

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 431 667**

51 Int. Cl.:

**G08B 25/00** (2006.01)

**G08B 13/196** (2006.01)

**G08B 25/04** (2006.01)

**H04N 7/18** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **25.04.2007 E 07742371 (3)**

97 Fecha y número de publicación de la concesión europea: **31.07.2013 EP 2037426**

54 Título: **Dispositivo y método para detectar una actividad sospechosa, programa y medio de grabación**

30 Prioridad:

**31.05.2006 JP 2006152582**

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

**27.11.2013**

73 Titular/es:

**NEC CORPORATION (100.0%)  
7-1, Shiba 5-chome Minato-ku  
Tokyo 108-8001, JP**

72 Inventor/es:

**ISHIDERA, EIKI**

74 Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

ES 2 431 667 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

**DESCRIPCIÓN**

Dispositivo y método para detectar una actividad sospechosa, programa y medio de grabación

5 Campo técnico

La presente invención se refiere a una tecnología de vigilancia, en particular a un aparato y un método de detección de actividad sospechosa, actividad anómala y actividad prohibida utilizando un sensor de autenticación y una imagen por cámara.

10 Antecedentes de la técnica

Hasta la fecha se han propuesto muchos métodos para emitir automáticamente una alarma mediante la detección de una persona o un vehículo a partir de una imagen tomada mediante una cámara y el análisis de sus actividades.

15 Las técnicas específicas para llevar a cabo el método descrito anteriormente incluyen, por ejemplo, una técnica dada a conocer en el documento no de patente número 2 ("A System for Video Surveillance and Monitoring", informe técnico CMU-RI-TR-00-12, Robotics Institute, Carnegie Mellon University, mayo de 2000) y una técnica utilizada en el producto denominado VEW, de ObjectVideo, Inc.

20 De acuerdo con estas técnicas, es posible emitir una alarma mediante el recurso de detectar automáticamente una actividad ilegal o una actividad prohibida, tal como cuando una persona o un vehículo invaden una zona indicada como de acceso prohibido, y cuando una persona o un vehículo atraviesan una línea divisoria que dicha persona o dicho vehículo tienen prohibido atravesar.

25 Sin embargo, estas técnicas tienen el problema de que se emitirá una alarma de actividad prohibida o actividad ilegal incluso para una persona o un vehículo que tienen autorización, igual que en el caso de una persona ordinaria y un vehículo, por ejemplo, cuando una persona pertinente autorizada entra en una zona de "acceso prohibido sin autorización" o entra en el área de "acceso prohibido sin autorización", cuando una ambulancia entra en un cruce teniendo el semáforo en rojo, y similares.

30 Por otra parte, se conocen diversas formas de utilización de RFID (Radio Frequency IDentification, identificación por radiofrecuencia) como dispositivo de autenticación y están siendo aplicadas, por ejemplo, en el control de entrada y salida en el que la autorización para acceder a un edificio u oficina es autenticada mediante RFID y la puerta se abre para admitir a una persona o un vehículo que han sido autenticados como teniendo autorización para acceder por dicha puerta.

35 Además, cuando el objetivo es únicamente el personal, se conocen asimismo métodos que utilizan autenticación biométrica en base a características de la cara, de huellas digitales, de las venas o del iris.

40 Sin embargo, en un sistema de vigilancia que utiliza únicamente RFID, puesto que la ausencia de una respuesta RFID es equivalente a la ausencia de evento, existe el problema de que no puede conseguirse una función de vigilancia suficiente salvo que todo el personal sea monitorizado transportando una RFID consigo, y por lo tanto el rango de aplicación de dicho sistema está limitado.

45 Resulta difícil conseguir un sistema de vigilancia eficaz utilizando únicamente RFID, en particular en una zona o área pública, tal como el vestíbulo de un edificio, una estación ferroviaria, un aeropuerto, etc., donde hay muchas personas que no llevan consigo una RFID.

50 Además, existe un problema similar incluso en el caso de la autenticación biométrica, y es necesario soportar un entorno o una situación en la que todo el personal a monitorizar pueda ser autenticado, lo que tiene como resultado una gran carga de gestión de datos.

55 Además, existe asimismo el problema de que no es posible realizar el análisis detallado de una persona o de un vehículo a monitorizar, solamente mediante autenticación RFID o biométrica, en la que solamente es posible llevar a cabo una vigilancia gruesa, tal como monitorizar en qué momento y a través de qué puerta ha accedido la persona o el vehículo, y en qué momento y en qué lugar está presente la persona o el vehículo, y similares.

60 Por ejemplo, el documento de patente 1 (patente japonesa abierta a la inspección pública número 2004-127142) da a conocer un método en el que la validez de una persona que entra en un espacio predeterminado es determinada mediante el recurso de autenticar a una persona que tiene autorización para entrar/en utilizar dicho espacio, utilizando una tarjeta IC y similares; sin embargo, esta técnica tiene un problema consistente en que solamente es posible determinar la validez de la entrada de una persona particular en un lugar particular, y no es posible determinar la validez de la actividad de una persona o vehículo particulares en un lugar particular.

65 El documento de patente número 2 (patente japonesa abierta a la inspección pública número 2005-11057) da a conocer un método en el que se mejora la precisión combinando una vigilancia por imágenes y una vigilancia por sensores, tal como RFID.

De acuerdo con la técnica del documento de patente 2, es posible obtener información dinámica detallada del una persona o un objeto, etc., la cual no puede ser reconocida solamente mediante información de imágenes tomada por una cámara, etc.

5 Además, de acuerdo con la técnica del documento de patente 2, puesto que se supone que cada persona posee una etiqueta RFID en una ubicación tal como un lugar corporativo, cuando se detecta una persona pero no existe respuesta de RFID, es posible considerar a dicha persona como sospechosa emitiendo por lo tanto una alarma.

10 Sin embargo, dado que esta técnica solamente utiliza la información simplemente acerca de si un sujeto a monitorizar posee o no una etiqueta RFID o un terminal GPS, y no autentica a un sujeto que tiene autorización, resulta difícil llevar a cabo un control preciso de alarmas tal como el siguiente.

15 Es decir, existe un problema consistente en que se emite erróneamente una alarma incluso para una persona que tiene autorización, debido a la ausencia de aplicación de políticas precisas de vigilancia correspondientes a esta autorización, tales como: cuando una persona está autorizada para entrar en cualquier lugar, la persona queda excluida del objeto a monitorizar y no se emitirá la alarma; cuando se permite a una persona entrar solamente en un área específica, la entrada a un área no permitida se considerará como una actividad ilegal, y se emitirá una alarma; cuando una persona no tiene permitida la entrada en absoluto o no posee una etiqueta RFID, ha de generarse la alarma en cuanto dicha persona es detectada; incluso cuando una persona que se desplaza en sentido opuesto es detectada en una trayectoria en la que el desplazamiento en sentido opuesto está prohibido, no se emitirá una alarma si la persona tiene una autorización específica para desplazarse en sentido opuesto; incluso cuando una persona que está quieta es detectada en una trayectoria en la que está prohibido permanecer quieto, no se emitirá una alarma si la persona tiene autorización específica para permanecer quieta.

25 Documento de patente 1: patente japonesa abierta a la inspección pública número 2004-127142,  
Documento de patente 2: patente japonesa abierta a la inspección pública número 2005-11057,  
Documento no de patente 2: "A System for Video Surveillance and Monitoring", informe técnico CMU-RI-TR-00-12, Robotics Institute, Carnegie Mellon University, mayo de 2000.

30 Descripción de la Invención

En la técnica dada a conocer en el documento no de patente 2, existe un problema consistente en que incluso cuando una persona o un vehículo tienen una autorización, se emite una alarma que indica una actividad prohibida o violación, del mismo modo que en el caso de una persona o vehículo ordinarios.

35 En un sistema de vigilancia que utiliza solamente RFID, puesto que la ausencia de respuesta RFID es equivalente al hecho de que no exista evento, no puede conseguirse una función de vigilancia suficiente salvo que todos los sujetos a monitorizar lleven consigo una RFID, provocando por lo tanto el problema de que el rango de aplicación de dicho sistema está limitado. Lo mismo puede decirse del caso de autenticación biométrica, y por lo tanto es necesario soportar un entorno en el que todos los sujetos a monitorizar puedan ser autenticados, imponiendo por lo tanto una gran carga en la gestión de datos.

40 Además, existe asimismo el problema de que no es posible realizar el análisis detallado de una persona o de un vehículo a monitorizar, solamente mediante autenticación RFID o biométrica, en la que solamente es posible llevar a cabo una vigilancia gruesa, tal como monitorizar en qué momento y a través de qué puerta ha accedido la persona o el vehículo, y en qué momento y en qué lugar está presente la persona o el vehículo, y similares.

