(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 609**

(51) Int. CI.:
G07C 9/00 (2006.01)
G06F 15/00 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09163462 .6**
(96) Fecha de presentación: **02.09.2002**
(97) Número de publicación de la solicitud: **2101300**
(97) Fecha de publicación de la solicitud: **16.09.2009**

(54) Título: **Procedimiento de certificación individual**

(30) Prioridad:
03.09.2001 JP 2001265929

(45) Fecha de publicación de la mención BOPI:
16.04.2012

(45) Fecha de la publicación del folleto de la patente:
16.04.2012

(73) Titular/es:
KABUSHIKI KAISHA EIGHTING
20-14, MINAMIOUI 6-CHOME, SHINAGAWA-KU, TOKYO, JP

(72) Inventor/es:
Fujisawa, Tomonori y
Satou, Shoji

(74) Agente/Representante:
Fúster Olaguibel, Gustavo Nicolás

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

Procedimiento de certificación individual

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un procedimiento de autenticación individual que usa un terminal de telefonía móvil.

TECNOLOGÍA ANTECEDENTE

Convencionalmente la autenticación individual se ha realizado principalmente usando una tarjeta de plástico con una banda magnética adherida a ella, como se representa mediante una tarjeta de crédito y, en este procedimiento, la información sobre cada individuo almacenada en la banda magnética es leída por un lector de tarjetas, y el individuo es identificado verificando la información leída con datos específicos para una compañía que gestiona el sistema de crédito. Recientemente, sin embargo, a menudo se producen actividades criminales tales como falsificación de una tarjeta de crédito y, por lo tanto, tarjetas inteligentes (IC) que son difíciles de falsificar se han presentado como una herramienta para autenticación individual.

Además, en un caso de autenticación en línea, la tecnología de encriptado o números de identificación personal se combinan con el procedimiento de autenticación individual convencional para mejorar la seguridad y, por lo tanto, el riesgo de que el número de una tarjeta sea leído ilegalmente desde el exterior es bajo.

Además se ha conocido, como procedimiento de autenticación individual, el uso de un terminal de telefonía móvil, el procedimiento para autenticación individual en el que un usuario recibe previamente datos de identificación individual enviados desde una compañía de crédito mediante un terminal de telefonía móvil y la autenticación individual se realiza verificando el número de identificación personal del usuario con los datos de identificación individual almacenados en el terminal de telefonía móvil cuando se realiza el pago.

En cualquiera de los procedimientos tales como el uso de una tarjeta IC, la autenticación en línea y la autenticación individual mediante un terminal de telefonía móvil, sin embargo, no se da ninguna solución fundamental a los diversos problemas asociados con la autenticación individual en la medida de los problemas de “información fija” y “presencia de lectores de tarjetas”. Además, los problemas asociados con el pago en línea para actividades comerciales cibernéticas, que se espera que aumenten sustancialmente en el futuro, no se han resuelto.

El documento WO-A-01/41081 da a conocer procedimientos y sistemas para permitir a los usuarios de un sistema de comunicación celular obtener servicios, bienes u otros beneficios de una tercera parte. El sistema permite al usuario pedir una credencial de un sistema de emisión de credenciales, recibir la ficha en su medio de comunicación móvil y obtener un servicio, bienes o algún otro tipo de beneficio comunicando la credencial a un sistema de verificación, que verifica la credencial y permite al usuario obtener el servicio deseado.

El documento US5.576.528 da a conocer un procedimiento y un aparato para aumentar la densidad de información de un símbolo de código de barras generando símbolos de código de barras de múltiples constituyentes, en los que cada uno está formado en un color diferente seleccionado entre un grupo de diversos colores primarios, y solapando cada símbolo de color diferente uno encima de otro, formando de este modo un símbolo de código de barras agregado de diversos colores. En zonas en las que las barras de diferente color se solapan entre sí, se forman colores distintos de aquellos en el grupo original de colores. El símbolo de código de barras agregado es escaneado por un dispositivo de formación de imágenes en estado sólido, y la imagen escaneada se resuelve mediante técnicas de procesamiento de imágenes en los tres símbolos de código de barras constituyentes de los diversos colores. Cada símbolo de código de barras es procesado y decodificado a continuación de forma individual según la simbología particular usada para codificar los símbolos constituyentes del código de barras. Como resultado, múltiples símbolos de código de barras se imprimen en el espacio normalmente requerido por un símbolo de código de barras, y cada símbolo constituyente se separa mediante resolución del color y se decodifica para formar los datos originales. Por lo tanto, la densidad de información del sistema de código de barras aumenta sin necesidad de una nueva simbología. Además, un único símbolo de código de barras puede dividirse en múltiples partes de sustancialmente el mismo tamaño e imprimirse sustancialmente una sobre otra en diferentes colores, produciendo de este modo un único símbolo de código de barras compactado con mayor densidad de información. El símbolo de código de barras compactado puede recuperarse escaneando y resolviendo el símbolo de vuelta a sus partes constituyentes, concatenando las partes conjuntamente y decodificando el símbolo de código de barras resultante según técnicas convencionales.

DIVULGACIÓN DE LA INVENCIÓN

Según la presente invención, se proporciona un procedimiento de autenticación individual como se expone en la reivindicación 1.

En las otras reivindicaciones se exponen características adicionales.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es una vista que ilustra un sistema de autenticación individual según una realización de la presente invención como un todo;

La figura 2 es una vista explicativa que muestra principios básicos de una realización;

La figura 3 es un diagrama de bloques que muestra la configuración de un archivo de datos para autenticación individual almacenado en un servidor de autenticación 10;

La figura 4 es un diagrama de flujo que muestra la secuencia desde la generación de un “código de verificación” hasta su supresión en el servidor de autenticación 10;

La figura 5 es un diagrama de bloques que muestra la configuración del servidor de autenticación 10;

La figura 6 es una vista explicativa que muestra la autenticación individual realizada cuando el usuario pasa a través de una puerta de embarque;

La figura 7 es una vista en aumento de una pantalla de autenticación de un terminal de telefonía móvil 30 en la que se muestra un “código de verificación”;

La figura 8 es un diagrama de flujo que muestra la secuencia operativa de extracción, análisis, y conversión de puntos que constituyen el código de verificación;

La figura 9 es un diagrama de bloques que muestra principalmente una sección de generación de datos de visualización 509 del servidor de autenticación 10 en la que se genera una señal de imagen; y

La figura 10 es un diagrama de bloques que muestra principalmente una sección de análisis de información sobre puntos 102 de un lector 21.

REALIZACIONES

A continuación se describe una realización preferida de la presente invención en referencia a los dibujos relacionados.

A continuación se describe un procedimiento de autenticación individual seguro y rápido usando un terminal de telefonía móvil, en el que información de señal sin sentido y no fija es usada temporalmente entre redes, en las que no se ha establecido la seguridad.

