(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 769 127**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04W 4/02 (2008.01)
G07C 9/00 (2006.01)
H04W 4/021 (2008.01)
H04W 64/00 (2009.01)
H04W 4/029 (2008.01)
H04L 29/08 (2006.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2017 E 17188515 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.11.2019 EP 3291505**

(54) Título: **Mecanismo de seguridad multinivel para acceder a un panel**

(30) Prioridad:

02.09.2016 US 201615256372

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.06.2020

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road, M/S 4D3, P.O. Box 377
Morris Plains, NJ 07950, US

(72) Inventor/es:

MOHAN, RESHMA;
GAURAV, GALIB;
RAJKUMAR, MALATHY;
SAMPATHKUMAR, KARTHIC y
ANKIREDDY, VENKATA PRAKASH REDDY

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Mecanismo de seguridad multinivel para acceder a un panel

Antecedentes

La exposición se refiere a la seguridad y en particular a la seguridad de los teléfonos móviles.

Compendio

La presente invención se define mediante las reivindicaciones adjuntas.

La exposición muestra un panel asociado a mantener la seguridad de dispositivos móviles. Los dispositivos, por ejemplo, teléfonos móviles, se pueden registrar con códigos de usuario en el panel. Los números de los dispositivos móviles se pueden correlacionar con los códigos de usuario en el panel. Si un usuario quiere acceder al panel, el usuario puede entonces introducir un código de usuario correspondiente a un número de teléfono del dispositivo móvil. En este momento, el usuario puede estar autorizado para utilizar el dispositivo móvil. El dispositivo puede tener una aplicación de geolocalización en la que el panel puede realizar un seguimiento del dispositivo, en particular si el dispositivo se encuentra dentro de un rango predeterminado de una ubicación protegida. Si el usuario del dispositivo está autorizado para estar dentro del rango predeterminado, se puede efectuar otra comprobación acerca del usuario con una aplicación de reconocimiento facial que se ejecuta en un escaneo por parte del dispositivo de la cara del usuario y, a continuación, se puede comparar la imagen escaneada con una imagen de un usuario autorizado que el panel recupera y proporciona. Si se descubre que el usuario no está autorizado para utilizar el dispositivo móvil en cualquier instante a lo largo del proceso citado anteriormente, entonces se puede considerar al usuario como un intruso y se puede enviar una alerta a una estación central de monitorización, que puede adoptar medidas para eliminar cualquier amenaza asociada con el intruso.

Existe constancia de la técnica anterior relacionada con la seguridad de los dispositivos móviles que utilizan un panel a partir de los documentos US 9 141 150 B1 y US2016/0055698 A1.

Descripción breve de los dibujos

La figura 1 es un diagrama de la seguridad multinivel para el acceso a un panel por parte de un usuario de, por ejemplo, un dispositivo móvil;

la figura 2 es un diagrama de un registro de una lista de dispositivos móviles en correspondencia con los códigos de usuario en un panel de seguridad;

la figura 3 es un diagrama de los componentes que pueden estar involucrados cuando un intruso intenta acceder a un panel de seguridad; y

la figura 4 es un diagrama de una aplicación de reconocimiento facial tal como se implementa en un dispositivo móvil.

Descripción

El presente sistema y procedimiento pueden incorporar uno o más procesadores, ordenadores, controladores, interfaces de usuario, conexiones inalámbricas y/o cableadas y/o similares, en una implementación descrita y/o mostrada en la presente.

Esta descripción puede proporcionar uno o más ejemplos ilustrativos y específicos o maneras de implementar el presente sistema y procedimiento. Pueden existir numerosos ejemplos o maneras diferentes de implementación del sistema y procedimiento.

Algunos aspectos del sistema o procedimiento se pueden describir en términos de símbolos en el dibujo. Los símbolos pueden tener virtualmente cualquier forma (p. ej., un bloque) y pueden designar *hardware*, objetos, componentes, actividades, estados, pasos, procedimientos y otros elementos.

Los códigos de usuario para autentificar el acceso de seguridad pueden ser fáciles de reproducir y piratear. No se adoptan las medidas necesarias cuando una persona no autorizada intenta manipular el panel (tal como desarmar el panel) en ausencia de usuarios autorizados. Si el intruso pertenece a la familia (tal como una criada) y suplanta el código de usuario maestro, entonces se puede producir una vulnerabilidad de seguridad.

Introducir un nivel de seguridad extra para acceder al sistema de seguridad puede satisfacer una necesidad. La presente característica puede ser fácil de implementar utilizando interfaces de programación de aplicaciones de geolocalización (API) e integrarla en un sistema de seguridad existente.

El presente procedimiento puede involucrar un teléfono móvil que hace factible la presente solución. Los teléfonos

móviles pueden soportar una característica de geolocalización.

Las aplicaciones de protección/sistema de seguridad pueden tratar a cualquier usuario que introduzca un código de usuario válido como un usuario autorizado. Si un intruso intenta acceder al panel utilizando un código de usuario válido en ausencia del usuario autorizado, el presente procedimiento y solución pueden evitar un acceso e informan de la actividad ilegal al usuario y a una estación central de monitorización (CMS). El procedimiento puede involucrar añadir eficientemente una seguridad de dos niveles para garantizar una autentificación adecuada e impedir la suplantación de identidad.