45 Dado que la técnica dada a conocer en el documento de patente 2 solamente utiliza la información sobre si un sujeto a monitorizar simplemente posee o no una etiqueta RFID o un terminal GPS, y no autentica a un sujeto a monitorizar que tiene autorización, no resulta posible aplicar políticas de vigilancia precisas correspondientes a la autorización, causando por lo tanto el problema de que puede emitirse erróneamente una alarma incluso para una persona que tiene una autorización.

50 Es un objetivo de la presente invención solucionar los problemas descritos anteriormente y dar a conocer un aparato y un método de detección de actividad sospechosa que posibiliten analizar de manera precisa la actividad de una persona o de un vehículo a monitorizar incluso sin asumir una situación en la que todo el personal y los vehículos a monitorizar lleven consigo una RFID o en la que estos pueden estar sujetos a autenticación biométrica, y detectar automáticamente una actividad ilegal y una actividad prohibida para generar una alarma pero sin emitir una alarma innecesaria si la actividad está dentro del intervalo de autorización proporcionado a la persona o al vehículo a monitorizar.

55 La presente invención da a conocer un aparato de detección de actividad sospechosa para detectar actividad sospechosa utilizando medios de generación de señal, un sensor para recibir una señal de dichos medios de generación de señal, y una imagen tomada por una cámara, que comprende:

60

una sección de entrada de imágenes adaptada para capturar datos de imagen de dicha cámara y para emitir dichos datos de imagen;

una sección de análisis de la actividad adaptada para detectar un objeto móvil tal como una persona y un vehículo incluidos en una imagen indicada mediante los datos de imagen procedentes de dicha sección de entrada de imágenes, reconocer si el objeto móvil detectado es una persona, un vehículo u otra entidad diferente a estos, obtener la posición del objeto detectado, y extraer además una trayectoria del movimiento del objeto detectado, para emitir la información así obtenida como información de actividad del objeto móvil;

una sección de entrada de información de autenticación adaptada para obtener un número de ID indicado en dicha señal recibida mediante dicho sensor, un tiempo de recepción y una posición de recepción de dicha señal mediante la salida de dicho sensor, y emitir la información así obtenida como información de autenticación;

una sección de autenticación de la autorización adaptada para almacenar información de autorización correspondiente a dicha información de autenticación, obtener información de autorización correspondiente a la información de autenticación introducida desde dicha sección de entrada de información de autenticación y emitir dicha información de autenticación introducida con dicha información de autorización obtenida añadida a la misma;

una sección de integración de la información adaptada para poner la información de autenticación complementada con información de autorización introducida desde dicha sección de autenticación de la autorización, en correspondencia con información de actividad del objeto móvil introducida desde dicha sección de análisis de la actividad, y emitir la información de actividad del objeto móvil con la información de autorización añadida a la misma;

una sección de determinación de la actividad adaptada para incluir una lista de actividades permitidas y actividades prohibidas dependiendo del nivel de autorización, reconocer una actividad de violación y una actividad prohibida predeterminadas haciendo referencia a dicha lista, con respecto al nivel de autorización añadido a la información de actividad del objeto móvil introducida desde dicha sección de integración de la información, y tras la detección de que la actividad indicada mediante la información de actividad del objeto móvil es una actividad ilegal o una actividad prohibida, generar y emitir la información de alarma; y

una sección de salida adaptada para emitir una alarma cuando recibe información de alarma procedente de dicha sección de determinación de la actividad;

caracterizado por que:

dicha sección de determinación de la actividad está adaptada además para, cuando existe información de autenticación en la sección de determinación de la actividad que no está en correspondencia con ninguna información de actividad del objeto móvil, crear información de actividad del objeto móvil provisional para ponerla en correspondencia con dicha información de autenticación, y asumir el nivel de autorización de la misma como estando al mínimo nivel.

En este caso, cuando se introduce información de actividad del objeto móvil que no corresponde con ninguna información de autenticación, dicha sección de determinación de la actividad puede adaptarse para asumir que el nivel de autorización con respecto a la información de actividad del objeto móvil está al mínimo nivel.

La sección de autenticación de la autorización puede adaptarse para almacenar una plantilla de un uniforme o de ropa; y está configurada para obtener una imagen parcial de una persona haciendo referencia a la posición de dicha persona a partir de la información de actividad del objeto móvil procedente de dicha sección de análisis de la actividad, está configurada para comparar dicha imagen parcial con el uniforme o la ropa almacenados en dicha plantilla; y cuando existe un uniforme o ropa cuya similitud es mayor que un umbral predeterminado, está configurada para obtener información de autenticación introducida desde dicha sección de entrada de información de autenticación con información acerca del uniforme o la ropa siendo la información de autenticación, o está configurada para obtener información de autorización correspondiente a información de reconocimiento que es información acerca del uniforme y de la ropa, y está configurada para emitir la información de autenticación introducida con dicha información de autorización añadida a la misma.

En este caso, cuando se introduce información de actividad del objeto móvil que no corresponde con ninguna información de autenticación, dicha sección de autenticación de la autorización puede configurarse para establecer el nivel de autorización con respecto a la información de actividad del objeto móvil al nivel mínimo.

La lista de actividades permitidas y actividades prohibidas en dicha sección de determinación de la actividad puede variar en función del tiempo.

La sección de determinación de la actividad puede configurarse para aplicar una autorización, que ha sido añadida a un elemento de información de actividad del objeto móvil, a otro elemento de información de actividad del objeto móvil.

La invención da a conocer asimismo un método de detección de actividad sospechosa llevado a cabo en un aparato de detección de actividad sospechosa que comprende una sección de entrada de imágenes, una sección de análisis de la actividad, una sección de entrada de información de autenticación, una sección de autenticación de la

autorización, una sección de integración de la información, una sección de determinación de la actividad y una sección de salida, detectando dicho aparato de detección de actividad sospechosa una actividad sospechosa mediante la utilización de un medio de generación de señal, un sensor para recibir una señal procedente de dicho medio de generación de señal y una imagen tomada mediante una cámara, en el que  
 5 dicha sección de entrada de imágenes captura datos de imagen procedentes de dicha cámara y emite dichos datos de imagen;

dicha sección de análisis de la actividad detecta un objeto móvil, tal como una persona y un vehículo incluido en una imagen indicada mediante datos de imagen procedentes de dicha sección de entrada de imágenes, reconoce si el objeto móvil detectado es una persona, un vehículo u otra entidad, obtiene la posición del objeto detectado y extrae  
 10 además una trayectoria del movimiento del objeto detectado para emitir la información así obtenida como información de actividad del objeto móvil;

dicha sección de entrada de información de autenticación obtiene un número de ID indicado en dicha señal recibida mediante dicho sensor, un tiempo de recepción y una posición de recepción de dicha señal mediante la salida de dicho sensor, y emite la información así obtenida como información de autenticación;

15 dicha sección de autenticación de la autorización almacena información de autorización correspondiente a dicha información de autenticación; obtiene información de autorización correspondiente a la información de autenticación introducida desde dicha sección de entrada de información de autenticación y emite la información de autenticación introducida con dicha información de autorización obtenida añadida a la misma;

dicha sección de integración de la información pone información de autenticación complementada con información de autorización introducida desde dicha sección de autenticación de la autorización, en correspondencia con información de actividad del objeto móvil introducida desde dicha sección de análisis de la actividad, y emite la información de actividad del objeto móvil con la información de autorización añadida a la misma;

dicha sección de determinación de la actividad incluye una lista de actividades permitidas y actividades prohibidas en función del nivel de autorización, reconoce una actividad de violación o una actividad prohibida predeterminadas haciendo referencia a dicha lista, con respecto al nivel de autorización añadido a la información de actividad del objeto móvil introducida desde dicha sección de integración de la información, y al detectar que la actividad indicada mediante la información de actividad del objeto móvil es una actividad ilegal o una actividad prohibida, genera y emite información de alarma; y

30 dicha sección de salida emite una alarma cuando recibe información de alarma desde dicha sección de determinación de la actividad; caracterizado por que:

cuando existe información de autenticación en la sección de determinación de la actividad que no está en correspondencia con ninguna información de actividad del objeto móvil, dicha sección de determinación de la actividad crea información de actividad del objeto móvil provisional poniéndola en correspondencia con dicha información de autenticación, y asume que el nivel de autorización de la misma está al nivel mínimo.

La sección de autenticación de la autorización puede almacenar una plantilla de uniforme o de ropa; obtener una imagen parcial de una persona haciendo referencia a la posición de la persona a partir de información de actividad del objeto móvil procedente de dicha sección de análisis de la actividad; comparar dicha imagen parcial con el uniforme o la ropa almacenados en dicha plantilla; y cuando existe un uniforme o ropa cuya similitud es mayor que un umbral predeterminado, obtener información de autenticación introducida desde dicha sección de entrada de información de autenticación con información acerca del uniforme o la ropa siendo la información de autenticación, u obtener información de autorización correspondiente a información de reconocimiento que es información acerca del uniforme o la ropa, para emitir la información de autenticación introducida con dicha información de autorización añadida a la misma.

