un sistema de administración del edificio, en el que el sistema de control de acceso 1 puede acceder a esta base de datos a través de una red de comunicación.

Si uno de los usuarios presentes 2 desea acceder a la zona de acceso restringido 8, se mueve en la zona pública 10, por ejemplo, desde una entrada principal del edificio, en la dirección del acceso 12. Si el usuario 2 entra en un área de detección de la cámara 16 dispuesta allí, la cámara 16 genera una o varias imágenes digitales o una grabación de vídeo, que están presentes en cada caso como un conjunto de datos digitales y se almacenan brevemente para su procesamiento posterior. El módulo de procesamiento de imágenes 22 determina la plantilla en tiempo real a partir del conjunto de datos, como se explica en otra parte de esta descripción.

Si se determina la plantilla en tiempo real, el módulo de evaluación 24 inicia un algoritmo de búsqueda para comprobar si la plantilla en tiempo real determinada se puede asociar a un usuario registrado 2. En lugar de buscar en todos los perfiles de usuario almacenados en el dispositivo de almacenamiento 26, el algoritmo de búsqueda solo busca en los perfiles de usuario de los usuarios presentes 2. El grupo de usuarios presentes 2 se almacena en la memoria intermedia 28, como se describió anteriormente. Si las características faciales determinadas coinciden en un grado determinado con las características faciales almacenadas en el perfil de usuario del usuario 2, el módulo de evaluación 24 genera una señal de resultado que indica que el usuario 2 tiene derecho de acceso. Si, por el contrario, no existe tal coincidencia, la señal de resultado generada por el módulo de evaluación 24 indica que el usuario 2 no tiene derecho de acceso.

El dispositivo móvil 6 puede ser, por ejemplo, un teléfono móvil, un teléfono inteligente, una tableta o un reloj inteligente, en los que estos dispositivos suelen estar equipados con hardware que permite la comunicación a través de una red inalámbrica de campo cercano. Pero el dispositivo móvil 6 también pueden ser gafas con un ordenador en miniatura u otro dispositivo asistido por ordenador que se lleve en el cuerpo (también denominado como "dispositivo portátil"), si estos dispositivos están diseñados para una comunicación de campo cercano. Dependiendo de la configuración del dispositivo móvil 6, por ejemplo, puede disponer de una interfaz gráfica de usuario (también denominada interfaz gráfica de usuario, GUI) para poder activar y desactivar selectivamente el dispositivo móvil 6 y sus funciones.

Con la comprensión de los componentes básicos del sistema descritos anteriormente y sus funcionalidades, se realiza a continuación, en combinación con la fig. 3, una descripción de un procedimiento de control de acceso ilustrativo como un aspecto de un procedimiento para operar el sistema de control de acceso 1 (otro aspecto es un procedimiento de registro para un visitante descrito en combinación con la fig. 4). La descripción se refiere a un usuario 2 que desea entrar en la zona de acceso restringido 8 en el acceso 12, por ejemplo, para utilizar un ascensor allí. El usuario 2 lleva consigo el dispositivo móvil 2 y ha activado su módulo de radio (por ejemplo, para la comunicación Bluetooth) y,

posiblemente, una aplicación de software asociada. El procedimiento comienza en una etapa S1 y termina en una etapa S10.

Si el usuario 2 se encuentra con su dispositivo móvil 6 en la zona pública 10 y dentro del alcance de radio del transceptor 14, el transceptor 14 recibe en una etapa S2 un identificador emitido por el dispositivo móvil 6. El transceptor 14 y el dispositivo móvil 6 se comunican según el mismo estándar de comunicación, en este ejemplo de realización a través de una conexión inalámbrica Bluetooth. El identificador recibido se almacena en una etapa S3; por ejemplo, en el dispositivo de almacenamiento intermedio 28.