El presente procedimiento puede indicar que los números de los teléfonos móviles de los usuarios deberían estar registrados en un panel en correspondencia con unos códigos de usuario particulares o únicos, respectivamente. Se puede añadir una geolocalización del teléfono móvil junto con la introducción de un código de usuario para autorizar a un usuario. Un panel puede necesitar una lista de números de teléfono móvil “amistoso” correlacionados con códigos de usuario de usuarios registrados del panel. Si el panel está en un estado armado (armado total y armado parcial) y se puede desarmar con un código de usuario válido, el panel puede realizar un seguimiento de la presencia de cualesquiera números de teléfono móvil “amistoso” en su proximidad utilizando un seguimiento basado en geolocalización. El seguimiento basado en geolocalización en el panel puede ayudar a la hora de realizar el seguimiento de números de teléfono amistoso dentro de un rango de, por ejemplo, aproximadamente veinte 20 metros (una distancia que se puede personalizar para cada panel) alrededor de las instalaciones protegidas. Si no hay coincidencias con relación a la lista de números de teléfono móvil amistoso, el usuario que accede al panel puede ser tratado como no autorizado o como un intruso. Se puede enviar una alerta a los números de teléfono móvil amistoso acerca de la presencia de intrusos. Tras la confirmación, se puede enviar una alerta a una estación central de monitorización (CMS). La CMS puede adoptar las medidas necesarias, tal como informar al personal de emergencias o a la policía. Este procedimiento puede ser una seguridad de dos niveles añadida eficientemente para garantizar una autentificación adecuada y ayudar a impedir la suplantación de identidad.

Un escenario puede involucrar al panel en un modo de armado total cuando no hay nadie en las instalaciones. Una vez que un usuario entra en las instalaciones, el panel puede identificar al usuario con la geolocalización del móvil del intruso. Si cualquier persona no autorizada comienza a desarmar el panel o si cualquier persona autorizada con menos privilegios intenta suplantar la identidad de un usuario con más privilegios (tal como la criada), el panel puede comprobar la presencia de números de móvil registrados en las instalaciones. Si no hay un usuario registrado en las instalaciones, el panel tratará a dicho usuario como un intruso. El panel puede capturar una imagen del intruso y enviar una notificación a todos los usuarios registrados del panel junto con una identidad del intruso. Si el intruso tiene un teléfono móvil, se puede guardar la identidad del teléfono móvil en el panel.

Los usuarios autorizados pueden confirmar la notificación o un mensaje. Un usuario puede tener un par de opciones. Una opción puede conllevar ser tratado como un “usuario conocido” o una de “monitorizar y enviar una notificación”. Si el usuario escoge la opción de “usuario conocido”, no se enviará necesariamente una alerta al CMS. Si el usuario escoge una opción de “monitorizar y enviar notificación”, se puede enviar una alerta al CMS, y el panel quedará establecido en un modo de máxima seguridad con todas las notificaciones e informaciones de eventos habilitadas. El CMS puede adoptar las medidas necesarias, tal como informar al personal de emergencia o a la policía junto con los detalles necesarios de la última opción. En el caso de que un propietario de una vivienda no responda a una alerta, incluso después de tres o más avisos, entonces se puede enviar una notificación al CMS que indique una entrada no autorizada o una suplantación de identidad.

Otro escenario puede incorporar una situación cuando un panel está en un modo de armado parcial con únicamente los sensores de perímetro activados. El panel puede tener en cuenta que ya hay móviles amistosos dentro del rango. Cuando se produce una situación de entrada no autorizada, en la que un intruso o una criada intenta suplantar la identidad de un usuario mediante el desarme con la utilización del código de usuario maestro, el panel puede hacer sonar una alerta audible con un anuncio acerca de la suplantación de identidad.

La figura 1 es un diagrama de un sistema y procedimiento para acceder a, por ejemplo, un panel de seguridad 12 con un dispositivo móvil 11. El panel de seguridad 12 puede tener una lista de dispositivos móviles o números de teléfono amistoso correlacionados con un conjunto de códigos de usuario. Cada número de teléfono móvil puede estar correlacionado con un código de usuario que es único frente a los demás códigos de usuario en el conjunto de códigos en el panel 12. Un usuario de un dispositivo móvil 11 puede intentar obtener acceso al panel 12. Con un código de acceso correcto el usuario puede tener éxito. Sin el código de usuario correcto el usuario puede no tener éxito y ser considerado un intruso. En el símbolo 13, se puede preguntar si el usuario obtuvo acceso al panel 12. Si la respuesta es negativa, entonces el usuario se puede considerar como un intruso 14. Si la respuesta es afirmativa, entonces el panel 11 puede geolocalizar el teléfono del usuario en el símbolo 15. Una determinación puede indicar si el usuario está geolocalizado dentro de un rango predeterminado de una ubicación protegida en el símbolo 15. Si la respuesta es negativa, el usuario aún podría ser un intruso 14. Si la respuesta es afirmativa, entonces puede ser importante verificar si el usuario es auténtico continuando con un reconocimiento facial en el símbolo 17. Una comparación de una cara escaneada del usuario se puede comparar con una cara de un usuario autorizado. Si una comparación de las caras revela que son diferentes, entonces el usuario puede ser un intruso 14. Si la comparación

revela que la cara escaneada y la cara del usuario autorizado son la misma, entonces el usuario se puede considerar un usuario autorizado.