En este caso, cuando se introduce la información de actividad del objeto móvil que no corresponde con ninguna información de autenticación, dicha sección de autenticación de la autorización puede configurar el nivel de autorización con respecto a la información de actividad del objeto móvil al nivel mínimo.

La lista de actividades permitidas y actividades prohibidas en dicha sección de determinación de la actividad puede variar en función del tiempo.

La invención da a conocer asimismo un programa o un medio de grabación o soporte de registro que almacena dicho programa, el cual hace que el sistema informático ejecute el proceso llevado a cabo en cada componente del método descrito anteriormente.

#### Breve descripción de los dibujos

La figura 1 es un diagrama de flujo de un lector gráfico según un ejemplo de realización;

la figura 2 es un diagrama de flujo del esquema de lectura de gráficos según el ejemplo de realización;

la figura 3 es un diagrama de bloques del lector gráfico según el ejemplo de realización;

la figura 4 muestra un ejemplo en el que una imagen de cámara es transformada en coordenadas en un mapa;

la figura 5 muestra un ejemplo de la posición según la información de actividad del objeto móvil obtenida a partir de una imagen de cámara;

la figura 6 muestra un ejemplo del intervalo de estimación de la posición según la información de autenticación obtenida a partir de un sensor RFID;  
 la figura 7 muestra un ejemplo que indica la posición de acuerdo con la información de actividad del objeto móvil y la posición del sensor de autenticación representadas mediante las coordenadas en un mapa en el tiempo "t";  
 la figura 8 muestra un ejemplo que indica la posición de acuerdo con la información de actividad del objeto móvil y la posición de acuerdo con la información de autenticación representadas mediante las coordenadas en un mapa en el tiempo "t+1";  
 la figura 9 muestra un ejemplo de una imagen de cámara obtenida fotografiando una trayectoria en un aeropuerto con tráfico en un solo sentido;  
 la figura 10 muestra un ejemplo de una imagen de cámara que muestra una fotografía de un andén de una estación; y  
 la figura 11 muestra un ejemplo de información de objetos móviles, información de autenticación y un área de "acceso prohibido sin autorización" detectadas en un andén de una estación.

Descripción de los símbolos

11	Sección de entrada imágenes
12	Sección de análisis de la actividad
13	Sección de entrada de información de autenticación
14	Sección de autenticación de la autorización
15	Sección de integración de la información
16	Sección de determinación de la actividad
17	Sección de salida
21	Proceso de entrada de imágenes
22	Proceso de análisis de la actividad
23	Proceso de entrada de información de autenticación
24	Proceso de autenticación de la autorización
25	Proceso de integración de la información
26	Proceso de determinación de la actividad
27	Proceso de salida

Mejor modo de llevar a cabo la Invención

A continuación, se describirán realizaciones ejemplares haciendo referencia a las figuras.

La figura 1 es un diagrama de bloques para mostrar la configuración de un ejemplo de realización de un lector gráfico de acuerdo con la presente invención.

El ejemplo de realización incluye, tal como se muestra en la figura, la sección 11 de entrada de imágenes, la sección 12 de análisis de la actividad, la sección 13 de entrada de información de autenticación, la sección 14 de autenticación de la autorización, la sección 15 de integración de la información, la sección 16 de determinación de la actividad, la sección de salida 17; y cada una de estas secciones ejecuta el proceso 21 de entrada de imágenes, el proceso 22 de análisis de la actividad, el proceso 23 de entrada de la información de autenticación, el proceso 24 de autenticación de la autorización, el proceso 25 de integración de la información, el proceso 26 de determinación de la actividad y el proceso de salida 27 mostrados en la figura 2.

La sección 11 de entrada de imágenes, que puede fabricarse fácilmente mediante una cámara CCD normal y una memoria, captura datos de imagen que indican una imagen tomada mediante una cámara, etc., y los emite a la sección 12 de análisis de la actividad.

La sección 12 de análisis de la actividad que ha detectado un objeto móvil (imagen), tal como una persona y un vehículo incluidos en una imagen indicada mediante datos de imagen introducidos desde la sección 11 de entrada de imágenes, reconoce si el objeto móvil detectado es una persona, un vehículo o alguna otra entidad, obtiene la posición del objeto detectado, y extrae además una trayectoria del movimiento del objeto detectado para emitir la información así obtenida a la sección 15 de integración de la información como información de actividad del objeto móvil.

La sección 13 de entrada de información de autenticación, que puede fabricarse fácilmente a partir de un lector RFID normal, una memoria y medio de control (CPU), obtiene un número ID de una persona o un vehículo, y el tiempo y la posición en los que el número ID es leído con un sensor (no mostrado), y emite como información de autenticación la información así obtenida a la sección 14 de autenticación de la autorización.

La sección 14 de autenticación de la autorización, que incluye medios de almacenamiento para almacenar información de autenticación e información de autorización correspondiente, obtiene la información de autorización correspondiente a la información de autenticación procedente de la sección 13 de entrada de información de autenticación, y emite a la sección 15 de integración de la información la información de autenticación introducida con la información de autorización obtenida incorporada a la misma.

- 5 Debe observarse que para la sección 13 de entrada de la información de autenticación, es posible asimismo utilizar, por ejemplo, autenticación mediante caras, huellas digitales, venas y ropa, y autenticación mediante etiquetas ID ópticas o teléfonos portátiles equipados con GPS, etc. Cuando se utiliza autenticación mediante cara, iris y ropa o una etiqueta ID óptica, la sección 13 de entrada de la información de autenticación puede fabricarse fácilmente mediante una cámara CCD ordinaria, una memoria y una CPU. Cuando se utiliza autenticación mediante huellas digitales, ésta puede fabricarse fácilmente mediante un sensor de huellas digitales ordinario, una memoria y una CPU. Cuando se utiliza autenticación mediante venas, ésta puede fabricarse fácilmente mediante un sensor de venas ordinario, una memoria y una CPU.
- 10 Además, para la sección 13 de entrada de información de autenticación, es posible asimismo utilizar un GPS ordinario y un terminal portátil con GPS, tal como un teléfono portátil equipado con GPS, etc.
- 15 La sección 15 de integración de la información pone la información de autenticación complementada con información de autorización que es introducida desde la sección 14 de autenticación de la autorización, en correspondencia con la información de actividad del objeto móvil introducida desde la sección 12 de análisis de la actividad, y emite la información de actividad del objeto móvil con la información de autorización añadida a la misma, a la sección 16 de determinación de la actividad.
- 20 La sección 16 de determinación de la actividad, que incluye una lista de actividades permitidas y actividades prohibidas en función de autorizaciones, reconoce una actividad de violación y una actividad prohibida predeterminadas haciendo referencia a la lista mencionada, con respecto a la autorización añadida a la información de actividad del objeto móvil entregada desde la mencionada sección 15 de integración de la información, y cuando se detecta que la actividad indicada mediante la información de actividad del objeto móvil es una actividad ilegal o una actividad prohibida, genera y emite información de alarma a la sección de salida 17.
- 25 La sección de salida 17 emite una alarma cuando recibe información de alarma desde la sección 16 de determinación de la actividad.
- 30 La sección 12 de análisis de la actividad, la sección 14 de autenticación de la autorización, la sección 15 de integración de la información, la sección 16 de determinación de la actividad y la sección de salida 17 pueden fabricarse fácilmente en un ordenador o un terminal PDA ordinarios.
- 35 En el proceso 22 de análisis de la actividad que se lleva a cabo en la sección 12 de análisis de la actividad, se detecta un objeto móvil a partir de una imagen, y se reconoce si el objeto móvil es una persona, un vehículo o alguna otra entidad, se obtiene la posición del objeto móvil, se extrae una trayectoria del movimiento del objeto móvil, y se obtiene asimismo información temporal para crear la información de actividad del objeto móvil.
- 40 Como algoritmo para detectar un objeto móvil, es posible utilizar un algoritmo basado, por ejemplo, en el método descrito en "A System for Video Surveillance and Monitoring", informe técnico CMU-RI-TR-00-12, Robotics Institute, Carnegie Mellon University, mayo de 2000, tal como un algoritmo para reconocer si el objeto móvil detectado es una persona, un vehículo o alguna otra entidad, y un algoritmo para obtener la posición del objeto móvil y para extraer la trayectoria del movimiento del mismo en el proceso 22 de análisis de la actividad que se lleva a cabo en la sección 12 de análisis de la actividad.
- 45 La información de actividad del objeto móvil puede obtenerse, como información en serie cronológica, información tal como, por ejemplo, información temporal, el rectángulo que circunscribe un objeto móvil en una imagen e información en la que el resultado del reconocimiento de un objeto móvil es una persona, un vehículo o alguna otra entidad.
- 50 Además, utilizando una cámara que ha sido sometida a una calibración de la cámara para correlacionar coordenadas universales reales con las coordenadas de la imagen de la cámara, y utilizando un mapa del entorno de la posición en la que está instalada la cámara, es posible obtener valores que se obtienen transformando las coordenadas de una posición de un objeto móvil en una imagen en coordenadas de un mapa.
- 55 La trayectoria del movimiento puede consistir en información en serie cronológica del punto central, o del punto medio del lado inferior del rectángulo que circunscribe un objeto móvil en una imagen, y puede ser asimismo la información obtenida transformando los mencionados puntos en coordenadas en el mapa.
- 60 La información de actividad del objeto móvil puede obtenerse en tiempo real, de manera que las mediciones pueden realizarse N veces por segundo para obtener información en serie cronológica, donde N puede ser un entero positivo, por ejemplo, de 1 a 30.
- 65 En el proceso 23 de entrada de la información de autenticación llevado a cabo en la sección 13 de entrada de información de autenticación, se crea información de autenticación. La información de autenticación incluye un

número de ID leído, el tiempo en el que se lee el número de ID e información posicional de la posición en la que se lee el número de ID.