Las etapas S2 y S3 se realizan para cada dispositivo móvil 6 que se encuentra dentro del alcance de radio del transceptor 14 y funciona según el mismo estándar de comunicación que el transceptor 14. Dependiendo del número de usuarios 2 en la zona pública 10, en un momento determinado se puede almacenar una pluralidad de identificadores, correspondiente a un grupo de usuarios presentes 2, en el dispositivo de almacenamiento intermedio 28. El experto en la materia reconoce que el dispositivo de almacenamiento intermedio 28 se actualiza cuando un dispositivo móvil 6 ya no está dentro del alcance de radio, por ejemplo, porque el usuario 2 correspondiente ha abandonado la zona pública 10 sin desear el acceso a la zona de acceso restringido 8 o porque el usuario 2 correspondiente ya ha entrado en la zona de acceso restringido 8. Por lo tanto, el dispositivo de almacenamiento intermedio 28 almacena los identificadores de los dispositivos móviles 6, cuyos usuarios 2 están presentes en un momento determinado en la zona pública 10.

En una etapa S4 se determina si uno de los usuarios presentes 2 desea acceder a la zona de acceso restringido 8. El sistema de control de acceso 1 reconoce este deseo según un ejemplo de realización con la ayuda del módulo de sensor mencionado anteriormente o la detección de cambios de fondo. Por ejemplo, el módulo sensor detecta cuando el usuario 2 entra en el área de detección de la cámara 16, después de lo cual se activa la cámara 16. Si se reconoce una solicitud de acceso, el procedimiento avanza a lo largo de la rama Sí hacia una etapa S5. De lo contrario, el procedimiento permanece en un bucle a lo largo de la rama No.

En la etapa S5, la cámara 16 activada genera una imagen digital que representa al menos el rostro del usuario 2 detectado, y el módulo de procesamiento de imágenes genera una plantilla en tiempo real a partir de la imagen digital, como se explica en otra parte de esta descripción.

En una etapa S6, cada perfil de usuario asociado a un identificador recibido se busca en la base de datos 34 mediante la plantilla en tiempo real determinada en la etapa S5. Un perfil de usuario solo se busca si está asociado a un usuario presente 2 en base a un identificador recibido. Si un usuario registrado 2 solicita acceso, existe un perfil de usuario para este usuario 2 en la base de datos 34, en el que se almacena el identificador del dispositivo móvil 6. Si el usuario que solicita el acceso 2 no es un usuario registrado 2, no se asocia ningún perfil de usuario al identificador del dispositivo móvil 6.

Al buscar según la etapa S6, en una etapa S7 se comprueba si la plantilla en tiempo real coincide con una plantilla de referencia en un grado determinado. La plantilla en tiempo real y las plantillas de referencia, en un ejemplo de realización, respectivamente comprenden un número determinado de parámetros faciales definidos y sus valores (por ejemplo, distancia entre los ojos, ancho de la boca, distancia entre la parte superior y el borde inferior de los labios, distancia entre la nariz y el borde inferior de los labios, etc.). Durante la búsqueda, los valores de los parámetros de la plantilla en tiempo real se comparan con los valores de los parámetros de la plantilla de referencia. La coincidencia existe si el grado de similitud de las plantillas corresponde al menos al grado especificado. El grado especificado indica una coincidencia porcentual de los parámetros faciales de la plantilla en tiempo real con los parámetros faciales de una plantilla de referencia. Dependiendo de los requisitos de precisión, el grado especificado se puede seleccionar, por ejemplo, entre aprox. el 60 % y aprox. el 90 %.

Si hay una coincidencia, el procedimiento avanza a lo largo de la rama Sí hasta una etapa S9, en la que se concede acceso al usuario 2. Si, por otro lado, no hay una coincidencia, el procedimiento avanza a lo largo de la rama No hacia una etapa S8 y se le niega el acceso al usuario 2.

Por la descripción de un procedimiento ilustrativo para operar el sistema de control de acceso 1, realizada en combinación con la fig. 3, es evidente que un usuario 2 no tiene que manejar su dispositivo móvil 6 para acceder a la zona de acceso restringido 8. Dependiendo del diseño del acceso, es decir, con o sin barrera física, el control de la autorización de acceso se puede realizar sin que el usuario 2 note algo.