En un diagrama de la figura 2, una solución puede incorporar registrar una lista de móviles 21 en correspondencia con unos códigos de usuario 22 en un panel de seguridad 23.

De acuerdo con un diagrama de la figura 3, un intruso 24 puede intentar introducir un código de usuario válido 25 en el panel 23. Un usuario con menos o pocos privilegios 26 puede intentar introducir un código de usuario maestro 27 en el panel 23. El panel 23 puede realizar un seguimiento de la presencia de cualquiera de los números de móvil "amistoso" en las proximidades del panel 23 utilizando un seguimiento basado en geolocalización a través de una conexión 28. Una lista de móviles registrados 29 puede no necesariamente estar en las instalaciones, tal como se indica en la conexión 31. Se puede enviar una alerta a números de móvil amistoso 29 acerca de la presencia de un intruso por medio de la conexión 32. Un usuario puede confirmar la alerta en la conexión 33 al panel 23. Tras una confirmación, se puede enviar una alerta a un CMS 34 por medio de la conexión 35. El CMS 34 puede adoptar las medidas necesarias, tal como informar a una unidad de emergencias o a la policía 36 por medio de la transmisión 37.

Se puede añadir reconocimiento facial al presente sistema, tal como se indica mediante un diagrama de la figura 4. Se puede suponer que un usuario pierde su teléfono móvil y el teléfono móvil se lo lleva una tercera persona, y si la tercera persona intenta acceder al panel de seguridad con un código correcto, se puede permitir que él o ella lo haga, ya que el teléfono móvil se encuentra a la distancia necesaria. Para solucionar este problema se puede añadir un paso más a la solución anterior (como los pasos secundarios de transmisión 28) donde una vez que el sistema de seguridad encuentra un teléfono móvil amistoso de ese usuario a la distancia necesaria, se puede activar una notificación para una aplicación de reconocimiento facial que se encuentra en ese teléfono móvil, en la cual es necesario que se autentifique el usuario. Si el usuario es un usuario verdadero, la aplicación de reconocimiento facial puede enviar un indicador afirmativo al sistema de seguridad o en caso contrario no enviar ningún indicador. Tras recibir el indicador afirmativo procedente de la aplicación móvil, el sistema de seguridad permitirá acceder a un usuario al sistema de seguridad (panel 23) o en caso contrario se informará a una estación central de monitorización (CMS). El sistema de seguridad puede ejecutar una aplicación de reconocimiento facial en el teléfono del usuario 38 por medio de la conexión 44. La cara del usuario se puede escanear utilizando la aplicación de reconocimiento facial 39 por medio de la conexión 42. La aplicación puede autentificar al usuario a través de la transmisión 43. Se puede enviar un resultado de la autentificación al panel de seguridad 23 a través de la conexión 44.

A modo de recapitulación, un mecanismo de acceso de seguridad puede incorporar un panel de seguridad, una estación central de monitorización, conectada al panel de seguridad, y uno o más teléfonos móviles. Cada uno del o de los teléfonos móviles puede tener un número de teléfono que esté registrado en el panel de seguridad con un código de usuario. El panel de seguridad puede estar en un estado armado, que se puede desarmar con un código de usuario desde un teléfono móvil que tenga el número de teléfono correlacionado con el código de usuario registrado en el panel de seguridad. Se puede proporcionar una aplicación de geolocalización a cada uno del o de los teléfonos móviles que esté registrado con su número de teléfono en correspondencia con un código de usuario en el panel de seguridad. La aplicación de geolocalización puede permitir que el panel de seguridad realice un seguimiento de la presencia de cada teléfono móvil dentro de un rango predeterminado alrededor de una instalación protegida.

Una persona puede desarmar y acceder al panel de seguridad con un teléfono móvil si la persona utiliza el código de usuario registrado en el panel de seguridad para el teléfono móvil.

Si el teléfono móvil que la persona utiliza para acceder al panel de seguridad no tiene un código de usuario registrado en el panel de seguridad, entonces el panel de seguridad puede tratar a la persona como una persona que llama no autorizada o un intruso.

Si la persona es tratada como una persona que llama no autorizada o un intruso, entonces se puede enviar una alerta, que indique que un intruso intenta acceder al panel de seguridad, al o a los teléfonos móviles que están registrados en el panel de seguridad de acuerdo con los códigos de usuario. Si un usuario del o de los teléfonos móviles confirma la alerta, entonces se puede enviar una segunda alerta sobre el intruso a la estación central de monitorización.

Tras la recepción de la segunda alerta, la estación central de monitorización puede adoptar medidas para eliminar cualquier amenaza asociada con el intruso.

Si una persona desarma y accede al panel de seguridad con un teléfono móvil y un código de usuario registrado en el panel de seguridad para ese teléfono móvil, y el teléfono móvil está presente dentro de un rango predeterminado alrededor de la instalación protegida, entonces el panel de seguridad puede ejecutar una comprobación de si la persona es un usuario auténtico con una aplicación de reconocimiento facial en el teléfono móvil.