En el procedimiento de autenticación individual, un usuario recibe con su terminal de telefonía móvil un código de verificación generado por un servidor de autenticación después de la petición desde el terminal de telefonía móvil del usuario; este código de verificación es devuelto desde un servidor de gestión de ventas al servidor de autenticación; el código de verificación generado en el servidor de autenticación es verificado con el enviado mediante el servidor de gestión de ventas; y la información personal del usuario correspondiente al código de verificación es transmitida al servidor de gestión de ventas cuando los dos tipos de código de verificación son idénticos, y el procedimiento de autenticación se caracteriza porque el código de verificación recibido por el terminal de telefonía móvil se muestra como una imagen.

El código de verificación recibido por el terminal de telefonía móvil se lee con un lector de imágenes conectado al servidor de gestión de ventas. La visualización de imágenes se proporciona como una visualización de puntos con un color específico. El lector de imágenes tiene un medio para analizar la visualización de puntos con un color específico. Preferentemente, el código de verificación comprende un código que no tiene ninguna relación con la información personal. El código de verificación preferentemente no debe ser idéntico a ningún código de verificación generado por el servidor de autenticación en el pasado. Además preferentemente, después de que se ha generado el código de verificación, el servidor de autenticación suprime el código de verificación generado en un periodo de tiempo especificado previamente para deshabilitar la verificación.

La figura 1 es una vista que ilustra un procedimiento de autenticación individual según una realización de la presente invención como un todo, y un campo 20 cerrado por líneas de puntos muestra el estado en el que un lector 21 instalado en un punto para vender o proporcionar diversos productos y servicios o un lector (no se muestra) incorporado en una máquina de venta automática 22 o similar, y un servidor de gestión de ventas 23 para gestionar la máquina y lectores están conectados entre sí a través de una red 50, tal como Internet.

Convencionalmente, el pago con una tarjeta de crédito ordinaria o similar se realiza en este campo 20 y, en ese caso, una tarjeta de crédito es leída por el lector 21 o similar para el establecimiento de la autenticación individual.

En la figura 1, un servidor de terminal de telefonía móvil 31 para gestionar un grupo de terminales de telefonía móvil 30, 30,... está conectado a una red 50, y el grupo de terminales de telefonía móvil 30, 30,... y el servidor de terminal de telefonía móvil 31 están conectados entre sí por el aire 32. El número de referencia 10 indica un servidor de autenticación para proporcionar autenticación individual a cada terminal de telefonía móvil 30 en el grupo de terminales de telefonía móvil 30, 30,..., y el servidor de autenticación está conectado a la red 50 así como al servidor de gestión de ventas 23 a través de una línea dedicada 60.

En el procedimiento según la presente realización, cuando un propietario del terminal de telefonía móvil 30 realiza el pago por un artículo en venta o un servicio, o cuando el propietario trata de identificarse, el propietario usa el terminal de telefonía móvil 30 en lugar de una tarjeta de crédito, una tarjeta de débito, una tarjeta bancaria, u otros diversos tipos de certificados (tales como diversos tipos de tickets, tarjetas de ID, certificados de pagos y recibos), y los principios básicos se describen en referencia a la figura 2.

En un primer momento, cuando el propietario envía una petición de autenticación desde el terminal de telefonía móvil 30 al servidor de autenticación 10 (a través de una ruta 201), el servidor de autenticación 10 transmite el código de verificación para la autenticación al terminal de telefonía móvil 30 (a través de una ruta 202). El terminal de telefonía móvil 30 envía el código de verificación mediante el lector 21 o similar al servidor de gestión de ventas 23 (a través de una ruta 203). Este lector 21 es un tipo de lector no de contacto. El servidor de gestión de ventas 23 transmite el código de verificación al servidor de autenticación 10 para solicitar la autenticación (a través de una ruta 204). El servidor de autenticación 10 verifica el código de verificación con el código de verificación generado previamente, y devuelve un resultado de verificación e información personal requerida por el servidor de gestión de ventas 23 al servidor de gestión

de ventas 23 (a través de una ruta 205).

El código de verificación para autenticación es un código temporal y sin sentido generado de nuevo cuando se recibe una petición desde el terminal de telefonía móvil 30, y nunca se usa de nuevo no solamente en respuesta a otros terminales de telefonía móvil 30, sino ni siquiera aunque el mismo terminal de telefonía móvil 30 envíe una petición de autenticación la próxima vez. La expresión "código sin sentido" como se usa en este documento indica datos diferentes de datos de atributos tales como un número de afiliación fijo, ID, un nombre, una dirección, un número de teléfono, datos del producto, y datos encriptados de los mismos.

Debe observarse que un propio proveedor de un producto o servicio puede autenticar al propietario del terminal de telefonía móvil 30 como un usuario y el procesamiento por parte del servidor de autenticación 10 y el procesamiento por parte del servidor de gestión de ventas 23 se realizan en el mismo servidor.

Un flujo del código de verificación se describe a continuación de nuevo en referencia a la figura 1. Cuando un usuario realiza el pago por un producto o un servicio usando el lector 21, la máquina de venta automática 22, o similar conectada a la red 50 como medio de pago, en primer lugar se requiere autenticación individual.

El usuario que intenta realizar el pago solicita la transmisión de un código de verificación desde el terminal de telefonía móvil 30, que pertenece al usuario, al servidor de autenticación 10. Esta señal de solicitud es transmitida en forma de ondas eléctricas 32 bajo el control de la empresa de servicios de telefonía móvil, y llega al servidor de autenticación 10 mediante el servidor de terminal de telefonía móvil 31 que es un servidor de conversión de señales para conectarlo a la red 50.

El servidor de autenticación 10 genera un código de verificación para el usuario que realiza la solicitud, y transmite el código de verificación a través de la misma ruta de señal, pero en la dirección inversa. El terminal de telefonía móvil 30 que ha recibido el código de verificación hace que el lector 21 o similar lea el código de verificación en el estado sin contacto, y a continuación el código de verificación es transmitido a través de la red 50 al servidor de gestión de ventas 23.

El servidor de gestión de ventas 23 transmite el código de verificación al servidor de autenticación 10 para verificar el código de verificación recibido. La ruta de transmisión usada en esta etapa puede ser la red 50, pero la seguridad entre los servidores debe ser, de forma deseable, completa, y es preferible una ruta, tal como la línea dedicada 60, que no permite el acceso ilegal a ella.

El servidor de autenticación 10 verifica el código de verificación en la señal de verificación con el código de verificación generado previamente, y devuelve un resultado de la verificación y un contenido de la solicitud al servidor de gestión de ventas 23. Con esta etapa de retorno, se establece la autenticación individual, y el procedimiento posterior cambia al procedimiento ordinario específico para compañía de crédito o similar.

El "código de verificación" se describe a continuación en referencia a la figura 3 que muestra la configuración de los archivos de datos almacenados en el servidor de autenticación 10. En la figura 3, un archivo de datos 310 para autenticación individual que comprende un grupo de registros de datos cada uno para autenticación individual se registra en un medio de registro de datos 300 provisto en el servidor de autenticación 10. Comprendiendo cada registro de datos 320 para autenticación individual una ID de miembro 311 que es un número de ID para cada individuo y otro elemento 312, y el "código de verificación" 321 está presente como uno de los elementos.