En un ejemplo de realización, el sistema de control de acceso 1 está conectado a un sistema de ascensor, en particular a un control de ascensor. La comunicación entre el sistema de control de acceso 1 y el control de ascensor se puede realizar a través de la red 38. Si el control de acceso se realiza, por ejemplo, en el vestíbulo de entrada del edificio, por el que los usuarios 2 deben pasar para acceder a los ascensores, se puede iniciar una llamada de destino cada vez que se conceda acceso al usuario 2 en cuestión. El control de ascensor del sistema de ascensor procesa la llamada de destino y le asigna un ascensor. El ascensor asignado a la llamada de destino se puede mostrar al usuario 2, por ejemplo, a través de un terminal en el acceso 12 y/o se puede comunicar por voz. Por lo tanto, el usuario 2 puede ir directamente al ascensor asignado sin tener que introducir una llamada de ascensor.

En la descripción realizada con relación a la fig. 3, cada usuario 2 está registrado en el sistema de control de acceso número 1, como usuario autorizado 2. Dependiendo del tipo de edificio, incluso los usuarios no registrados 2 pueden desear acceder a la zona de acceso restringido 8, por ejemplo, los visitantes. La fig. 4 muestra un diagrama de señal de un ejemplo de realización de un procedimiento que permite conceder también a los visitantes un acceso cómodo a la zona de acceso restringido 8. Para ilustrar una situación a modo de ejemplo, la figura 4 muestra esquemáticamente interacciones entre un anfitrión o un sistema anfitrión 36 utilizado por el mismo, un visitante o su dispositivo móvil 6 y el sistema de control de acceso 1, para registrar al visitante mediante un procedimiento de registro en el sistema de control 1. Según la tecnología aquí descrita, el visitante también es un usuario 2 (el número de referencia 2 se utilizará en lo sucesivo tanto para el visitante como para uno o más usuarios).

En esta situación, el anfitrión y el visitante 2 acuerdan una fecha, es decir, una fecha y un horario o período en el que el anfitrión espera al visitante 2. A continuación, el anfitrión genera, por ejemplo, una invitación con el sistema anfitrión (por ejemplo, PC, portátil, tableta, teléfono inteligente u otro dispositivo electrónico) y una aplicación de software instalada en el mismo (por ejemplo, con la ayuda de Outlook o programas de aplicaciones similares) y la envía al visitante 2, por ejemplo, a través de la red de comunicación 38 y la conexión de comunicación 40. La conexión de comunicación 40 se puede realizar, por ejemplo, a través de un sistema de comunicación de telefonía móvil.

La invitación comprende, además de los datos de la fecha, un número de identificación asociado a la invitación (identificado en la fig. 4 como "ID") y, además, datos sobre un canal de comunicación que el visitante 2 tiene que utilizar para una comunicación con el sistema de control de acceso 1, con el fin de registrarse. En un ejemplo de realización, el canal de comunicación es la Internet; por lo tanto, los datos sobre el canal de comunicación comprenden una dirección de Internet para un portal web (identificado en la fig. 4 como "enlace"). La dirección de Internet puede comprender, por ejemplo, un indicador de recursos uniforme (Uniform Resource Locator (URL)), que identifica y localiza el portal web como un recurso a través del procedimiento de acceso que se utilizará (por ejemplo, un protocolo de red utilizado, como HTTP o FTP) y la ubicación del recurso en una red informática. El portal web está asociado a un sistema informático del sistema de control de acceso 1. La transmisión de la invitación, en un ejemplo de realización, se realiza a través de la red de comunicación 38 por medio de una señal DS1; se puede realizar, por ejemplo, como un mensaje de texto hacia el dispositivo móvil 6 del visitante 2 o como un correo electrónico a la dirección de correo electrónico del visitante 2.

El anfitrión o el sistema anfitrión 36 también envía los datos de la invitación por medio de una señal DS2 al sistema de control de acceso 1, por ejemplo, a través de la red de comunicación 38 y esencialmente al mismo tiempo que el envío de la invitación o en un momento posterior. El sistema de control de acceso 1, controlado por el procesador 20, crea un perfil de visitante para los datos de invitación recibidos. En un ejemplo de realización, los datos de invitación comprenden, además de los datos de la fecha, también datos sobre el anfitrión, por ejemplo, nombre, número de teléfono, piso y/o número de vivienda u oficina. Además, se puede establecer una ventana de tiempo dentro de la cual se debe conceder acceso al visitante 2. La ventana de tiempo puede indicar, por ejemplo, que el visitante 2 tiene acceso aproximadamente media hora antes y después del inicio del momento fijado, en caso de que el visitante 2 llegue demasiado pronto o se retrase. El perfil del visitante se puede eliminar después de la llegada del visitante 2 o en un momento posterior.