Se puede escanear la cara de la persona que utiliza el teléfono móvil mediante la aplicación de reconocimiento

facial. La cara que se escanea se puede comparar con una cara de un usuario autorizado del teléfono móvil. Un resultado de una comparación de la cara que se escanea con la cara del usuario autorizado del teléfono móvil puede indicar si la persona es un intruso o el usuario autorizado del teléfono móvil.

Si la persona queda señalada como intruso con el teléfono móvil de acuerdo con el resultado de la comparación, entonces se puede enviar una alerta a la estación central de monitorización para adoptar medidas con el fin de eliminar cualquier amenaza asociada con la persona.

Un sistema de seguridad de dispositivos móviles multinivel puede incorporar un panel de seguridad, uno o más dispositivos móviles y una estación central de monitorización conectada al panel de seguridad. El o los dispositivos móviles pueden tener números que estén registrados en el panel de seguridad con códigos de usuario, respectivamente. Un número de móvil puede armar y puede desarmar el panel de seguridad que esté registrado con un código de usuario en el panel de seguridad. El panel de seguridad puede realizar el seguimiento del o de los teléfonos móviles que tienen números registrados con los códigos de usuario en el panel de seguridad, dentro de un rango predeterminado alrededor de una ubicación protegida.

El panel de seguridad puede contener una lista de números de dispositivo móvil amistoso que incorpore los números del o de los dispositivos móviles que tienen sus números registrados con códigos de usuario, respectivamente, en el panel de seguridad.

Si un dispositivo móvil está dentro del rango predeterminado y un número del dispositivo móvil no está en la lista de números de dispositivo móvil amistoso, entonces se puede considerar a un usuario del dispositivo móvil que accede al panel de seguridad como un usuario no autorizado y, por tanto, un intruso.

Tras considerar al usuario como un intruso se puede enviar una alerta sobre una presencia del intruso dentro del rango predeterminado a los números de la lista de números de dispositivo móvil amistoso.

Si el panel de seguridad recibe una confirmación a la alerta, entonces se puede enviar una alerta a una estación central de monitorización, que adopta medidas para eliminar al intruso o cualquier problema asociado con el intruso.

Si una persona, diferente a un usuario autorizado de un dispositivo móvil, accede al panel de seguridad con un código de usuario correcto del dispositivo móvil, y el dispositivo móvil está dentro del rango predeterminado, el panel de seguridad puede activar una notificación para una aplicación de reconocimiento facial que se encuentra en el dispositivo móvil con el fin de autentificar o no autentificar la persona como un usuario autorizado del dispositivo con un escaneo de la cara de la persona que utiliza el dispositivo móvil, que se compara con la cara del usuario autorizado del dispositivo móvil.

Si una comparación del escaneo de la cara de la persona que utiliza el dispositivo móvil con la cara del usuario autorizado da como resultado la no similitud de las dos caras, entonces se puede considerar a la persona que utiliza el dispositivo móvil como un intruso.

Un procedimiento para obtener un acceso autorizado a un panel de seguridad puede incorporar introducir un código de usuario para cada uno de uno o más teléfonos móviles en un panel de seguridad, que conecta una estación central de monitorización al panel de seguridad, correlacionar los números del o de los teléfonos móviles con los códigos de usuario en el panel de seguridad y añadir una aplicación de geolocalización a cada uno del o de los teléfonos móviles para que el panel de seguridad realice un seguimiento de un teléfono móvil de entre el o los teléfonos móviles.

El procedimiento puede incorporar además determinar si una persona que utiliza un teléfono móvil de entre el o los teléfonos móviles es un intruso.

Determinar si una persona que utiliza un teléfono móvil seleccionado de entre el o los teléfonos móviles es un intruso puede incorporar comprobar que el código de usuario introducido por la persona en el panel de seguridad se corresponde con un código de usuario que está correlacionado con un número de teléfono del teléfono móvil seleccionado en el panel de seguridad, y comprobar que una presencia del teléfono móvil seleccionado con la aplicación de geolocalización en el teléfono móvil seleccionado mediante el panel de seguridad está fuera de un rango predeterminado alrededor de una instalación protegida.

Determinar si una persona que utiliza un teléfono móvil seleccionado de entre el o los teléfonos móviles es un intruso puede incorporar además ejecutar una aplicación de reconocimiento facial en el teléfono móvil seleccionado. Se puede escanear la cara de la persona que utiliza el teléfono móvil seleccionado con la aplicación de reconocimiento facial. El panel de seguridad puede comparar la cara que se escanea con una cara de un usuario autorizado del teléfono móvil seleccionado. Un resultado de una comparación de la cara que se escanea con la cara de un usuario autorizado del teléfono móvil seleccionado puede indicar si la persona es un usuario autorizado del teléfono móvil seleccionado o un intruso.

Si la persona que utiliza el teléfono móvil seleccionado es un intruso, entonces el panel de seguridad puede transmitir un mensaje a la estación central de monitorización para eliminar cualquier amenaza asociada con la persona.

Cualquier publicación o documento de patente citado en la presente se incorpora por referencia a la presente en la misma medida que si se indicara de manera específica e individual que cada publicación o documento de patente se incorpora por referencia.

En la presente memoria descriptiva, parte del contenido puede tener naturaleza hipotética o profética aunque se exponga de otra manera o en otro tiempo gramatical.