Concretamente, el "código de verificación" 321 es una serie de datos presentes como un campo en el registro de datos 320 para autenticación individual en el archivo de datos 310 para autenticación individual que comprende un grupo de registros de datos almacenados en el medio de registro de datos 300 en el servidor de autenticación 10.

Debe observarse que estos datos son datos temporales que se generan en primer lugar cuando se recibe una señal de solicitud procedente del terminal de telefonía móvil 30, presente en un periodo de tiempo especificado previamente, y se suprimen cuando no se requiere una señal de verificación en un periodo de tiempo especificado previamente desde el servidor de gestión de ventas 23. Estos datos no son datos fijos, y se diferencian cada vez que se generan en el campo. Los datos son diferentes de datos fijos significativos tales como un registro de datos para autenticación individual.

La secuencia de operación desde la generación del "código de verificación" hasta la supresión del mismo en el servidor de autenticación 10 se describe en referencia a la figura 4.

En un primer momento, el servidor de autenticación 10 comprueba, cuando recibe una solicitud de código de verificación del terminal de telefonía móvil 30 propiedad de un miembro registrado (401), si el emisor es o no el miembro registrado.

Una vez que la autenticación del miembro se ha establecido, el servidor de autenticación 10 genera el "código de verificación" (402), y este código de verificación es verificado inmediatamente con los datos del historial de generación de códigos de verificación (403) para comprobar si el código de verificación es o no uno generado en el pasado (404). Cuando el código de verificación coincide con los datos correspondientes generados en el pasado, un código de verificación se genera de nuevo (405). Esta operación se realiza para impedir el riesgo que podría producirse si el código de verificación generado en el pasado fuera conocido por otra persona y la persona usara ilegalmente este código de verificación.

El código de verificación generado como se ha descrito anteriormente es emitido (406), y es transmitido al terminal de telefonía móvil 30 (407). A continuación, el código de verificación se pone bajo control mediante un temporizador o similar, y se suprime cuando se realiza la comprobación de una petición de verificación recibida del servidor de gestión de ventas 23 (408) y se determina mediante un temporizador o similar que una petición de verificación para el código de verificación no se ha recibido en un periodo de tiempo especificado previamente (412).

Cuando se determina que una petición de verificación se ha recibido desde el servidor de gestión de ventas 23 en el periodo de tiempo especificado previamente, el código de verificación recibido se verifica con el código generado en el pasado (410) con los datos personales solicitados transmitidos (411), y al mismo tiempo el "código de verificación" generado se suprime (412).

La figura 5 es un diagrama de bloques que muestra la configuración del servidor de autenticación 10. El servidor 10 comprende, como secciones componentes que deben disponerse generalmente para ejecutar el procesamiento, entrada/salida, y recepción y transmisión de diversos tipos de datos, una sección de control 520 para controlar las operaciones del servidor de autenticación 10 como un todo, una sección de procesamiento 530 para procesar datos, una interfaz de entrada/salida 510 conectada a diversos tipos de dispositivos de entrada/salida así como a la red 50 y similares, una sección de entrada 550 para recibir datos de la interfaz de entrada/salida 510, una sección de salida 560 para emitir datos, una sección de almacenamiento 540 para almacenar temporalmente en su interior datos durante el procesamiento de los datos, una sección de recepción 570 para recibir diversos tipos de datos, y una sección de transmisión 580 para transmitir diversos tipos de datos.

El servidor de autenticación 10 comprende adicionalmente, además de las secciones componentes que se proporcionarán habitualmente en su interior, una sección de determinación de la ID 502 para determinar una ID de una señal de solicitud o una señal de verificación, una sección de almacenamiento de la ID 503 para almacenar en su interior ID registradas, una sección de recuperación de datos registrados 504 para recuperar, a partir de un número de miembro registrado, información relativa al miembro, una sección de almacenamiento de información sobre el miembro 505 para almacenar en su interior información sobre la afiliación, tal como datos del código de verificación, una sección de generación de un código de verificación 506 para generar un nuevo código de verificación, una sección de comprobación del historial de códigos de verificación 507 para comprobar si los datos del nuevo código de verificación coinciden con cualquiera de los datos de código de verificación generados en el pasado, una sección de almacenamiento del historial de códigos de verificación 508 para almacenar en su interior datos del código de verificación generados en el pasado, sección de generación de datos de visualización 509 para convertir los datos del código de verificación en aquellos con un formato de visualización para un terminal de telefonía móvil, una sección de generación de datos de autenticación 511 para extraer y generar datos personales solicitados con una señal de verificación, una sección de control del temporizador del código de verificación 512 para controlar los datos del nuevo código de verificación como parte de una información sobre afiliación, una sección de generación de señal de transmisión 513 para convertir los datos personales generados en la sección de generación de datos de autenticación 511 en aquellos con un formato especificado previamente para el servidor de gestión de ventas 23, y una sección de comprobación del código de verificación 514 para comprobar si el código de verificación en una señal de verificación del servidor de gestión de ventas 23 coincide o no con cualquiera de los códigos de verificación almacenados en su interior.

Las acciones del servidor de autenticación 10 se describen a continuación.

En el servidor de autenticación 10, una señal de solicitud de un código de verificación desde el terminal de telefonía móvil 30 es transmitida mediante la interfaz 510 a la sección de recepción 570. Cuando la sección de procesamiento 530 recibe una orden procedente de la sección de control 520, la sección de procesamiento 530 envía a la sección de determinación de la ID 502 una pregunta para comprobar si la señal de solicitud es una señal registrada previamente, y a continuación la sección de determinación de la ID 502 verifica la señal de solicitud con los datos almacenados en la sección de almacenamiento de la ID 503, y cuando se determina que la señal recibida es una registrada, la sección de determinación de la ID 502 transfiere la señal a la sección de almacenamiento 540.

La señal de solicitud transferida es verificada por la sección de procesamiento 530 que ha recibido la orden de la sección de control 520 con la sección de recuperación de datos registrados 504 para comprobar a que ID de miembro 311 le corresponde la señal de solicitud, y la sección de recuperación de datos registrados 504 verifica la señal con la sección de almacenamiento de información sobre afiliación 505 y notifica a la sección de procesamiento 530 de los datos. La sección de procesamiento 530 que ha recibido los datos ordena a la sección de generación de un código de verificación 506 que genere nuevos datos del código de verificación en un campo del código de verificación de los datos correspondientes, y transfiere los nuevos datos del código de verificación generados a la sección de almacenamiento 540. A continuación, la sección de procesamiento 530 realiza una pregunta a la sección de verificación del historial de códigos de verificación 507 para comprobar si los nuevos datos del código de verificación están duplicados o no con cualesquiera datos del código de verificación generados en el pasado. La sección de verificación del historial de códigos de verificación 507 realiza una pregunta a la sección de almacenamiento del historial de códigos de verificación 508 y, cuando recibe que los nuevos datos del código de verificación están duplicados con cualesquiera generados en el pasado, la sección de verificación del historial de códigos de verificación 507 ordena de nuevo a la sección de generación de un código de verificación 506 que genere nuevos datos del código de verificación en el campo del código de verificación de los datos correspondientes, y repite esta operación hasta que se determina que el código de verificación recientemente generado no está duplicado con ningún código generado en el pasado.