La invitación invita al visitante 2 a enviar una imagen digital que muestre el rostro del visitante 2 al sistema de control de acceso 1 a través del canal de comunicación especificado, que comprende, por ejemplo, el portal web. El visitante 2, por ejemplo, puede hacer un autorretrato actual (también conocido como "selfie") de sí mismo con la cámara de su dispositivo móvil 6 y cargarlo a través del portal web. En otro ejemplo de realización, el visitante 2 también puede cargar una imagen digital guardada, tomada en un momento anterior. Una ventaja de la tecnología aquí descrita reside en que el visitante 2 puede cargar la imagen digital en el momento que elija, siempre que esto se haga antes de la fecha. El visitante 2 puede estar geográficamente lejos del edificio o estar ya dentro o cerca del edificio.

En relación con la carga de la imagen digital, también se realiza una transmisión del número de identificación de la invitación, para que el sistema de control de acceso 1 pueda asociar inequívocamente la imagen digital recibida a la invitación. Dependiendo de la configuración, se le puede pedir al visitante que introduzca el identificador del dispositivo móvil 6 (por ejemplo, número de teléfono o número de identificación del dispositivo). Si el visitante carga la imagen digital mediante el dispositivo móvil 6, en un ejemplo de realización el identificador del dispositivo móvil 6 también se transmite al sistema de control de acceso 1, por ejemplo, automáticamente. Si se instala una aplicación de software específica de la aplicación en el dispositivo móvil 6, como se describió anteriormente, ayuda al visitante 2 a cargar la imagen digital. La transmisión de la imagen digital, del identificador y del número de identificación de la invitación se realiza mediante una señal DS3, por ejemplo, a través de la red de comunicación 38 y la conexión de comunicación 40. La transmisión de la señal DS3 se puede realizar según un protocolo de transmisión conocido, por ejemplo, TCP (Transmission Control Protocol), IP (Internet Protocol) y UDP (User Data Protocol). El sistema de control de acceso 1 almacena los datos recibidos (imagen digital, identificador y número de identificación de la invitación) en el perfil del visitante.

La tecnología aquí descrita también puede utilizar otros canales de comunicación. Como alternativa al uso de un portal web, la invitación puede solicitar al visitante 2 que transmita la imagen digital, el identificador y el número de identificación de la invitación a una administración del edificio. La administración del edificio puede administrar, por ejemplo, la base de datos 34 para el edificio en cuestión, en la que se almacenan los perfiles de usuario de los usuarios

autorizados 2. La transmisión a la administración del edificio se puede realizar, por ejemplo, a una dirección de correo electrónico de la administración del edificio especificada en la invitación o al número de teléfono de la administración del edificio, por ejemplo, para un mensaje SMS o MMS. El personal de la administración del edificio puede entonces disponer el procesamiento posterior de los datos recibidos.

En un ejemplo de realización, el procesador 20 mostrado en la fig. 2 controla la recepción y el procesamiento posterior de la imagen digital, del identificador y del número de identificación de la invitación. Con la ayuda del dispositivo de procesamiento de imágenes 22, el sistema de control de acceso 1 crea una plantilla de referencia a partir de la imagen digital del visitante 2, como se describe con relación a la fig. 2, y almacena la plantilla de referencia en el perfil del visitante. Por lo tanto, según un ejemplo de realización, el perfil de visitante está completo, a los efectos del control de acceso, y se ha completado el procedimiento de registro mediante el cual el visitante 2 se registra en el sistema de control de acceso 1. Al acceder al perfil de visitante, por ejemplo, por medio del identificador del dispositivo móvil 6 del visitante 2, se pueden leer la plantilla de referencia y los datos de invitación.