5 Como una descripción más detallada, en el proceso 23 de entrada de información de autenticación llevado a cabo en la sección 13 de entrada de información de autenticación, cuando se utiliza RFID o ID óptica, se obtienen el número ID leído de la RFID o la ID óptica, y el tiempo en el que se lee el número de ID, para crear la información de autenticación.

10 La información posicional puede consistir, por ejemplo, en las coordenadas del lugar de instalación de un lector RFID o un sensor de ID óptico, en el mapa. Además, cuando se utiliza una cámara que ha sido sometida a una calibración de la cámara para correlacionar coordenadas universales reales con las coordenadas de imagen de la cámara, la información posicional puede consistir en los valores que se obtienen transformando las coordenadas en una imagen obtenida mediante el proceso 21 de entrada de imágenes llevado a cabo en la sección 11 de entrada de imágenes, en coordenadas universales reales.

15 Cuando se utilizan tres o más lectores de RFID utilizando RFID de banda UHF o RFID activo, etc., que tiene un amplio rango de detección, es posible obtener coordenadas posicionales de cada lector RFID en un mapa y medir la intensidad de las ondas radioeléctricas de la RFID mediante triangulación, de manera que se obtienen las coordenadas posicionales de la RFID en un mapa para su utilización como información posicional.

20 Además, utilizar una cámara que ha sido sometida a una calibración de la cámara para correlacionar coordenadas universales reales con coordenadas de imagen de la cámara, permite transformar las coordenadas en una imagen obtenida mediante el proceso 21 de entrada de imagen llevado a cabo en la sección 11 de entrada de imágenes, en valores de coordenadas universales reales.

25 Además, en este caso, es posible obtener la información posicional de RFID en tiempo real si está dentro de un intervalo de detección de la RFID, y es posible asimismo obtener y emitir la información posicional como una serie cronológica, midiendo aquella N veces por segundo. En este caso, N puede ser un entero positivo, por ejemplo, de 1 a 30.

30 En particular, cuando el objeto a autenticar es una persona, y cuando se utiliza autenticación mediante cara, huella digital, vena o iris, es posible crear información de autenticación a partir del número de ID de la persona autenticada y a partir del momento en el que la persona es autenticada, haciendo referencia a una lista de información biométrica prealmacenada.

35 Además, la información posicional puede consistir, por ejemplo, en las coordenadas de un mapa del lugar de instalación de un sensor de autenticación por huella digital, de un sensor autenticación por vena o de un sensor de autenticación por iris.

40 Además, utilizar una cámara que ha sido sometida a una calibración de la cámara para correlacionar coordenadas universales reales con coordenadas de imagen de la cámara, permite transformar las coordenadas en una imagen obtenida mediante el proceso 21 de entrada de imagen llevado a cabo en la sección 11 de entrada de imágenes, en valores de coordenadas universales reales.

45 Cuando se utiliza un sensor de autenticación facial, es posible tratar como información posicional las coordenadas de una cara en una imagen detectada en el curso de la autenticación facial, dado que la detección de la posición de la cara se lleva a cabo habitualmente para la autenticación facial.

50 Además, utilizando una cámara que ha sido sometida a una calibración de la cámara para correlacionar coordenadas universales reales con coordenadas de imagen de la cámara, y utilizando un mapa del entorno de la posición en la que está instalada la cámara, es posible asimismo obtener valores de un objeto móvil transformando sus coordenadas sobre una imagen en coordenadas en el mapa.

55 Además, en el caso de autenticación facial, es posible obtener la posición de una cara en tiempo real, y es posible asimismo obtener la información posicional de la cara de una persona, el tiempo de la medición y el número de ID de la persona como una serie cronológica, mediante medir la posición de la cara N veces por segundo, y utilizarla como información de autenticación. En este caso, N puede ser un entero positivo, por ejemplo, de 1 a 30.

60 La figura 3 es un diagrama de bloques para mostrar la configuración de un lector de gráficos cuando el objeto a autenticar es una persona y cuando se utiliza autenticación mediante ropa.

65 El aparato mostrado en la figura 3 comprende la sección 31 de entrada de imágenes, la sección 32 de análisis de la actividad, la sección 33 de entrada de información de autenticación, la sección 34 de autenticación de la autorización, la sección 35 de integración de la información, la sección 36 de determinación de la actividad y la sección de salida 37.

Si bien el funcionamiento de cada sección en el ejemplo de realización es similar al de la sección 11 de entrada de imágenes, la sección 12 de análisis de la actividad, la sección 13 de entrada de información de autenticación, la sección 14 de autenticación de la autorización, la sección 15 de integración de la información, la sección 16 de determinación de la actividad y la sección de salida 17 mostradas en la figura 1, en la sección 34 de autenticación de la autorización del ejemplo de realización, se almacena una plantilla de un uniforme o de ropa, se obtiene una imagen parcial de una persona haciendo referencia a la posición de dicha persona de acuerdo con la información de actividad del objeto móvil procedente de la sección 32 de análisis de la actividad y se compara con el uniforme o la ropa almacenados en la plantilla; y cuando existe un uniforme o ropa cuya similitud está por encima de un umbral predeterminado, la información sobre el uniforme y la ropa se trata como información de reconocimiento, y la información de autorización correspondiente a la información de reconocimiento es obtenida y añadida a la información de autenticación introducida, para ser emitida.

Como medida de la similitud en la creación de la información de autenticación, puede utilizarse una probabilidad, una simple similitud, y un ( $D_{max}$  - valor de distancia), etc., donde  $D_{max}$  es un entero positivo predeterminado. Además, la información posicional y la información temporal pueden proporcionar la misma información que la información de actividad del objeto móvil obtenida en la sección 12 de análisis de la actividad y en el proceso 22 de análisis de la actividad.

Además, en los últimos años, se ha propuesto una ID óptica en la que se hace que la luz parpadee con un periodo de tiempo fijo para representar una cadena de bits para la identificación y la detección de la posición de un objeto. Cuando se lleva a cabo la autenticación utilizando dicha ID óptica, es posible asimismo adoptar la configuración que se muestra en la figura 3.

Es posible crear información de autenticación obteniendo una imagen parcial haciendo referencia a la posición de una persona o de un vehículo de acuerdo con la información de actividad del objeto móvil obtenida en la sección 32 de análisis de la actividad a efectos de detectar una ID óptica, y leyendo el número de ID.

Además, la información posicional y la información temporal pueden proporcionar la misma información que la información de actividad del objeto móvil obtenida mediante el proceso 22 de análisis de la actividad de la sección 12 de análisis de la actividad.

En el proceso 24 de autenticación de la autorización de la sección 14 de autenticación de la autorización, se añade un nivel de autorización a la información de autenticación haciendo para ello referencia a una base de datos tabular que incluye números de ID predeterminados y niveles de autorización correspondientes a los mismos, por ejemplo, utilizando un número de ID de la información de autenticación como clave.

En el proceso 25 de integración de la información de la sección 15 de integración de la información de la figura 1, se compara una información de actividad del objeto móvil y una información de autenticación que se confirma son aproximadamente simultáneas, o se determina son próximas en el tiempo, para obtener qué información de objeto móvil corresponde a qué información de autenticación, añadiendo de ese modo un nivel de autorización a la información de actividad del objeto móvil.

Como un algoritmo para comparar la información de actividad del objeto móvil obtenida a partir de una imagen con la información de autenticación obtenida a partir de varios sensores y para obtener la correspondencia entre las mismas, pueden utilizarse diversos algoritmos, por ejemplo, la técnica dada a conocer en el documento de patente 2 descrito anteriormente.