Cuando la sección de procesamiento 530 recibe la información de que los datos del código de verificación recientemente generados no están duplicados con ningún código generado en el pasado, la secuencia de procesamiento cambia a la siguiente tarea y, en este caso, los datos del código de verificación se almacenan en la sección de almacenamiento de información sobre afiliación 505 y, al mismo tiempo, la sección de procesamiento 530 ordena a la sección de generación de datos de visualización 509 que convierta el formato de los datos en un formato especificado previamente descrito en lo sucesivo en este documento y transmita los datos con el formato convertido a la sección de almacenamiento 540. Los nuevos datos del código de verificación con el formato de datos que se ha convertido son transferidos por la sección de procesamiento 530 que ha recibido una orden de la sección de control 520 a la sección de transmisión 570, y son transmitidos desde ésta mediante la interfaz de entrada/salida 510 al terminal de telefonía móvil solicitante 30. A continuación, los nuevos datos del código de verificación se ponen bajo control por la sección de gestión del temporizador del código de verificación 512, y los nuevos datos del código de verificación son suprimidos automáticamente por la sección de gestión del temporizador del código de verificación 512 a menos que no se reciba una señal de verificación en un periodo de tiempo especificado previamente procedente del servidor de gestión de ventas 23.

El “código de verificación” sin sentido y no fijo como se ha descrito anteriormente debe disponerse cada vez que se usa el código, y se requiere un gran número de códigos de verificación. Sin embargo, en la pantalla que comprende letras y figuras, aunque esto depende de la capacidad de visualización de cada terminal de telefonía móvil, es concebible que una serie de dígitos visualizables de una vez sea de, como máximo, 100 dígitos, y un número de combinaciones sea de 36^{100}.

El procedimiento según la presente realización es para aumentar sustancialmente el “número de combinación”, y se proporciona una sección de generación de señal de imágenes para mostrar una imagen en el terminal de telefonía móvil 30 como la sección de generación de datos de visualización 509 del servidor de autenticación 10, y esta imagen mostrada se lee con el lector 21.

A continuación, el procedimiento según la presente realización se describe en referencia al caso en el que se realiza autenticación individual con el terminal de telefonía móvil 30 cuando un propietario del terminal de telefonía móvil 30 pasa a través de una puerta de embarque.

Como se muestra en la figura 6, cuando un propietario 62 del terminal de telefonía móvil 30 intenta pasar a través de una puerta de embarque 63, el propietario 62 tiene una pantalla de autenticación mostrada en el terminal de telefonía móvil 30 portado por el propietario 62. Como una imagen de la cara del propietario registrada previamente por el propietario en el servidor de autenticación 10 se muestra en colores, de modo que, cuando la pantalla de autenticación 61 se muestra a un guarda (o un portero) 64, la cara del propietario es verificada de forma visual con la imagen de la cara mostrada en el terminal de telefonía móvil 30 para la verificación, siendo de este modo identificado el propietario.

A continuación la persona 62 a autenticar coloca la pantalla de autenticación 61 del terminal de telefonía móvil 30 más cerca del lector 21 instalado en o cerca de la puerta de embarque 63 para hacer que el “código de verificación” mostrado en forma de puntos con colores específicos en la pantalla de autenticación 61 sea leído por el lector 21. Como se describe en lo sucesivo en este documento, una sección de análisis de información sobre puntos 102 para analizar la visualización de puntos está provista en el lector 21.

Cuando la comprobación se realiza por partida doble, concretamente de forma visual y con cualquier equipo, es posible salvar los límites de seguridad que depende solamente de un sistema, tales como los causados por la pérdida o el robo del terminal de telefonía móvil 30, o el chantaje. La imagen de visualización provista en la pantalla de autenticación 61 puede ser, además de una imagen de la cara del propietario, otra imagen, una ilustración, una foto o similares. La configuración es permisible en que una pantalla de cristal líquido o similar (no se muestra) está provista en la puerta de embarque 63 y la pantalla de autenticación 61 en el terminal de telefonía móvil 30 se muestra en la pantalla de cristal líquido o similar de modo que la comprobación visual puede realizarse por partida doble.

Como se conoce bien, una pantalla de cristal líquido del terminal de telefonía móvil 30 comprende una fina zona cuadrada (punto) como unidad, y se muestra mediante diversos colores generados en los puntos respectivamente. En esta realización, se generan colores específicos en una pluralidad de puntos especificados previamente que se proporcionan en una organización especificada previamente respectivamente, y el “código de verificación” se forma con una matriz de los colores específicos.

Concretamente, es posible dar valores de coordenadas a cada uno de los puntos 70, 70,... dispuestos de forma regular en las direcciones vertical y horizontal en la pantalla de cristal líquido como se muestra en la figura 7, y una combinación de los puntos de coordenadas formados con una pluralidad de puntos 70, 70,... se da como un código de verificación. En la descripción anterior, 1 punto se considera una unidad, pero una combinación de una pluralidad de puntos puede considerarse una unidad.

En la figura 7, en un primer momento, un campo de visualización formado con puntos 70, 70,... que constituyen cada uno el código de verificación se define mediante cuatro puntos, concretamente cualquier punto de partida 71, un segundo punto 72 que define un borde que es una línea de base horizontal que incluye el punto de partida 71, un tercer punto 73 que define otro borde que es una línea de base vertical que incluye el punto de partida 71, y un cuarto punto 74 situado en un punto de intersección de la línea vertical que incluye el segundo punto 72 y la línea horizontal que incluye el tercer punto 73. De este modo, una serie de puntos 77, 77,... que constituyen cada uno el código de verificación están presentes en la zona de visualización cuadrada.

En el punto de partida 71 y un punto de medición de la distancia horizontal 75 en la línea de base horizontal, una distancia entre puntos que varía para cada parte se mide en la pantalla de cristal líquido. Análogamente, en el punto de partida 71 y en un punto de medición de la distancia vertical 76 en la línea de base vertical, se mide una distancia entre puntos vertical en la pantalla de cristal líquido. Al medir las distancias entre puntos en la pantalla de cristal líquido, los puntos 77, 77,... pueden analizarse como puntos de coordenadas respectivamente, y pueden convertirse en el “código de verificación”.

Preferentemente, el color visualizado en el punto de partida 71, el segundo punto 72, el tercer punto 73, el cuarto punto 74, un color de visualización en los puntos 77, 77,..., y los colores de visualización en el punto de medición de la distancia horizontal 75 y el punto de medición de la distancia vertical 76 deben diferenciarse entre sí.

El procesamiento para extraer, analizar y convertir los puntos 77, 77,... que constituyen cada uno el código de verificación se describe a continuación en referencia al diagrama de flujo mostrado en la figura 8.