Una vez creado el perfil de visitante, se podrá conceder el acceso al visitante 2, según el procedimiento de control de acceso descrito con relación a la fig. 3, si se presenta en el edificio en la fecha acordada. Tan pronto como el visitante llega al área de recepción del transceptor 14 en la zona pública 10, el transceptor 14 recibe el identificador emitido por el dispositivo móvil 6. La recepción del identificador del dispositivo móvil 6 se realiza como se ha descrito anteriormente y está representada en la fig. 4 mediante una señal DS4. Si el visitante a continuación ingresa al área de detección de la cámara 16, la cámara 16 genera una imagen digital que muestra el rostro del visitante. La generación de la imagen digital mediante la cámara 16 y la generación subsiguiente de una plantilla en tiempo real se realizan como se ha descrito anteriormente; en la fig. 4 esto está representado por medio de una señal DS 5.

El sistema de control de acceso 1 comprueba si la plantilla en tiempo real coincide con la plantilla de referencia en el grado especificado. Además, el sistema de control de acceso 1 comprueba si el visitante solicita el acceso dentro de la ventana de tiempo establecida en el perfil del visitante. Si se cumplen ambas condiciones, se concede el acceso al visitante.

En un ejemplo de realización, el sistema de control de acceso 1 genera y envía un mensaje para el anfitrión que informa al anfitrión que se ha concedido acceso al visitante. De este modo, el anfitrión puede prepararse rápidamente para la llegada del visitante.

Dependiendo del diseño del edificio, el sistema de control de acceso 1 puede comunicarse con un control de ascensor para generar una llamada de destino para el visitante 2 al conceder el acceso. El control del ascensor asigna un ascensor a la llamada de destino, de manera que el ascensor asignado se puede comunicar al visitante 2 en la zona de acceso 12 por pantalla o voz. El ascensor asignado transporta al visitante 2 al piso en el que se encuentra el anfitrión. Por ejemplo, el piso del anfitrión está almacenado en el perfil del visitante junto con los datos de la invitación. Por lo tanto, el visitante 2, especialmente si es la primera vez en el edificio, no tiene que ocuparse de ingresar el piso de destino. Al visitante 2 también se le puede proporcionar más información para orientarse mejor en el edificio, por ejemplo, se le puede comunicar al visitante 2 en qué dirección (posiblemente también hasta dónde) debe ir después de llegar al piso. La comunicación de dicha información de orientación se puede realizar, por ejemplo, por medio del dispositivo móvil 6 del visitante 2 y/o pantallas en los pisos o en la cabina del ascensor.

REIVINDICACIONES

1. Procedimiento para operar un sistema de control de acceso (1) para el control de un acceso a una zona de acceso restringido (8) en un edificio o un terreno, en el que el sistema de control de acceso (1) comprende un dispositivo de emisión y de recepción (14), un dispositivo de almacenamiento (26, 28), un procesador (20) y un dispositivo de procesamiento de imágenes (16, 22, 24), en el que el procedimiento comprende un procedimiento de registro para un visitante (2), en el que en el procedimiento de registro:

a través del sistema de control de acceso (1) se reciben datos de invitación generados por un sistema de anfitrión electrónico (36) y enviados como señal eléctrica (DS2) por el sistema de anfitrión (36), en el que los datos de invitación comprenden un número de identificación de una invitación y se refieren a una fecha en la que un anfitrión espera a un visitante (2) en la zona de acceso restringido (8);

en el dispositivo de almacenamiento (26, 28) se crea un perfil de visitante asociado a la invitación y los datos de la invitación se almacenan en el perfil de visitante, en el que el dispositivo de almacenamiento (26, 28) contiene una base de datos (34) que está proporcionada para almacenar perfiles de usuario de usuarios (2) y visitantes (2) autorizados;

a través de un dispositivo electrónico (6) del visitante (2), se transmiten datos de imagen del visitante (2), el número de identificación de la invitación y un identificador específico del dispositivo electrónico (6), como otra señal eléctrica (DS3), a través de un canal de comunicación indicado en la invitación para un almacenamiento en el perfil de visitante creado para el visitante (2);

a través del sistema de control de acceso (1), se reciben los datos de imagen del visitante (2), el número de identificación de la invitación y el identificador específico del dispositivo electrónico (6) del visitante (2);

en el dispositivo de almacenamiento (26, 28), se almacenan los datos de imagen y el identificador, en el que los datos de imagen y el identificador se asocian al perfil de visitante creado para el visitante (2), por medio del número de identificación de la invitación;

a través del sistema de control de acceso (1) se procesan los datos de imagen para generar una plantilla de referencia; y

el perfil de visitante se almacena en la plantilla de referencia.