Aunque el presente sistema y/o procedimiento se ha descrito con respecto a, al menos, un ejemplo ilustrativo, tras la lectura de la memoria descriptiva serán evidentes múltiples variaciones y modificaciones para aquellos que son expertos en la técnica. Por lo tanto, se pretende que las reivindicaciones adjuntas se interpreten de manera tan amplia como sea posible habida cuenta de que la técnica relacionada incluye todas esas variaciones y modificaciones.

REIVINDICACIONES

1. Un sistema de acceso de seguridad que comprende:

un panel de seguridad (23);

una memoria acoplada de manera operativa al panel de seguridad y configurada de modo que almacene una lista de códigos de usuario (22) y una lista de números de teléfono, donde cada código de usuario de la lista de códigos de usuario se corresponde con al menos un número de teléfono de la lista de números de teléfono:

una estación central de monitorización (34) conectada al panel de seguridad; y

uno o más teléfonos móviles (11, 38); y

donde:

cada uno del o de los teléfonos móviles tiene un número de teléfono que está registrado en el panel de seguridad con un código de usuario;

el panel de seguridad está en un estado armado, el cual se puede desarmar con un código de usuario desde un teléfono móvil que tenga el número de teléfono correlacionado con el código de usuario tal como está registrado en el panel de seguridad;

cada uno del o de los teléfonos móviles que está registrado con su número de teléfono en correspondencia con un código de usuario en el panel de seguridad está provisto de una aplicación de geolocalización; y

el panel de seguridad está configurado de modo que realice un seguimiento de la presencia de cada teléfono móvil dentro de un rango predeterminado alrededor de una instalación protegida utilizando un seguimiento basado en geolocalización mediante:

la recepción de un código de usuario introducido por una persona en el panel de seguridad;

la identificación del código de usuario en la lista de códigos de usuario;

el acceso a la lista de números de teléfono móvil;

la identificación de un número de teléfono en la lista de números de teléfono que está correlacionado con el código de usuario;

el escaneo del rango predeterminado alrededor de la instalación protegida en busca de un teléfono móvil que tiene el número de teléfono;

el desarme en respuesta a localizar el teléfono móvil que tiene el número de teléfono en el rango predeterminado alrededor de la instalación protegida; y

el envío de una alerta al o a los teléfonos móviles en respuesta a no localizar el teléfono móvil que tiene el número de teléfono en el rango predeterminado alrededor de la instalación protegida.

2. El sistema de la reivindicación 1, donde:

el panel de seguridad (23) está configurado de modo que una persona con un teléfono móvil (11, 38) lo desarme y acceda a este si la persona utiliza el código de usuario (22) del teléfono móvil registrado en el panel de seguridad;

si el teléfono móvil que la persona utiliza para acceder al panel de seguridad no tiene un código de usuario registrado en el panel de seguridad, entonces el panel de seguridad está configurado de modo que trate a la persona como una persona que llama no autorizada o un intruso (14);

si se trata a la persona como una persona que llama no autorizada o un intruso, entonces el panel de seguridad está configurado de modo que envíe una alerta indicando que un intruso intenta acceder al panel de seguridad al o a los teléfonos móviles que están registrados en el panel de seguridad de acuerdo con los códigos de usuario;

si un usuario del o de los teléfonos móviles confirma la alerta, entonces el panel de seguridad está configurado de modo que envíe una segunda alerta sobre el intruso a la estación central de monitorización (34); y tras la recepción de la segunda alerta, la estación central de monitorización está configurada para que adopte medidas para eliminar cualquier amenaza asociada con el intruso.

3. El sistema de la reivindicación 1, donde:

si una persona desarma y accede al panel de seguridad (23) con un teléfono móvil (11, 38) y un código de usuario (22) registrado en el panel de seguridad (23) para ese teléfono móvil, y el teléfono móvil está presente dentro del rango predeterminado alrededor de la instalación protegida, entonces el panel de seguridad está configurado de modo que ejecute una comprobación de si la persona es un usuario auténtico con una aplicación de reconocimiento facial (39) en el teléfono móvil;

donde la aplicación de reconocimiento facial está configurada de modo que escanee la cara de la persona utilizando el teléfono móvil, donde la aplicación de reconocimiento facial está configurada de modo que compare la cara que se escanea con la cara de un usuario autorizado del teléfono móvil;

donde la aplicación de reconocimiento facial está configurada de modo que envíe al panel de seguridad un resultado de una comparación de la cara que se escanea con la cara del usuario autorizado del teléfono móvil, que indica si la persona es un intruso (14) o el usuario autorizado del teléfono móvil; y

si la persona queda señalada como intruso con el teléfono móvil de acuerdo con el resultado de la comparación, entonces el panel de seguridad está configurado de modo que envíe una alerta a la estación central de monitorización (34) para adoptar las medidas necesarias con el fin de eliminar cualquier amenaza asociada con la persona.