Además, como algoritmo que compara la información de actividad del objeto móvil obtenida a partir de una imagen con la información de autenticación obtenida a partir de varios sensores y que obtiene la correspondencia entre ambas cuando se utiliza RFID activa, puede utilizarse un algoritmo a describir a continuación utilizando un ejemplo mostrado en la figura 4.

La figura 4 muestra una imagen que ha sido obtenida transformando una imagen de cámara en coordenadas sobre un mapa.

Cada una de las personas 41A a 43A lleva etiquetas RFID activas, y unos sensores 41B a 44B reciben una señal desde la RFID activa que lleva cada una de las personas 41A a 43A.

La figura 5 muestra posiciones estimadas mediante la información de actividad del objeto móvil 41C a 43C obtenida en la sección 12 de análisis de la actividad (ó 32).

La sección 12 de análisis de la actividad (ó 32) obtiene la información de actividad del objeto móvil 41C a 43C a partir de una imagen de una cámara. Las posiciones estimadas mediante la información de actividad del objeto móvil 41C a 43C son posiciones mostradas en la figura 5.

La sección 13 (ó 33) de entrada de información de autenticación emite información de autenticación mediante las señales procedentes de los sensores 41B a 44B. Si se proporciona por adelantado la información de coordenadas de los sensores 41B a 44B en un mapa, es posible obtener las posiciones estimadas mediante la información de autenticación 41D a 43D, tal como se muestra en la figura 6, midiendo mediante triangulación la intensidad de las ondas radioeléctricas de la RFID activa que lleva cada persona 41A a 43A, presentándose la intensidad de la onda radioeléctrica en el resultado de la medición de cada sensor 41B a 44B como la información de autenticación, y la sección 13 (33) de entrada de la información de autenticación emite información que incluye posiciones estimadas como información de autenticación, además de la información mediante RFID.

En la sección 15 de integración de la información, se comparan informaciones posicionales estimadas descritas anteriormente, y si una posición acorde con la información de actividad del objeto móvil está dentro del intervalo estimado de cada información de autenticación, es posible determinar que ambas se corresponden entre sí. Además, es posible representar las posiciones de la información de actividad del objeto móvil y la información de autenticación como una probabilidad continua, tal como una distribución normal centrada en torno a cierto punto de coordenadas, y es posible asimismo determinar que un par de informaciones posicionales se corresponden cuando el valor obtenido multiplicando ambas informaciones posicionales de un par alcanza un máximo.

Además, no es necesario asumir una distribución normal, y es posible asimismo utilizar resultados de estimación posicional de cualquier clase de distribución, mediante tabular y mantener la probabilidad de ser localizado en una cierta coordenada. Además, cuando el sensor de autenticación es un sensor de autenticación facial, un sensor de ID óptica o un terminal portátil GPS, es posible asimismo obtener la correspondencia entre la información de actividad del objeto móvil y la información de autenticación de la misma forma que se ha descrito anteriormente.

Además, cuando se utiliza autenticación por huellas digitales, autenticación por venas, autenticación por iris o RFID que tienen un intervalo de detección estrecho para el sensor de autenticación, puede utilizarse un algoritmo que se describirá utilizando el siguiente ejemplo mostrado en la figura 5, como algoritmo para poner en correspondencia mutua la información de actividad del objeto móvil y la información de autenticación.

La figura 7 muestra una imagen que ha sido obtenida transformando una imagen de cámara en coordenadas sobre un mapa. Aunque se ha obtenido la información posicional basada en la información 51C de actividad del objeto móvil de la persona 51A obtenida desde un imagen de una cámara en el tiempo  $t$  y en la posición del sensor 51B, la información 51C de actividad del objeto móvil no ha sido autenticada.

En el tiempo  $t+1$ , tal como se muestra la figura 8, la persona 51A es autenticada y se genera la información de autenticación 51D; se encuentra que la posición acorde con la información de autenticación 51D es la misma que la posición del sensor 51B, y dado que la información de actividad del objeto móvil situada más cerca del sensor 51B es la información 51C de actividad del objeto móvil, se determina que la información 51C de actividad del objeto móvil se corresponde con la información de autenticación 51D, y a continuación es posible mantener la información 51C de actividad del objeto móvil en correspondencia con la información de autenticación 51D.

En el caso de autenticación de ropa o de la autenticación de ID óptica, es posible poner la información de actividad del objeto móvil en correspondencia con información posicional de la información de autenticación que tiene la misma información temporal.

En la sección 16 de determinación de la actividad, cuando existe información de actividad del objeto móvil que no está en correspondencia con ninguna información de autenticación, el nivel de autorización relativo a la información de actividad del objeto móvil se asume como el nivel mínimo independientemente del contenido de la información de autorización. A la inversa, cuando existe información de autenticación que no está en correspondencia con ninguna información de actividad del objeto móvil, puede considerarse que el objeto móvil está presente en el ángulo muerto de la cámara y se crea la información de actividad del objeto móvil provisional en correspondencia con el objeto móvil, y el nivel de autorización se asume como el nivel mínimo.

Además, en el caso de la configuración mostrada en la figura 3, puesto que la información de actividad del objeto móvil es introducida en la sección 34 de autenticación de la autorización desde la sección 32 de análisis de la actividad, es posible configurar el nivel de autorización del mismo modo que se ha determinado el reconocimiento del nivel de autorización en la sección 16 de determinación de la actividad descrita anteriormente, y por lo tanto puede adoptarse dicha configuración.

Además, incluso si existe una información de autenticación que no está en correspondencia con ninguna información de actividad del objeto móvil en cierto tiempo  $t$ , si se encuentra una nueva información de actividad del objeto móvil correspondiente en el tiempo  $t + 1$ , la información de actividad móvil provisional puede ser sustituida con la información de actividad del objeto móvil recién encontrada.

En el proceso 26 de determinación de la actividad de la sección 16 de determinación de la actividad, se hace referencia a una lista de actividades permitidas y actividades prohibidas en función de la autorización de una

persona o de un vehículo detectado, y si se detecta una actividad ilegal o una actividad prohibida, se genera información de alarma.

Esta operación se describirá en detalle en base a un ejemplo específico.

5 Se realizará la descripción en el caso de un sistema de vigilancia que está configurado de manera que, tal como en el ejemplo de la imagen de cámara mostrada en la figura 9, cuando en una imagen se detecta una persona ordinaria que camina en sentido incorrecto en un pasillo de un sentido, se generará información de alarma.

10 Por ejemplo, supóngase que se detecta una persona 61A que camina en sentido erróneo en un pasillo de un sentido de un aeropuerto. Si es posible saber que dicha persona 61A está autorizada para caminar libremente en ambos sentidos en un pasillo de un sentido de un aeropuerto, como resultado de que la persona 61A es autenticada, por ejemplo, mediante RFID activa, haciendo referencia a la lista de actividades permitidas y actividades prohibidas acorde con el nivel de autorización de dicha persona, es posible estimar que no existe necesidad de emitir una  
15 alarma, dado que la actividad de caminar en sentido incorrecto en el pasillo de un sentido está dentro de la autorización, y por lo tanto no se generará información de alarma.

20 Cuando la autorización de la persona 61A no puede autenticarse, o si es posible saber que el nivel de autorización es bajo de manera que haciendo referencia a la lista de actividades permitidas y actividades prohibidas no se permite la actividad de caminar libremente en ambos sentidos en un pasillo de un sentido, puede generarse información de alarma.

25 A este respecto, el método de autenticación puede no ser RFID activa, sino que puede ser la autenticación facial, mediante huellas digitales, venas, o autenticación por iris, RFID o ID óptica con un intervalo de detección estrecho, o autenticación mediante ropa.

30 A continuación, se realizará la descripción de un sistema de vigilancia en el que, tal como con el ejemplo de la imagen de cámara mostrado en la figura 10, la única área en la que se permite la entrada es el andén de una estación, y el sistema de vigilancia está configurado para crear información de alarma si una persona ordinaria entra en la vía ferroviaria.

35 Supóngase que es detectada la persona 71A que ha entrado en la vía ferroviaria. La figura 11 representa la figura 10 sobre un mapa, en el que el andén es la única área en la que se permite la entrada, y se determina que la persona 71A está en el área de acceso prohibido. Si esta persona 71A es autenticada por una etiqueta RFID activa o llevando puesto un uniforme y se encuentra que dicha persona está autorizada para entrar en la vía ferroviaria, de acuerdo con el nivel de autorización de dicha persona, haciendo referencia a la lista de actividades permitidas y actividades prohibidas en función del nivel de autorización de la persona; puede estimarse que la entrada a la vía ferroviaria está dentro de la autorización y por lo tanto no es necesario emitir una alarma, y por lo tanto no se generará información de alarma.