2. Procedimiento según la reivindicación 1, en el que los datos de imagen, el número de identificación de la invitación y el identificador se reciben a través del canal de comunicación que está indicado en la invitación generada por el sistema anfitrión.

3. Procedimiento según la reivindicación 2, en el que como canal de comunicación está indicada una dirección de Internet de un portal web.

4. Procedimiento según la reivindicación 2, en el que como canal de comunicación están indicados una dirección de correo electrónico o un número de teléfono de una administración del edificio.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, que presenta además el establecimiento de una ventana de tiempo que define una duración de tiempo antes y/o después de un horario especificado en la fecha, dentro de la cual se debe conceder acceso al visitante (2).

6. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende un procedimiento de control de acceso, el procedimiento de control de acceso comprende:

la recepción de un identificador específico del dispositivo, de un dispositivo electrónico móvil (6), a través del dispositivo de emisión y de recepción (14), cuando el dispositivo electrónico móvil (6) se encuentra en una zona pública (10) desde la que un usuario (2) o el visitante (2) puede solicitar acceso a la zona de acceso restringido (8);

el almacenamiento del identificador recibido del dispositivo electrónico móvil (6) en el dispositivo de almacenamiento (26, 28), como perteneciente a un usuario (2) o visitante (2) presente;

la generación de una plantilla en tiempo real para características faciales del usuario (2) o visitante (2) presente a partir de una toma de cámara del usuario (2) o visitante (2) presente generada por una cámara (16) del dispositivo de procesamiento de imágenes (16, 22, 24), cuando se detecta una presencia del usuario (2) o visitante (2) presente en una zona de detección de la cámara (16), cuando el usuario (2) o visitante (2) presente desea acceder a la zona de acceso restringido (8), en el que la plantilla en tiempo real es generada por el dispositivo de procesamiento de imágenes (16, 22, 24);

la búsqueda de perfiles de usuario almacenados en la base de datos (34), según una plantilla de referencia, que coincida en un grado determinado con la plantilla en tiempo real, en el que un perfil de usuario solo se busca si está asociado a un usuario (2) o visitante (2) presente, en base a un identificador recibido, en el que en caso de una coincidencia el sistema (1) concede al usuario (2) o visitante (2) acceso a la zona de acceso restringido (8) y, en caso de no coincidencia, lo niega.

7. Procedimiento según la reivindicación 6, en el que cuando una pluralidad de dispositivos electrónicos móviles (6) se encuentra en la zona pública (10),

- se almacena una pluralidad de identificadores recibidos en el dispositivo de almacenamiento (26, 28),

- para cada identificador almacenado se determina si en la base de datos (34) el identificador recibido está asociado a una plantilla de referencia; y,

- si existen asociaciones de esa clase, se comprueba si la plantilla en tiempo real coincide en un grado determinado con una de esas plantillas de referencia, en el que en el caso de una coincidencia, el sistema (1) concede al usuario (2) o al visitante (2) acceso a la zona de acceso restringido (8) y, en caso de no coincidencia, lo niega.

8. Procedimiento según la reivindicación 6 o 7, en el que la comprobación comprende una generación de una señal de resultado que, en el caso de una coincidencia, indica que el usuario (2) o visitante (2) tiene acceso a la zona de acceso restringido (8) y que, en caso de no coincidencia, indica que el usuario (2) o visitante (2) no tiene acceso a la zona de acceso restringido (8).

9. Procedimiento según la reivindicación 8, que además presenta la generación de una señal de control como función de la señal de resultado para liberar una barrera (18, 36).

10. Procedimiento según la reivindicación 8 o 9, que además presenta la generación de una señal de control como función de la señal de resultado para activar un dispositivo de información (38) en caso de una negación de acceso.

