(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 496 665**

(21) Número de solicitud: 201330190

(51) Int. CI.:

G06T 7/20 (2006.01)
G06K 9/00 (2006.01)
G07C 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

14.02.2013

(43) Fecha de publicación de la solicitud:

19.09.2014

(56) Se remite a la solicitud internacional:

PCT/ES2014/000019

(71) Solicitantes:

HOLDING ASSESSORIA I LIDERATGE, S.L. (100.0%)
Av. Sarrià 51 2º 1ª
08029 BARCELONA ES

(72) Inventor/es:

ARRUFAT RIBAS, Francesc Xavier

(74) Agente/Representante:

ESPIELL VOLART, Eduardo María

(54) Título: **MÉTODO DE DETECCIÓN DE ACCESO FRAUDULENTO EN PUNTOS DE ACCESO CONTROLADO**

(57) Resumen:

Método de detección de acceso fraudulento en puntos de acceso controlado.

Este método es aplicable en puntos de acceso provistos de mecanismos electromecánicos de apertura y cierre, adecuados para permitir el paso individualizado de sucesivos usuarios. El método comprende: la captación de imágenes de los usuarios que pasan por los puntos de acceso a controlar; el tratamiento informático de las imágenes recibidas y la detección mediante algoritmos de tratamiento de imágenes de los sucesivos usuarios que pasan por un punto de acceso; el cálculo del tiempo real transcurrido entre el paso de dos usuarios consecutivos por dicho punto de acceso, y la detección de accesos fraudulentos comparando, mediante análisis algorítmico, el tiempo real de paso con un umbral de alarma o tiempo mínimo estimado de paso de usuarios consecutivos.

ES 2 496 665 A1

DESCRIPCIÓN

Metodo de detección de acceso fraudulento en puntos de acceso controlado.

Objeto de la invención

La presente invención se refiere un método de detección de acceso fraudulento en puntos de acceso controlado; y principalmente en aquellos puntos de acceso provistos de mecanismos electromecánicos de apertura y cierre, adecuados para permitir el paso individualizado de sucesivos usuarios.

Este método presenta unas particularidades orientadas a detectar automáticamente el paso fraudulento de usuarios a través de puntos de acceso controlado, mediante la captación de imágenes del punto de acceso en cuestión y la detección, a partir del tratamiento informático de dichas imágenes, el tiempo real transcurrido entre el paso de dos usuarios consecutivos, y la determinación de la existencia, o no, de un acceso fraudulento dependiendo de que dicho tiempo real sea menor, o mayor, respectivamente que un umbral de alarma o tiempo mínimo de paso, permitido o estimado, entre dos usuarios consecutivos.

Campo de aplicación de la invención.

La presente invención es aplicable en la vigilancia y control de acceso de los usuarios a zonas o recintos con puntos de acceso controlados.

Antecedentes de la invención.

Actualmente existen diversas zonas a las que pueden acceder los usuarios, ya sean vehículos, personas o de cualquier otro tipo, a través de unos puntos de acceso controlado mediante mecanismos electromecánicos de apertura y cierre que pueden presentar diferentes configuraciones dependiendo del tipo de usuario cuyo acceso se desea controlar.

Así por ejemplo, en las autopistas de peaje los puntos de acceso controlado disponen de unas barreras para controlar el paso de los vehículos y que dicho paso se realice de forma individual; y en las estaciones de transporte los puntos de acceso controlados están constituidos por unas puertas desplazables o por unos tornos giratorios, adecuados para controlar el paso individualizado de las personas.

Estos puntos de acceso controlado, con independencia de su tipología, están ideados para permitir el paso individual y separado de los sucesivos usuarios; sin embargo, esto no evita que se produzcan accesos fraudulentos utilizando una técnica consistente en pasar dos usuarios consecutivos muy próximos entre sí, aprovechando una única apertura del mecanismo de apertura y cierre ubicado en el punto de acceso.

Actualmente la única manera de impedir estos accesos fraudulentos y de identificar al infractor consiste en disponer diversos vigilantes en los puntos de acceso, lo que requiere la dedicación de un número elevado de personas y unos elevados costes de personal.

Si bien es cierto que en estos puntos de acceso controlado es habitual la instalación de cámaras de vigilancia, éstas requieren la presencia, en un centro de control, de personal suficiente para su observación continuada lo que requiere, al igual que en el caso anterior, la dedicación de un número importante de personas y unos elevados costes de personal. Además, este tipo de vigilancia permite detectar la infracción, pero no resulta efectiva ni adecuada para localizar, retener y sancionar al usuario infractor, especialmente cuando dicho usuario es, por ejemplo, una persona que accede a una estación de transporte concurrida.

El solicitante de la presente invención desconoce la existencia de antecedentes que permitan solventar satisfactoriamente el problema que supone el acceso fraudulento de usuarios por puntos de acceso controlados.

Descripción de la invención.

El método de detección de acceso fraudulento en puntos de acceso controlados objeto de esta invención presenta unas particularidades constructivas orientadas a realizar de una manera totalmente automática la detección de accesos fraudulentos en puntos de acceso controlados y a realizar de modo también automático, cuando se produce la detección de un acceso fraudulento de una serie de acciones orientadas a permitir la posterior identificación del supuesto infractor, posibilitar su identificación e interceptación por parte del personal de seguridad o de vigilancia y a realizar el almacenaje de la información necesaria para probar documentalmente la existencia del acceso fraudulento en caso de que fuera preciso ante una reclamación tanto por parte del infractor como por parte del gestor o prestador del servicio.