40 Cuando la autorización de la persona 71A no puede ser autenticada, o cuando puede encontrarse que no se permite a dicha persona entrar en la vía ferroviaria debido a su bajo nivel de autorización haciendo referencia a la lista de actividades permitidas y actividades prohibidas, puede crearse información de alarma. A este respecto, el método de autenticación puede no ser autenticación de RFID activa o autenticación mediante ropa, y es posible adoptar  
45 autenticación facial, mediante huella digital, venas o autenticación por iris, y autenticación de RFID o ID óptica con un intervalo de detección estrecho.

50 Es posible asimismo modificar dinámicamente la definición de una actividad permitida y una actividad prohibida. Por ejemplo, es posible prohibir la entrada de una persona que tiene una autorización específica, en función de una zona horaria.

55 Además, la determinación de una actividad permitida y una actividad prohibida puede basarse en una estimación combinada de una serie de objetos móviles. Por ejemplo, puede configurarse asimismo de manera que solamente cuando se trata de una persona que es un supervisor y que lleva un uniforme específico, se permitirá a dicha persona entrar a una zona particular. Además, puede configurarse asimismo de manera que se permite la entrada de un número máximo de M personas que llevan un uniforme. A este respecto, M puede configurarse libremente siendo un entero positivo, por ejemplo, de 1 a 10.

60 Además, cuando el objeto móvil es una persona y el lugar de vigilancia consiste en ciertas instalaciones controladas, el algoritmo de determinación puede configurarse de manera que, incluso cuando se detecta una persona con el nivel de autorización mínimo, si se detecta una serie de personas con el nivel de autorización máximo en torno a la persona mencionada, no se generará información de alarma.

65 Específicamente, siendo BL el nivel de autorización y siendo N(BL) el número de personas detectadas en cada nivel, y haciendo que el número de personas que tienen el nivel de autorización mínimo sea N(0), puede generarse información de alarma cuando  $\sum BLBL \times N(BL) \leq A \times N(0)$ , donde A es una constante predeterminada.

5 En el proceso de salida 27 en la sección de salida 17, se genera una alarma en función del nivel de la información de alarma. Por ejemplo, puede realizarse con caracteres una visualización de "Intruso en zona de acceso prohibido", o bien los caracteres pueden mostrarse en colores amarillo, naranja y rojo en función del nivel, y así mismo el tamaño de los caracteres puede variarse en función del nivel de autorización.

Es posible, asimismo, distribuir información a correo electrónico, terminales portátiles de información y teléfonos móviles, etc., y es posible asimismo variar el número y el tipo de personas a las que se distribuye la información.

10 Además, es posible asimismo distribuir una alarma a otros sistemas de vigilancia través de una red, y también variar el número y el tipo de sistemas a los que se distribuye la información, en función del nivel de autorización. Es posible asimismo generar un sonido de alarma mediante una sirena o un altavoz de las instalaciones, y variar el volumen del sonido de alarma y la frecuencia del mismo en función del nivel de autorización.

15 Además, es posible asimismo emitir luz, tal como luz parpadeante, y variar la velocidad del parpadeo o discriminar el color, en colores amarillo, naranja y rojo, en función del nivel de autorización.

20 Es posible asimismo distribuir una imagen al mismo tiempo que se emite una alarma, y distribuir imágenes de manera rutinaria incluso cuando no se emite una alarma.

25 Debe observarse que la sección 11 de entrada de imágenes, la sección 12 de análisis de la actividad, la sección 13 de entrada de información de autenticación, la sección 14 de autenticación de la autorización, la sección 15 de integración de la información, la sección 16 de determinación de la actividad, y la sección de salida 17 mostradas en la figura 1; y la sección 31 de entrada de imágenes, la sección 32 de análisis de la actividad, la sección 33 de entrada de información de autenticación, la sección 34 de autenticación de la autorización, la sección 35 de integración de la información, la sección 36 de determinación de la actividad y la sección de salida 37 mostradas en la figura 3, pueden fabricarse en un ordenador al que se vayan a introducir señales desde sensores y una cámara CCD; y la presente invención incluye un programa que hace que un sistema informático ejecute el proceso que se realizará en cada componente descrito anteriormente, e incluye un medio de grabación o soporte de registro tal como un CD-ROM, un disco flexible, un DVD-ROM, etc., para almacenar el programa mencionado anteriormente.

30

## REIVINDICACIONES

1. Un aparato de detección de actividad sospechosa para detectar una actividad sospechosa utilizando medios de generación de señal, un sensor para recibir una señal procedente de dichos medios de generación de señal, y datos de imagen tomados mediante una cámara, que comprende:

una sección (11) de entrada de imágenes adaptada para capturar datos de imagen de dicha cámara y para emitir dichos datos de imagen;

una sección (12) de análisis de la actividad adaptada para detectar un objeto móvil tal como una persona y un vehículo incluidos en una imagen indicada mediante datos de imagen procedentes de dicha sección (11) de entrada de imágenes, reconocer si el objeto móvil detectado es una persona, un vehículo u otra entidad diferente a estos, obtener la posición del objeto detectado, y extraer además una trayectoria del movimiento del objeto detectado, para emitir la información así obtenida como información de actividad del objeto móvil;

una sección (13) de entrada de información de autenticación adaptada para obtener un número de ID indicado en dicha señal recibida mediante dicho sensor, un tiempo de recepción y una posición de recepción de dicha señal mediante la salida de dicho sensor, y emitir la información así obtenida como información de autenticación;

una sección (14) de autenticación de la autorización adaptada para almacenar información de autorización correspondiente a dicha información de autenticación, obtener información de autorización correspondiente a la información de autenticación introducida desde dicha sección (13) de entrada de información de autenticación y emitir dicha información de autenticación introducida con dicha información de autorización obtenida añadida a la misma;

una sección (15) de integración de la información adaptada para poner la información de autenticación complementada con información de autorización introducida desde dicha sección (14) de autenticación de la autorización, en correspondencia con información de actividad del objeto móvil introducida desde dicha sección de análisis de la actividad, y emitir la información de actividad del objeto móvil con la información de autorización añadida a la misma;

una sección (16) de determinación de la actividad adaptada para incluir una lista de actividades permitidas y actividades prohibidas dependiendo del nivel de autorización, reconocer una actividad de violación y una actividad prohibida predeterminadas haciendo referencia a dicha lista, con respecto al nivel de autorización añadido a la información de actividad del objeto móvil introducida desde dicha sección (15) de integración de la información, y tras la detección de que la actividad indicada mediante la información de actividad del objeto móvil es una actividad ilegal o una actividad prohibida, generar y emitir la información de alarma; y

una sección (17) de salida adaptada para emitir una alarma cuando recibe información de alarma procedente de dicha sección (16) de determinación de la actividad;

**caracterizado por que:**

dicha sección (16) de determinación de la actividad está adaptada además para, cuando existe información de autenticación en la sección de determinación de la actividad que no está en correspondencia con ninguna información de actividad del objeto móvil, crear información de actividad del objeto móvil provisional para ponerla en correspondencia con dicha información de autenticación, y asumir el nivel de autorización de la misma como estando al mínimo nivel.

2. El aparato de detección de actividad sospechosa según la reivindicación 1, en el que cuando es introducida información de actividad del objeto móvil que no corresponde con ninguna información de autenticación, dicha sección (16) de determinación de la actividad está adaptada para asumir el nivel de autorización con respecto a la información de actividad del objeto móvil como estando al mínimo nivel.

3. El aparato de detección de actividad sospechosa según la reivindicación 1, en el que la sección (14) de autenticación de la autorización está adaptada para almacenar una plantilla de un uniforme o de ropa; y está configurada para obtener una imagen parcial de una persona mediante hacer referencia a la posición de dicha persona a partir de la información de actividad del objeto móvil procedente de dicha sección de análisis de la actividad, está configurada para comparar dicha imagen parcial con el uniforme o la ropa almacenados en dicha plantilla; y cuando existe un uniforme o ropa cuya similitud es mayor que un umbral predeterminado, está configurada para obtener información de autenticación introducida desde dicha sección de entrada de información de autenticación con información acerca del uniforme o la ropa siendo la información de autenticación, o está configurada para obtener información de autorización correspondiente a información de reconocimiento que es información acerca del uniforme y de la ropa, y está configurada para emitir la información de autenticación introducida con dicha información de autorización añadida a la misma.

4. El aparato de detección de actividad sospechosa según la reivindicación 3, en el que cuando se introduce información de actividad del objeto móvil que no se corresponde con ninguna información de autenticación, dicha sección (14) de autenticación de la autorización está configurada para establecer el nivel de autorización con respecto a la información de actividad del objeto móvil estando al nivel mínimo.

5. El aparato de detección de actividad sospechosa según cualquiera de las reivindicaciones 1 a 4, en el que

la lista de actividades permitidas y actividades prohibidas en dicha sección (16) de determinación de la actividad varía en función del tiempo.