En un primer momento, el punto de partida 71, el segundo punto 72, el tercer punto 73 y el cuarto punto 74 en la pantalla de cristal líquido se extraen y se analizan (81), y la información obtenida sobre los puntos de coordenadas se almacena temporalmente en una sección de almacenamiento de coordenadas de un campo especificado (82). Análogamente, el punto de medición de la distancia horizontal 75 y el punto de medición de la distancia vertical 76 se extraen y se analizan (83), y la información sobre la distancia entre puntos obtenida se almacena temporalmente en una sección de almacenamiento de información sobre la distancia entre puntos respectivamente (84).

A continuación, se extraen los puntos 77, 77,... que constituyen cada uno el código de verificación (85), y los valores de coordenadas de los puntos 77, 77,... se analizan 86 mediante referencia a la información sobre la distancia entre puntos almacenada en la sección de almacenamiento de información sobre la distancia entre puntos (84). Los valores de coordenadas analizados se comprueban mediante referencia a la información sobre coordenadas almacenada en la sección de almacenamiento de coordenadas de campo especificado para determinar si los puntos de coordenadas están o no en el campo especificado (87). Los puntos de coordenadas que no están presentes en el campo especificado se suprimen (88), y solamente los valores de coordenadas para los puntos de coordenadas en el campo especificado se convierten (89) como el "código de verificación". Una organización de los puntos de coordenadas puede convertirse en una matriz de una pluralidad de valores de coordenadas, o en otras figuras, letras, o una mezcla de figuras y letras en base a una tabla de conversión de coordenadas.

La configuración de la sección de generación de señal de imágenes se describe a continuación.

La figura 9 es un diagrama de bloques que muestra principalmente una sección para generar una señal de imágenes en la sección de generación de datos de visualización 509 en el servidor de autenticación 10, y la sección comprende una sección de generación de información sobre puntos 91 para generar una imagen de organización de puntos con un color específico, una sección de almacenamiento de información sobre imágenes 92 con, por ejemplo, datos de una foto de la cara registrados previamente por cada usuario almacenados en su interior, y una sección de síntesis de información sobre imágenes 93 para sintetizar los dos tipos de imágenes.

En la figura 9, el código de verificación generado en la sección de generación de un código de verificación 506 en el servidor de autenticación 10 se pone bajo control mediante la sección de control 520 según una orden procedente de la sección de procesamiento 530, y es enviado a la sección de generación de información sobre puntos 91. La sección de generación de información sobre puntos 91 genera una imagen de puntos con una pluralidad de colores específicos organizados como se muestra en la figura 7 en base al código de verificación y según una norma especificada previamente. A continuación, la sección de síntesis de información sobre imágenes 93 busca una imagen de una foto de la cara de un miembro que ha solicitado la verificación desde la sección de almacenamiento de información sobre imágenes 92 y sintetiza la imagen de la foto de la cara con la imagen de puntos. La señal de imagen que incluye el "código de verificación" sintetizado es suministrada a la sección de procesamiento 530 según una orden procedente de la sección de control 520. Preferentemente, la imagen de la foto de la cara debe someterse al procesamiento para retirar los colores específicos que se han dado a la imagen de puntos antes de la etapa de sintetizado.

Los "colores específicos" pueden ser colores fijos específicamente, pero también pueden variar según algunas condiciones tales como, por ejemplo, una unidad como una fecha o momento de un día, o un propósito del uso.

La sección de análisis de información sobre puntos 102 se describe en referencia a un diagrama de bloques del lector 21 mostrado en la figura 10.

El lector 21 comprende una sección de lectura de imágenes 101 para leer una imagen mostrada en la pantalla de autenticación 61 del terminal de telefonía móvil 30, la sección de análisis de información sobre puntos 102 descrita anteriormente, una sección de transferencia de información sobre puntos 103 para transferir la señal convertida en el "código de verificación" a una sección especificada previamente descrita a continuación, y una sección de control 104 para controlar las secciones anteriores.

En la puerta de embarque 63, la información sobre la imagen sintetizada leída desde la sección de lectura de imágenes 101 del lector 21 se somete al procesamiento para extracción y análisis del "código de verificación" según cada color específico como una clave en la sección de análisis de información sobre puntos 102. La información que se ha convertido en el "código de verificación" es transferida por la sección de transferencia de información sobre puntos 103 a una sección que tiene una función de comunicación en la puerta de embarque 63, y es transmitida adicionalmente al servidor de gestión de ventas 23. Todos los controles en esta etapa se proporcionan desde las secciones de control 104.

El servidor de gestión de ventas 23 transmite la señal de verificación al servidor de autenticación 10, y el código de verificación es enviado mediante la sección de interfaz de entrada/salida 510 del servidor de autenticación 10 a la sección de recepción 570. La sección de procesamiento 530 realiza una pregunta a la sección de determinación de la ID 502, según una orden procedente de la sección de control 520, para comprobar si la señal de verificación corresponde o no a cualesquiera datos registrados previamente en el servidor de gestión de ventas 23 que tiene la conexión comercial con ella, y la sección de determinación de la ID 502 verifica la señal de verificación con los datos almacenados en la sección de almacenamiento de la ID 503 y transfiere la señal de verificación a la sección de almacenamiento 540 después de que se haya determinado que la señal corresponde a cualesquiera datos registrados en su interior.

A continuación, la sección de procesamiento 530 ordena a la sección de verificación del código de verificación 514 que verifique la señal de verificación transferida. La sección de verificación del código de verificación 514 extrae el código de verificación de la señal de verificación en la sección de almacenamiento 540, verifica el código de verificación con la sección de almacenamiento de información sobre afiliación 505 con el código de verificación almacenado en su interior, y devuelve la ID del miembro 311 a la sección de procesamiento 530 cuando se determine que el código de verificación corresponde a cualquier código almacenado en su interior.

La sección de procesamiento 530 que ha recibido la ID de miembro 311 ordena a la sección de generación de datos de autenticación 511 que extraiga y genere datos personales requeridos por la señal de verificación transferida desde la sección de almacenamiento de información sobre afiliación 505. Estos datos personales son transferidos por la sección de procesamiento 530 que ha recibido la orden de la sección de control 520 a la sección de almacenamiento 540. Los datos personales en la sección de almacenamiento 540 se convierten, después de una orden procedente de la sección de procesamiento 530 que ha recibido una orden procedente de la sección de control 520, en datos con un formato de señal previamente decidido por la sección de generación de señal de transmisión 513 tal como, por ejemplo,

un formato especificado previamente tal como aquellos basados en el sistema de encriptado de claves publicado o el sistema de encriptado de claves común, y son transferidos a la sección de transmisión 580, donde los datos se transmiten al servidor de gestión de ventas 23 que solicita los datos personales mediante la sección de interfaz de entrada/salida 510.

Como se ha descrito anteriormente, en la realización de la presente invención, se supone que el pinchado del cable puede realizarse de forma ilegal en una red que no tiene la seguridad en ella tal como Internet, y como contramedidas para establecer la seguridad, solamente se usan señales sin sentido generadas temporalmente para evitar la distribución de señales con sentido, y solamente se usan señales con sentido entre sistemas que han establecido la seguridad a un alto nivel respectivamente.