11. Procedimiento según cualquiera de las reivindicaciones anteriores 6-10, en el que el dispositivo de emisión y de recepción (14) se comunica con un dispositivo electrónico móvil (6) mediante una conexión de radio, en el que la conexión de radio entre el dispositivo de emisión y de recepción (14) y un dispositivo electrónico móvil (6) de un usuario (2) o visitante (2) se realiza según un estándar Bluetooth o un estándar WLAN/WiFi, y en el que el dispositivo de emisión y de recepción (14) recibe el identificador específico del dispositivo a través de la conexión de radio cuando el dispositivo electrónico móvil (6) se encuentra dentro del alcance de radio del dispositivo de emisión y de recepción (14).

12. Procedimiento según cualquiera de las reivindicaciones 6-11, en el que el dispositivo emisión y de recepción (14) recibe el identificador específico del dispositivo mediante una red de comunicación (38).

13. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el identificador es generado por un software específico de la aplicación que está activo en el dispositivo móvil (6), en el que el identificador es invariable en el tiempo.

14. Procedimiento según cualquiera de las reivindicaciones 6-13, en el que la plantilla en tiempo real y la plantilla de referencia comprenden respectivamente un número determinado de parámetros faciales especificados, y en el que el grado determinado se ubica entre aproximadamente el 60 % y aproximadamente el 90 %, en el que el grado determinado indica una coincidencia porcentual de los parámetros faciales de la plantilla en tiempo real con los parámetros faciales de una plantilla de referencia.

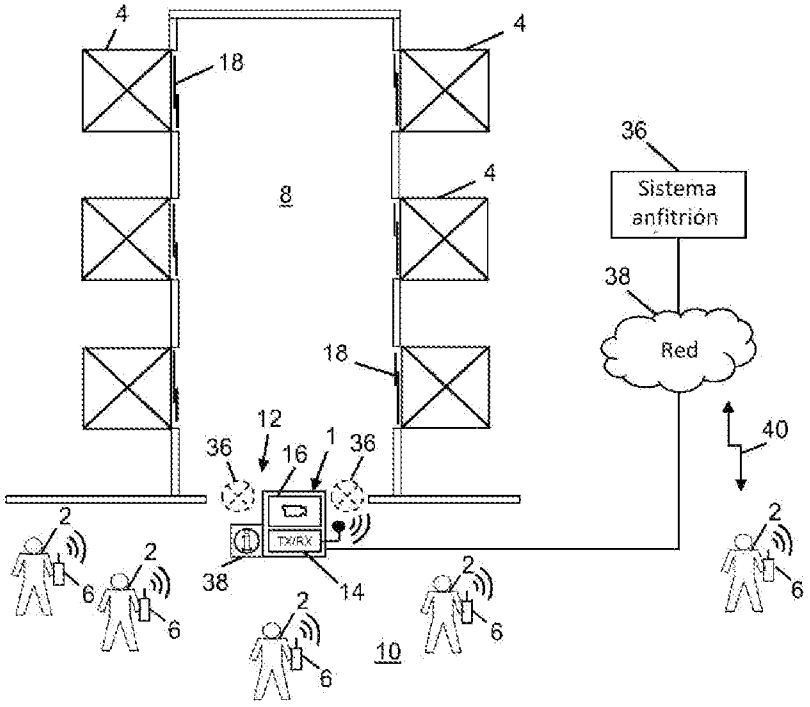
4
18
4
8
4
36
Sistema anfitrión
38
Red
18
12
36
16
1
36
40
TX/RX
2
6
38
14
2
6
2
6
2
6
10

Fig. 1

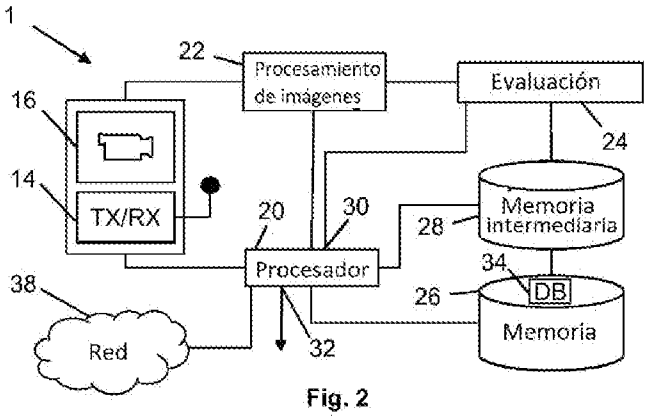
1
22
Procesamiento de imágenes
Evaluación
16
24
14
TX/RX
20
30
28
Memoria intermediaria
Procesador
34
38
26
DB
Memoria
Red
32