5 6. El aparato de detección de actividad sospechosa según cualquiera de las reivindicaciones 1 a 5, en el que dicha sección (16) de determinación de la actividad está configurada para aplicar una autorización, que ha sido añadida a un elemento de información de actividad del objeto móvil, a otro elemento de información de actividad del objeto móvil.

10 7. Un método de detección de actividad sospechosa llevado a cabo en un aparato de detección de actividad sospechosa que comprende la sección (11) de entrada de imágenes, una sección (12) de análisis de la actividad, una sección (13) de entrada de información de autenticación, una sección (14) de autenticación de la autorización, una sección (15) de integración de la información, una sección (16) de determinación de la actividad y una sección de salida (17), detectando dicho aparato de detección de actividad sospechosa una actividad sospechosa mediante la utilización de medios de generación de señal, un sensor para recibir una señal procedente de dichos medios de  
15 generación de señal, y datos de imagen tomados mediante una cámara, en el que dicha sección (11) de entrada de imágenes captura datos de imagen procedentes de dicha cámara y emite dichos datos de imagen;  
dicha sección (12) de análisis de la actividad detecta un objeto móvil, tal como una persona y un vehículo incluido en una imagen indicada mediante datos de imagen procedentes de dicha sección (11) de entrada de imágenes, reconoce si el objeto móvil detectado es una persona, un vehículo u otra entidad, obtiene la posición del objeto detectado y extrae además una trayectoria del movimiento del objeto detectado para emitir la información así obtenida como información de actividad del objeto móvil;  
dicha sección de entrada de información de autenticación (13) obtiene un número de ID indicado en dicha señal recibida mediante dicho sensor, un tiempo de recepción y una posición de recepción de dicha señal mediante la salida de dicho sensor, y emite la información así obtenida como información de autenticación;  
25 dicha sección (14) de autenticación de la autorización almacena información de autorización correspondiente a dicha información de autenticación; obtiene información de autorización correspondiente a la información de autenticación introducida desde dicha sección (13) de entrada de información de autenticación y emite la información de autenticación introducida con dicha información de autorización obtenida añadida a la misma;  
30 dicha sección (15) de integración de la información pone información de autenticación complementada con información de autorización introducida desde dicha sección (14) de autenticación de la autorización, en correspondencia con información de actividad del objeto móvil introducida desde dicha sección de análisis de la actividad, y emite la información de actividad del objeto móvil con la información de autorización añadida a la misma;  
dicha sección (16) de determinación de la actividad incluye una lista de actividades permitidas y actividades prohibidas en función del nivel de autorización, reconoce una actividad de violación o una actividad prohibida predeterminadas haciendo referencia a dicha lista, con respecto al nivel de autorización añadido a la información de actividad del objeto móvil introducida desde dicha sección (15) de integración de la información, y al detectar que la actividad indicada mediante la información de actividad del objeto móvil es una actividad ilegal o una actividad prohibida, genera y emite información de alarma; y  
40 dicha sección de salida (17) emite una alarma cuando recibe información de alarma desde dicha sección de determinación de la actividad;  
**caracterizado por que:**

45 cuando existe información de autenticación en la sección de determinación de la actividad que no está en correspondencia con ninguna información de actividad del objeto móvil, dicha sección (16) de determinación de la actividad crea información de actividad del objeto móvil provisional poniéndola en correspondencia con dicha información de autenticación, y asume que el nivel de autorización de la misma está al nivel mínimo.

50 8. Un método de detección de actividad sospechosa según la reivindicación 7, en el que dicha sección (14) de autenticación de la autorización almacena una plantilla de un uniforme o de ropa; obtiene una imagen parcial de una persona haciendo referencia a la posición de dicha persona a partir de la información de actividad del objeto móvil procedente de dicha sección (12) de análisis de la actividad; compara dicha imagen parcial con el uniforme o la ropa almacenados en dicha plantilla; y cuando existe un uniforme o ropa cuya similitud es mayor que un umbral predeterminado, obtiene información de autenticación introducida desde dicha sección (13) de entrada de  
55 información de autenticación con información acerca del uniforme o la ropa siendo la información de autenticación, u obtiene información de autorización correspondiente a la información de reconocimiento que es información acerca del uniforme o la ropa, y emite la información de autenticación introducida con dicha información de autorización estando añadida a la misma.

60 9. El método de detección de actividad sospechosa según la reivindicación 8, en el que cuando se introduce información de actividad del objeto móvil que no se corresponde con ninguna información de autenticación, dicha sección (14) de autenticación de la autorización establece el nivel de autorización con respecto a la información de actividad del objeto móvil estando al nivel mínimo.

65 10. El método de detección de actividad sospechosa según cualquiera de las reivindicaciones 7 a 9, en el que

la lista de actividades permitidas y actividades prohibidas en dicha sección (16) de determinación de la actividad varía en función del tiempo.

5 11. El método de detección de actividad sospechosa según cualquiera de las reivindicaciones 7 a 10, en el que dicha sección (16) de determinación de la actividad aplica una autorización, que ha sido añadida a un elemento de información de actividad del objeto móvil, a otro elemento de información de actividad del objeto móvil.

10 12. Un programa o un medio de grabación o soporte de registro para almacenar dicho programa, que hace que un sistema informático ejecute el proceso llevado a cabo en cada componente de cualquiera de las reivindicaciones 7 a 11.