Con la realización descrita, es posible establecer una autenticación individual segura y rápida usando un terminal de telefonía móvil. Por lo tanto, no solamente es posible impedir accidentes tales como el robo de de datos fijos tales como tarjetas de crédito, tarjetas de débito, tarjetas bancarias y otros diversos tipos de certificados que pueden ser falsificados fácilmente así como errores en la decodificación de datos encriptados a partir de estos, sino también proporcionar un medio de pago extremadamente útil en actividades comerciales cibernéticas que se espera que crezcan sustancialmente en la figura.

Con la realización descrita, puede realizarse una autenticación individual fácil y rápida, y también datos para autenticación individual pueden transferirse entre un terminal de telefonía móvil y un lector en la forma sin contacto, de modo que problemas tales como daños físicos al terminal de telefonía móvil nunca se produzcan.

REIVINDICACIONES

1. Un procedimiento de autenticación individual que comprende las etapas de:

recibir en un servidor de autenticación una petición de un código de verificación desde una terminal de telefonía móvil de un usuario;

generar en el servidor de autenticación (10) un código de verificación que comprende una imagen de organización de puntos con una pluralidad de colores específicos, comprendiendo la imagen de organización de puntos un punto de partida (71), un segundo punto (72), un tercer punto (73) y un cuarto punto (74) que definen una zona de visualización rectangular, un punto de medición de la distancia horizontal (75), un punto de medición de la distancia vertical (76) y una pluralidad de puntos (77) en la zona de visualización rectangular que tienen valores de coordenadas, de modo que una combinación de los valores de coordenadas constituye el código de verificación;

recibir (202), en el terminal de telefonía móvil (30), el código de verificación generado por el servidor de autenticación (10) en respuesta a la petición (201) procedente del terminal de telefonía móvil (30);

visualizar el código de verificación recibido por el terminal de telefonía móvil como la imagen de organización de puntos;

recibir (203) en un servidor de gestión de ventas (23), mediante un lector de imágenes (21) conectado al servidor de gestión de ventas, el código de verificación procedente del terminal de telefonía móvil (30);

devolver (204) el código de verificación desde el servidor de gestión de ventas (23) al servidor de autenticación (10);

verificar, en el servidor de autenticación, el código de verificación generado en dicho servidor de autenticación (10) con el código de verificación transmitido desde el servidor de gestión de ventas (23); y

transmitir (205) información personal del individuo correspondiente al código de verificación a dicho servidor de gestión de ventas (23) desde el servidor de autenticación (10) cuando se determina que los dos tipos de código de verificación son idénticos;

en el que el código de verificación recibido por dicho terminal de telefonía móvil (30) se lee con el lector de imágenes que tiene un medio para analizar una visualización de puntos con colores específicos;

y en el que el lector de imágenes;

extrae y analiza el punto de partida (71), el segundo punto (72), el tercer punto (73) y el cuarto punto (74) para obtener información sobre las coordenadas de los mismos;

extrae y analiza el punto de medición de la distancia horizontal (75) y el punto de medición de la distancia vertical (76) para obtener información sobre la distancia entre puntos;

extrae los puntos (77) que constituyen el código de verificación, analiza los valores de coordenadas de los mismos usando la información sobre la distancia entre puntos, comprueba los valores de coordenadas analizados usando la información sobre las coordenadas de los puntos de partida, segundo, tercero y cuarto para determinar si los valores de coordenadas analizados de los puntos (77) están o no en la zona de visualización, y convierte los valores de coordenadas de los puntos en la zona de visualización en un código de verificación.

2. El procedimiento de autenticación individual según la reivindicación 1, en el que el color del punto de partida (71), el segundo punto (72), el tercer punto (73), el cuarto punto (74), el color los puntos (77) que constituyen el código de verificación y los colores del punto de medición de la distancia horizontal (75) y el punto de medición de la distancia vertical (76) se diferencian entre sí.

3. El procedimiento de autenticación individual según la reivindicación 2, en el que los colores varían según la fecha, el momento del día o el propósito de uso.

4. El procedimiento de autenticación individual según la reivindicación 1, en el que dicho código de verificación comprende un código que no tiene relación con dicha información personal.

5. El procedimiento de autenticación individual según la reivindicación 1, en el que dicho código de verificación no es idéntico a ningún código de verificación generado en el pasado en dicho servidor de autenticación (10).

6. El procedimiento de autenticación individual según la reivindicación 1, en el que dicho código de verificación se suprime en un periodo de tiempo especificado previamente después de la generación del mismo para deshabilitar la verificación.