Este método de detección de acceso fraudulento en puntos de acceso controlado está especialmente indicado para realizar dicha detección en puntos de acceso provistos de mecanismos electromecánicos de apertura y cierre.

El método de la invención comprende las etapas o fases siguientes:

a) la captación de imágenes de los usuarios que pasan por los puntos de acceso a controlar y el envío de dichas imágenes en tiempo real a un sistema informático;

b) el tratamiento informático, de manera automática y en tiempo real de las imágenes recibidas y la detección mediante algoritmos de tratamiento de imágenes de los sucesivos usuarios que pasan por un punto de acceso;

c) el calculo en base a dicho tratamiento informático del tiempo real transcurrido entre el paso de dos usuarios consecutivos por dicho punto de acceso;

d) la comparación del tiempo real transcurrido con un umbral o alarma de tiempo mínimo estimado para el paso de dos usuarios consecutivos por un punto de acceso;

e) la detección de la existencia de un acceso fraudulento cuando el tiempo real de paso es inferior al umbral de alarma o tiempo mínimo estimado; y

f) cuando es detectado un acceso fraudulento: la retención, y/o el almacenaje en una memoria del sistema informático, y/ o la distribución por medios electrónicos a un centro de control y/o directamente a unos terminales móviles específicos, de una o múltiples imágenes del usuario supuestamente infractor durante su paso por el punto de acceso.

La utilización de este método requiere la utilización de determinados elementos disponibles en el mercado tales como unas cámaras de video u otros sensores, como pueden ser unos sensores infrarrojos dispuestos en los puntos de acceso a controlar para la captación de imágenes mencionada en el punto a) del método descrito y un sistema informático provisto de un software especifico para esta aplicación y que permite realizar automáticamente las fases b) a f) del método descrito anteriormente.

En base a este método el acceso fraudulento se determina a partir del tiempo que el sistema informático estima como transcurrido entre el paso de dos usuarios por el punto de acceso. El umbral de alarma (mínimo tiempo de paso permitido entre dos usuarios consecutivos) se puede estimar estadísticamente (a partir de la distribución estadística previa de los tiempos de paso) o bien se puede fijar determinísticamente.

En ambos casos la empresa encargada de gestionar y controlar el acceso puede ajustar los parámetros que permitan obtener un balance adecuado entre falsos positivos y falsos negativos.

De acuerdo con la invención este método comprende el almacenaje, conjuntamente de las imágenes del usuario supuestamente infractor, de los datos derivados del análisis de tiempo real de paso analizado y relacionado con dicho usuario supuestamente infractor.

El almacenaje de las imágenes del supuesto infractor y de los datos del tiempo de paso relativos al mismo en relación con algún usuario anterior o posterior permite justificar documentalmente a posteriori la existencia del paso fraudulento de dicho usuario por el punto de acceso para gestionar posibles reclamaciones realizadas por cualquiera de las dos partes implicadas es decir el usuario o la empresa encargada de gestionar y controlar el acceso.

Adicionalmente, cabe mencionar que la distribución por medios electrónicos de las imágenes del supuesto infractor directamente a los terminales móviles específicos, concretamente de un vigilante o vigilantes, ubicados en la zona o recinto próxima al punto de acceso en los que se ha cometido la supuesta infracción, permite realizar con un número mínimo de vigilantes la localización, interceptación y sanción de aquellos usuarios que accedan de manera fraudulenta por cualquiera de los puntos de acceso existentes en un mismo recinto.

Una vez descrita suficientemente la naturaleza de la invención, se hace constar a los efectos oportunos que la misma podrá ser modificada, siempre y cuando ello no suponga una alteración de las características esenciales de la invención que se reivindican a continuación.

REIVINDICACIONES

1.- Método de detección de acceso fraudulento en puntos de acceso controlados; estando dichos puntos de acceso provistos de mecanismos electro-mecánicos de apertura y cierre, adecuados para permitir el paso individualizado de sucesivos usuarios; **caracterizado** porque comprende:

a) la captación de imágenes de los usuarios que pasan por los puntos de acceso a controlar y el envío de dichas imágenes a un sistema informático;

b) el tratamiento informático, de manera automática y en tiempo real, de las imágenes recibidas y la detección mediante algoritmos de tratamiento de imágenes de los sucesivos usuarios que pasan por un punto de acceso,

c) el cálculo, en base a dicho tratamiento informático, del tiempo real transcurrido entre el paso de dos usuarios consecutivos por dicho punto de acceso,

d) la comparación, mediante análisis algorítmico, del tiempo real transcurrido con un umbral de alarma o tiempo mínimo estimado para el paso de dos usuarios consecutivos por un punto de acceso;

e) la detección de la existencia de un acceso fraudulento cuando el tiempo real de paso es inferior al umbral de alarma o tiempo mínimo estimado; y

f) cuando es detectado un acceso fraudulento: la retención, y/o el almacenaje en una memoria del sistema informático, y/o la distribución por medios electrónicos, a un centro de control y/o directamente a unos terminales móviles específicos, de una o múltiples imágenes del usuario supuestamente infractor durante su paso por el punto de acceso.

2.- Método, según la reivindicación 1, **caracterizado** porque comprende el almacenaje, conjuntamente con las imágenes del usuario supuestamente infractor, de los datos derivados del análisis de tiempo real de paso analizado y relacionado con dicho usuario supuestamente infractor.