Fig. 1

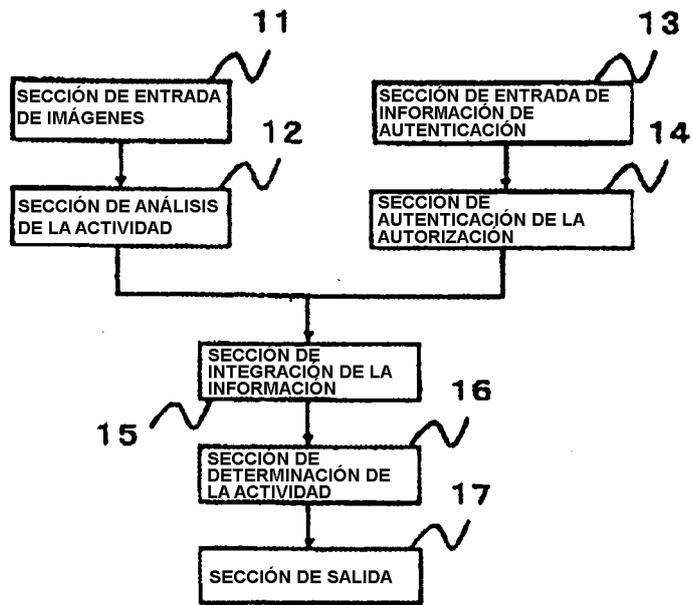


Fig. 2

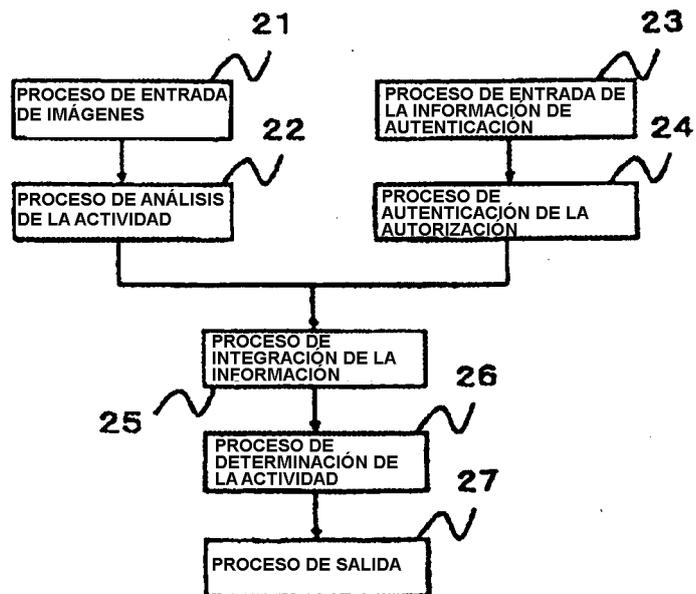


Fig. 3

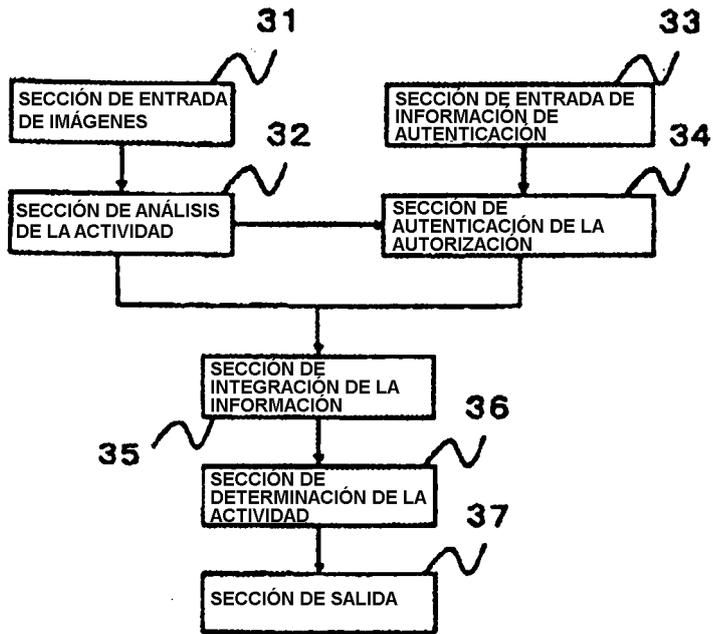


Fig. 4

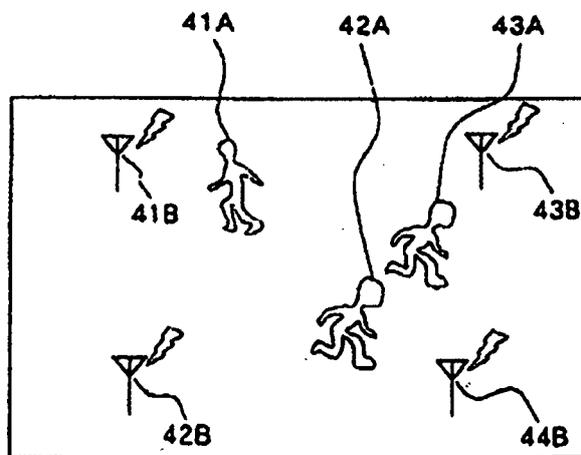


Fig. 5

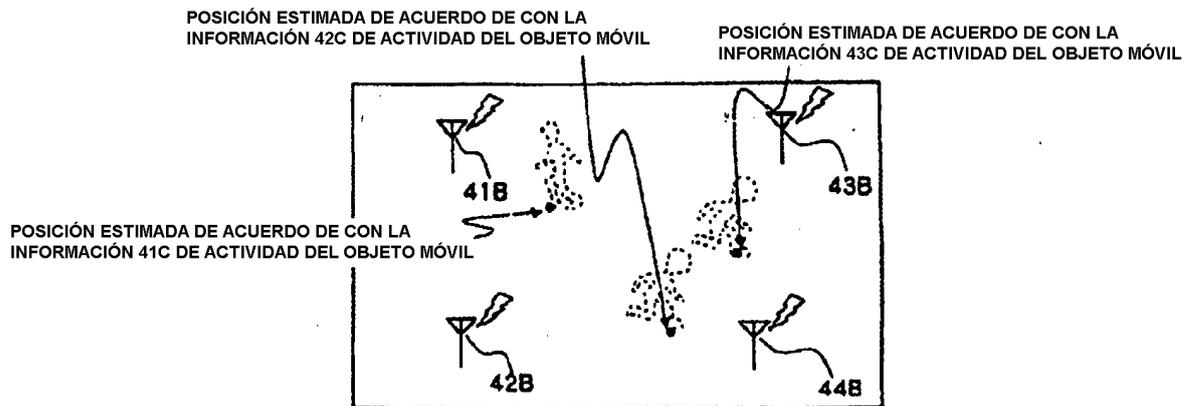


Fig. 6

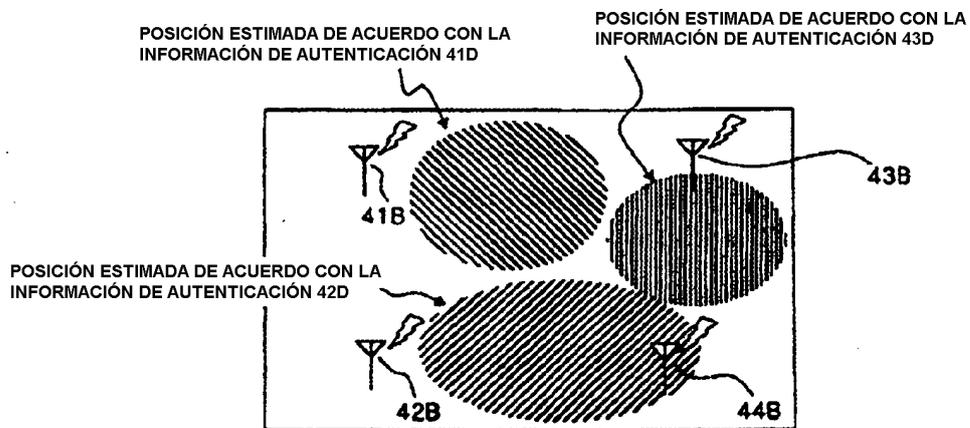
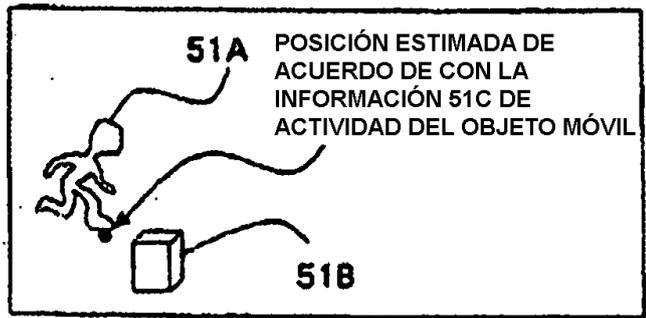
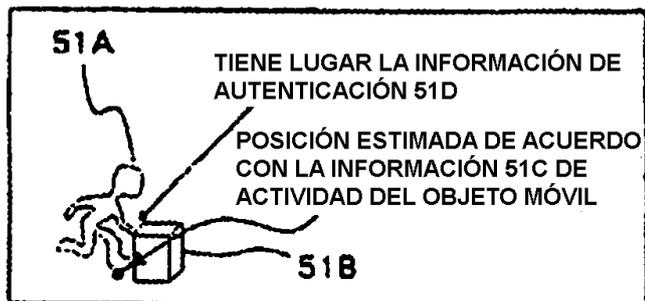


Fig. 7



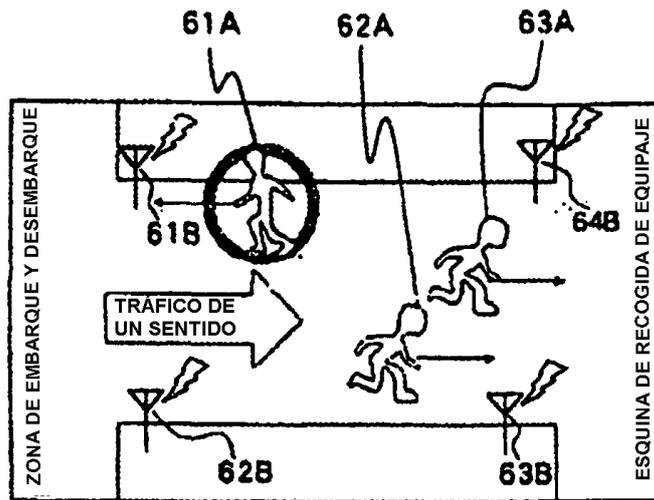
SIN INFORMACIÓN DE AUTENTICACIÓN EN EL TIEMPO  $t$

Fig. 8



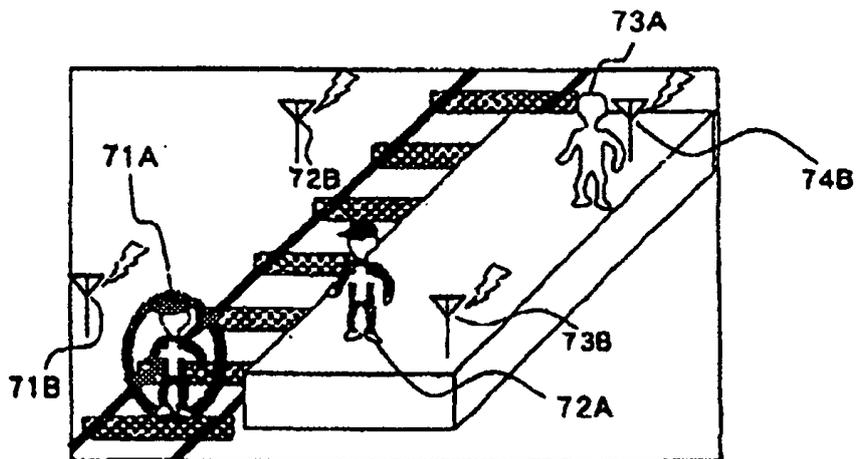
TIENE LUGAR LA INFORMACIÓN DE AUTENTICACIÓN 51 EN EL TIEMPO  $t + 1$

Fig. 9



EJEMPLO DE IMAGEN DE CÁMARA DE UN PASILLO DE AEROPUERTO

Fig. 10



EJEMPLO DE IMAGEN DE CÁMARA DE UN ANDÉN DE UNA ESTACIÓN

Fig. 11