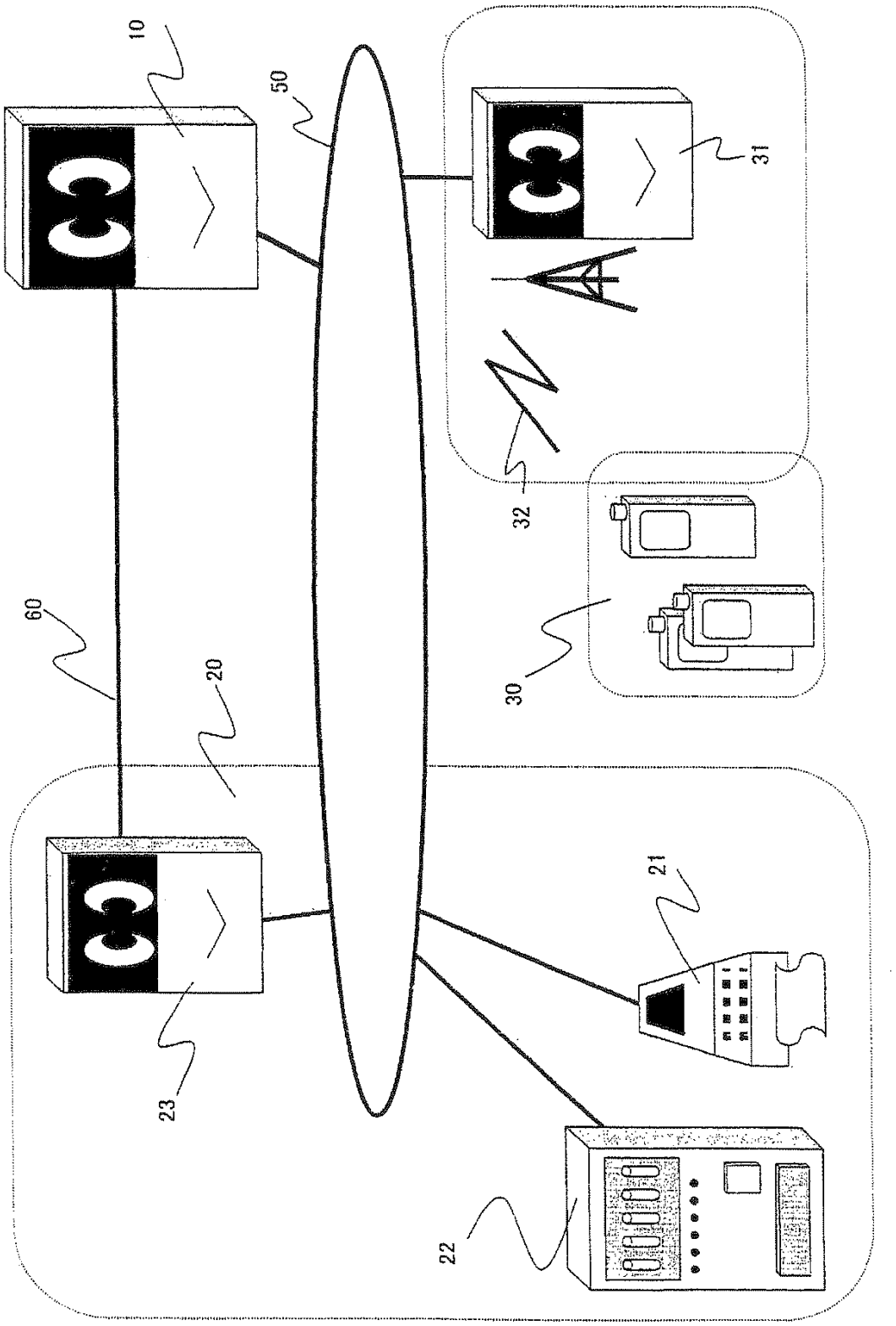


Fig.1

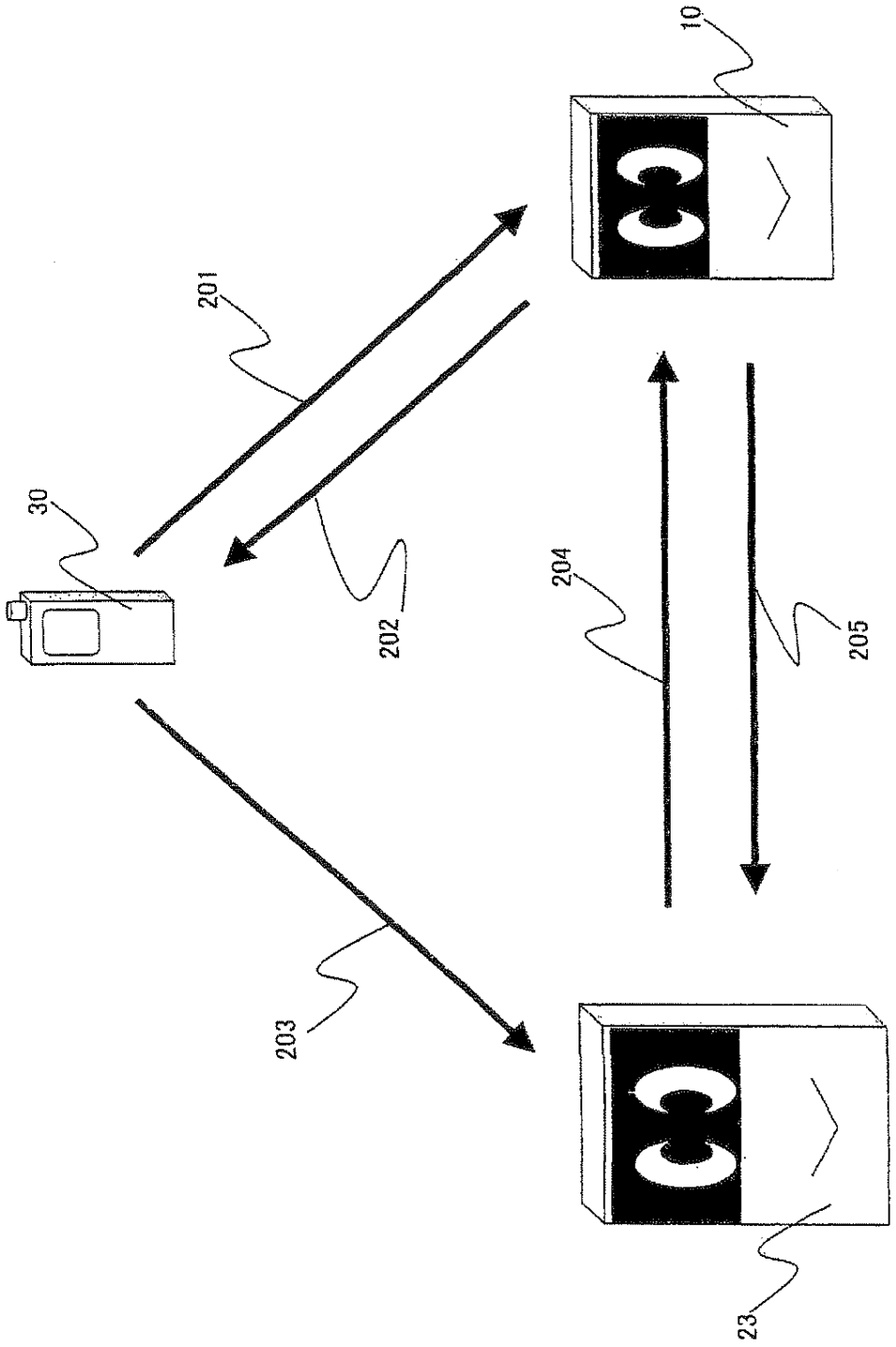


Fig.2

Fig.3

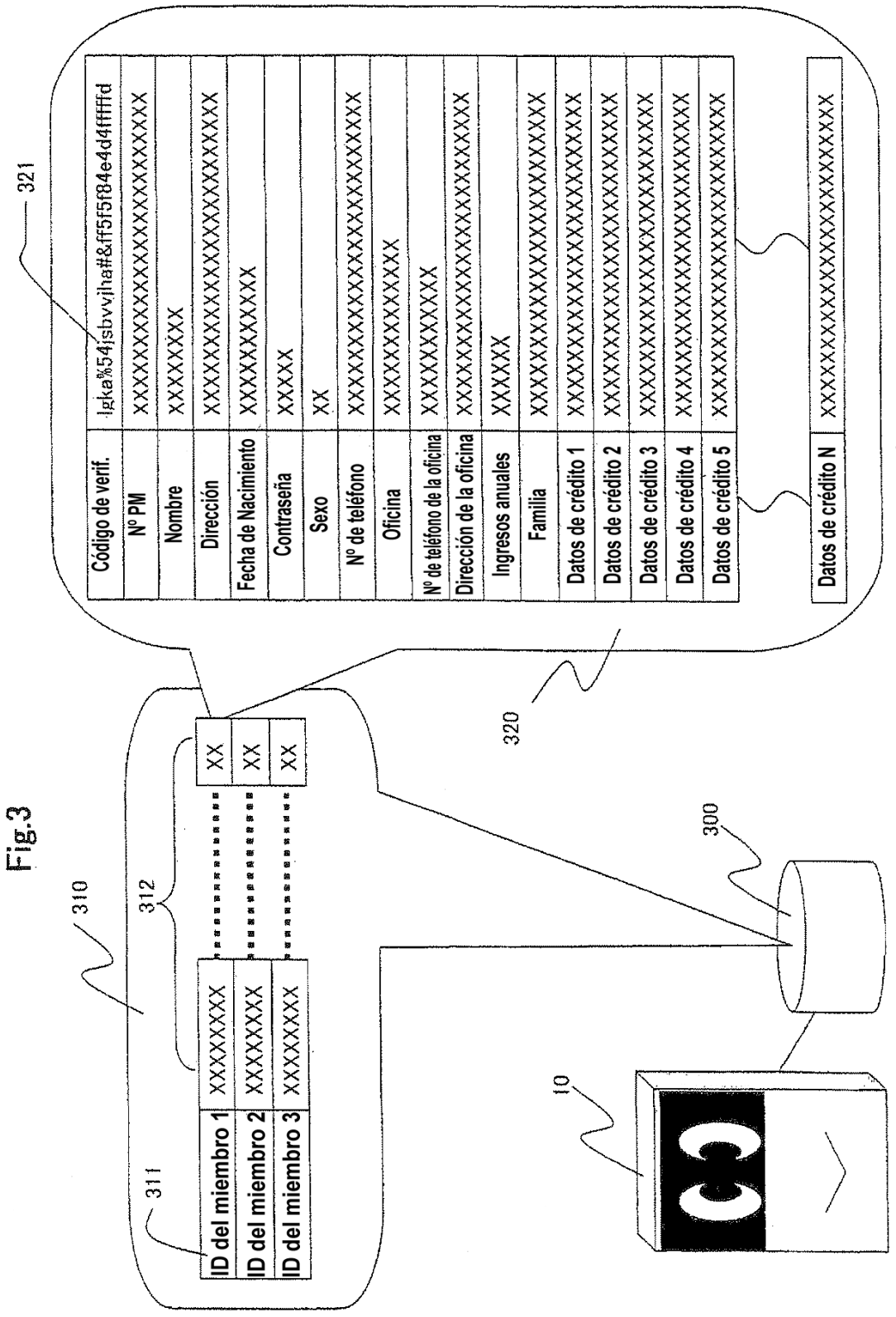

321
Código de verif.
lgka%54jsbvvjha#&ff5f5f84e4d4ffffffd
Nº PM
XXXXXXXXXXXXXXXXXXXXXXXXXX
Nombre
XXXXXXXX
Dirección
XXXXXXXXXXXXXXXXXXXXXXXXXX
Fecha de Nacimiento
XXXXXXXXXX
Contraseña
XXXXX
Sexo
XX
Nº de teléfono
XXXXXXXXXXXXXXXXXXXXXXXXX
Oficina
XXXXXXXXXXXXX
Nº de teléfono de la oficina
XXXXXXXXXX
Dirección de la oficina
XXXXXXXXXXXXXXXXXXXXXXXXX
Ingresos anuales
XXXXX
Familia