4. Un sistema de seguridad de dispositivos móviles multinivel que comprende:

un panel de seguridad (23);

una memoria acoplada de manera operativa al panel de seguridad y configurada de modo que almacene una lista de códigos de usuario (22) y una lista de números de dispositivo móvil, donde cada código de usuario de la lista de códigos de usuario se corresponde con al menos un número de dispositivo móvil de la lista de números de móviles;

uno o más dispositivos móviles (11, 38); y

una estación central de monitorización (34) conectada al panel de seguridad; y

donde:

el o los dispositivos móviles tienen unos números de dispositivo móvil que están registrados en el panel de seguridad con códigos de usuario, respectivamente;

el panel de seguridad está armado y se puede desarmar mediante un número de dispositivo móvil que esté registrado con un código de usuario en el panel de seguridad; y

el panel de seguridad está configurado de modo que realice un seguimiento del o de los dispositivos móviles que tienen números de dispositivo móvil registrados con los códigos de usuario en el panel de seguridad, dentro de un rango predeterminado alrededor de una ubicación protegida mediante:

la recepción de un código de usuario introducido por una persona en el panel de seguridad;

el acceso a una lista de códigos de usuario en respuesta a la recepción del código de usuario;

la identificación del código de usuario en la lista de códigos de usuario;

el acceso a la lista de números de dispositivo móvil;

la identificación de un número de dispositivo móvil en la lista de números de dispositivo móvil que está registrado con el código de usuario;

el escaneo del dispositivo móvil que tiene el número de dispositivo móvil en el rango predeterminado alrededor de la ubicación protegida;

el desarme en respuesta a la localización del dispositivo móvil que tiene el dispositivo móvil en el rango predeterminado alrededor de la ubicación protegida; y

el envío de una alerta al o a los dispositivos móviles en respuesta a la no localización de dispositivos móviles que tienen el número de dispositivo móvil en el rango predeterminado alrededor de la ubicación protegida.

5. El sistema de la reivindicación 4, donde el panel de seguridad (23) está configurado de modo que contenga una lista de números de dispositivo móvil amistoso (29) que comprende los números de dispositivo móvil del o de los dispositivos móviles que tienen sus números de dispositivo móvil registrados con códigos de usuario en el panel de

seguridad, respectivamente.

6. El sistema de la reivindicación 5, donde:

si un dispositivo móvil (11, 38) está dentro del rango predeterminado y el número del dispositivo móvil no se encuentra en la lista de números de dispositivo móvil amistoso, entonces el panel de seguridad (23) está configurado de modo que considere a un usuario del dispositivo móvil que accede al panel de seguridad (23) como un usuario no autorizado y, por tanto, un intruso (14);

tras considerar al usuario como un intruso, el panel de seguridad (23) está configurado de modo que envíe una alerta sobre una presencia del intruso dentro del rango predeterminado a los números de la lista de números de dispositivo móvil amistoso (29); y

si el panel de seguridad recibe una confirmación a la alerta, entonces el panel de seguridad (23) está configurado de modo que envíe una alerta a una estación central de monitorización (34), que está configurada de modo que adopte medidas para eliminar el intruso o cualquier problema asociado con el intruso.

7. El sistema de la reivindicación 6, donde:

si una persona, diferente a un usuario autorizado de un dispositivo móvil, accede al panel de seguridad (23) con un código de usuario correcto (22) del dispositivo móvil (11, 38), y el dispositivo móvil está dentro del rango predeterminado, el panel de seguridad está configurado de modo que active una notificación para una aplicación de reconocimiento facial (30) que se encuentra en el dispositivo móvil con el fin de autentificar o no autentificar la persona como un usuario autorizado del dispositivo con un escaneo de la cara de la persona que utiliza el dispositivo móvil, que se compara con la cara del usuario autorizado del dispositivo móvil; y

si una comparación del escaneo de la cara de la persona que utiliza el dispositivo móvil con la cara del usuario autorizado da como resultado una no similitud de las dos caras, entonces el sistema está configurado de modo que considere a la persona que utiliza el dispositivo móvil como un intruso (14).

8. Un método para obtener acceso autorizado a un panel de seguridad (23), que comprende:

almacenar un código de usuario (22) para cada uno de uno o más teléfonos móviles (11, 38) en un panel de seguridad;

conectar una estación central de monitorización (34) al panel de seguridad;

correlacionar los números de teléfono móvil del o de los teléfonos móviles con los códigos de usuario en el panel de seguridad; y

añadir una aplicación de geolocalización a cada uno del o de los teléfonos móviles para realizar un seguimiento de un teléfono móvil de entre el o los teléfonos móviles mediante el panel de seguridad, donde realizar un seguimiento del teléfono móvil mediante el panel de seguridad (23) incluye:

recibir un código de usuario introducido por una persona en el panel de seguridad (23);

acceder a una lista de códigos de usuario en respuesta a la recepción del código de usuario;

identificar el código de usuario en la lista de códigos de usuario;

acceder a una lista de números de teléfono móvil;

identificar un número de teléfono móvil en la lista de números de teléfono móvil que se corresponde con el código de usuario;

escanear un rango geográfico del teléfono móvil que tiene un número correspondiente al número de teléfono móvil;

permitir el acceso en respuesta a localizar el teléfono móvil que tiene el número en el rango geográfico; y

enviar una alerta a uno o más teléfonos móviles en respuesta a no localizar el teléfono móvil que tiene el número en el rango geográfico.

9. El método de la reivindicación 8, que comprende además, en el panel de seguridad: enviar una segunda alerta a una estación central de monitorización (34) en respuesta a la recepción de una orden para enviar una notificación desde al menos un teléfono móvil (11, 38) de entre el o los teléfonos móviles.