Fig. 2

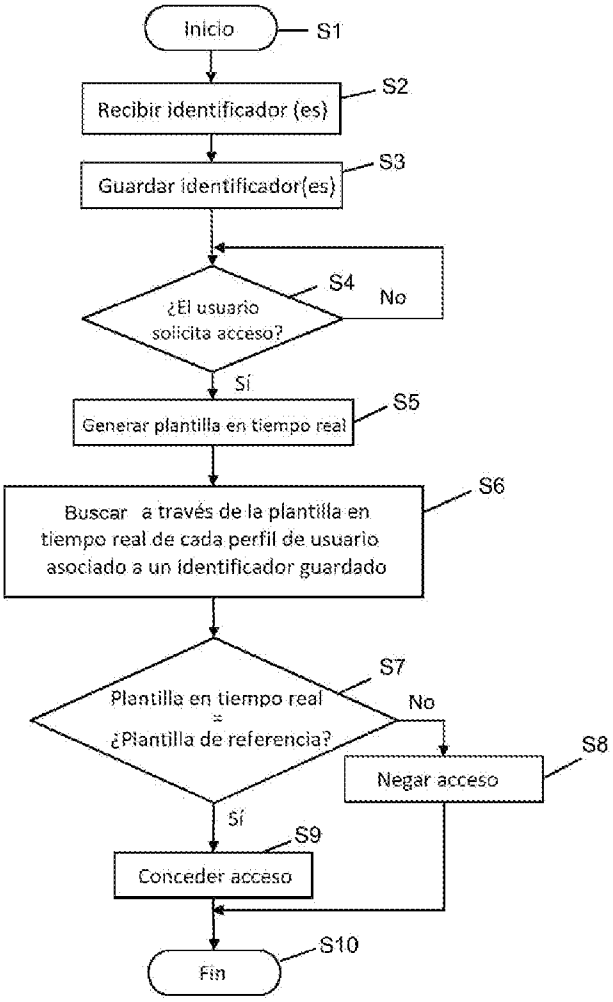
Inicio
S1
Recibir identificador (es)
S2
Guardar identificador(es)
S3
¿El usuario solicita acceso?
S4
No
Sí
Generar plantilla en tiempo real
S5
Buscar a través de la plantilla en tiempo real de cada perfil de usuario asociado a un identificador guardado
S6
Plantilla en tiempo real = ¿Plantilla de referencia?
S7
No
Negar acceso
S8
Sí
Conceder acceso
S9
Fin
S10

Fig. 3

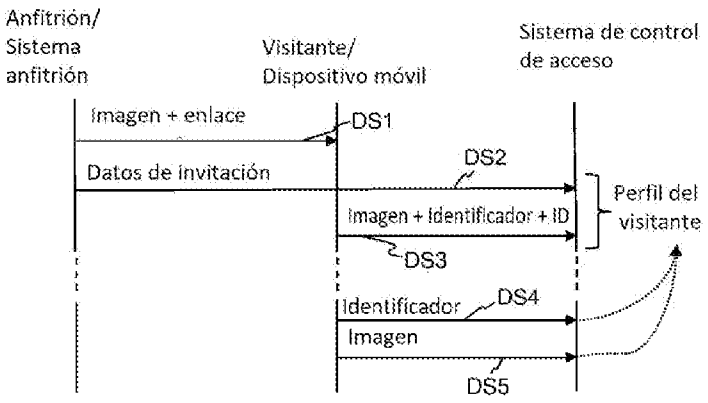
Anfitrión/
Sistema
anfitrión
Visitante/
Dispositivo móvil
Sistema de control
de acceso
Imagen + enlace
DS1
Datos de invitación
DS2
Imagen + identificador + ID
Perfil del
visitante
DS3
Identificador
DS4
Imagen
DS5

Fig. 4