10. El método de la reivindicación 8, que comprende, en el panel de seguridad:

enviar una notificación al teléfono móvil para escanear la cara de un usuario y determinar si el usuario es un usuario verdadero del teléfono móvil, en respuesta a la localización del teléfono móvil que tiene el número en el rango geográfico;

permitir el acceso en respuesta a la recepción de una confirmación de autentificación desde el teléfono móvil que el usuario es un usuario verdadero; y

enviar la alerta al o a los teléfonos móviles en respuesta a la no recepción de la confirmación de autentificación desde el teléfono móvil que el usuario es el usuario verdadero.

FIG. 1

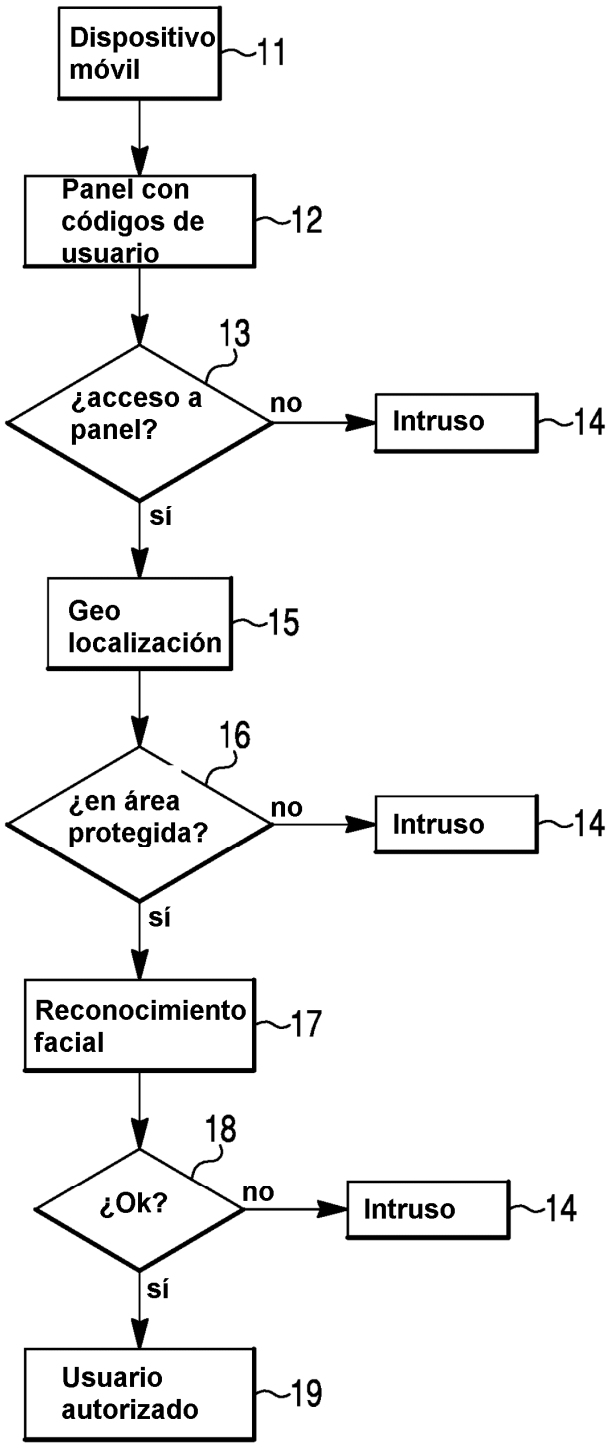
Dispositivo móvil
11
Panel con códigos de usuario
12
13
¿acceso a panel?
no
Intruso
14
sí
Geo localización
15
16
¿en área protegida?
no
Intruso
14
sí
Reconocimiento facial
17
18
¿Ok?
no
Intruso
14
sí
Usuario autorizado
19

FIG. 2

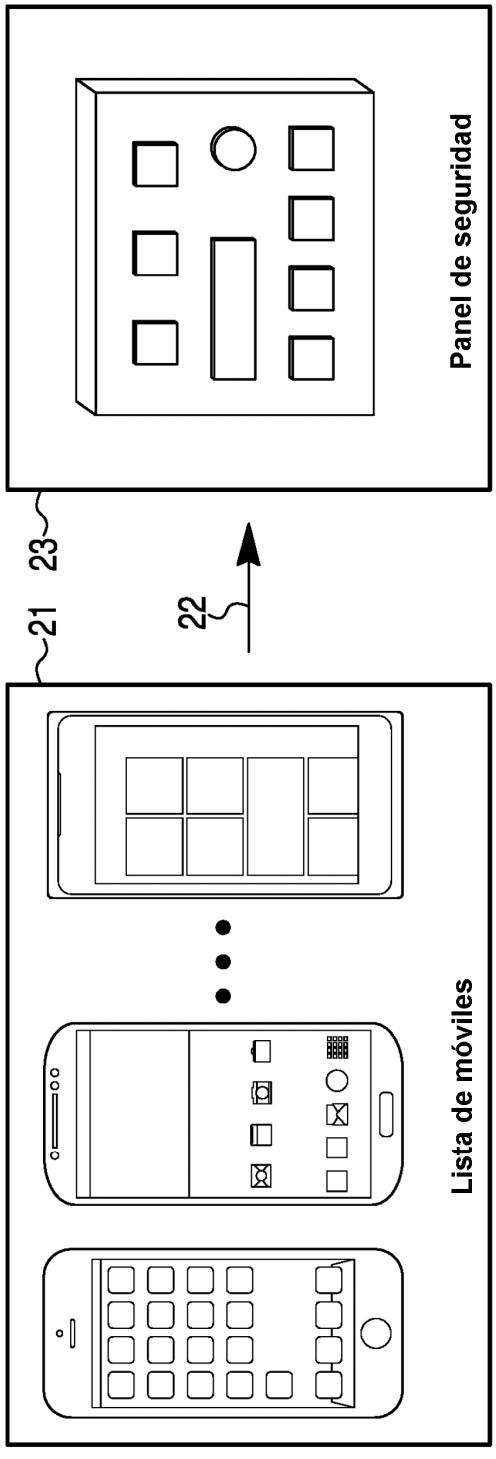

FIG. 3

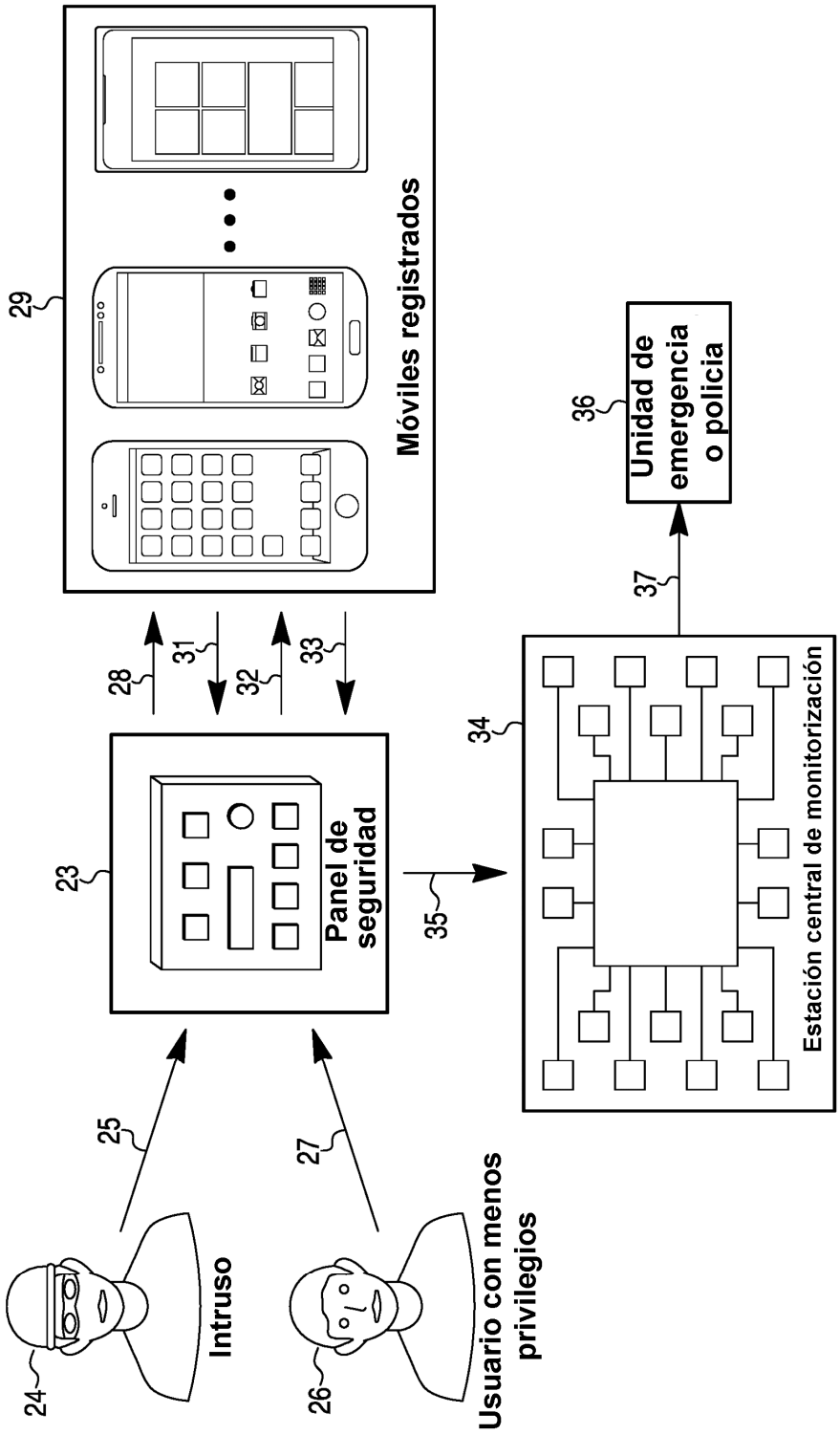
Móviles registrados
29
Unidad de emergencia o policía
36
37
Estación central de monitorización
34
Panel de seguridad
23
28
31
32
33
35
25
27
Intruso
24
Usuario con menos privilegios
26

FIG. 4