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 1
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 2
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 3
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 4
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 5
XXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito N
XXXXXXXXXXXXXXXXXXXXXXXXX
320
310
312
311
ID del miembro 1
XXXXXXXX
ID del miembro 2
XXXXXXXX
ID del miembro 3
XXXXXXXX
XX
XX
XX
300
10

Fig.4

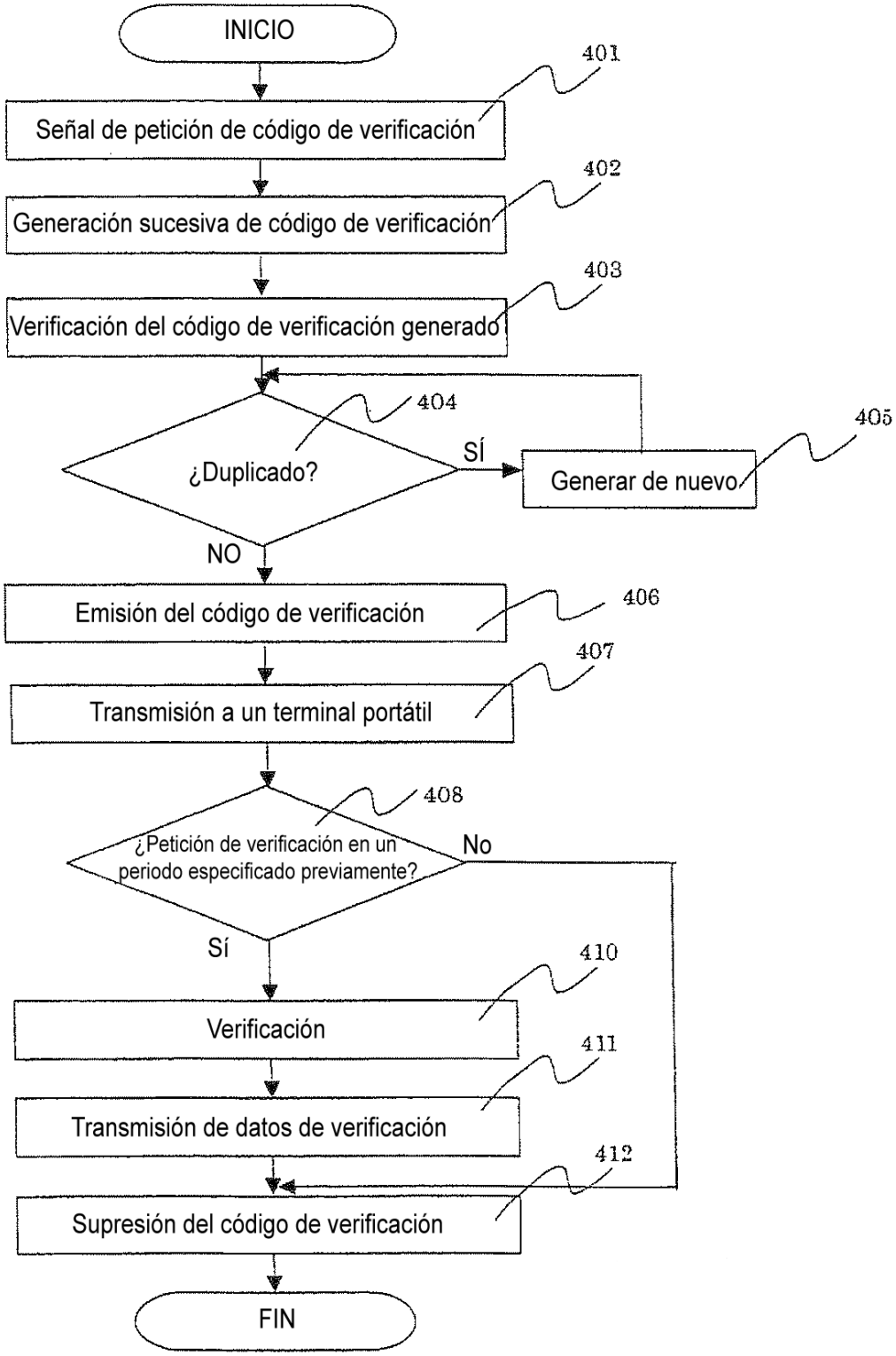
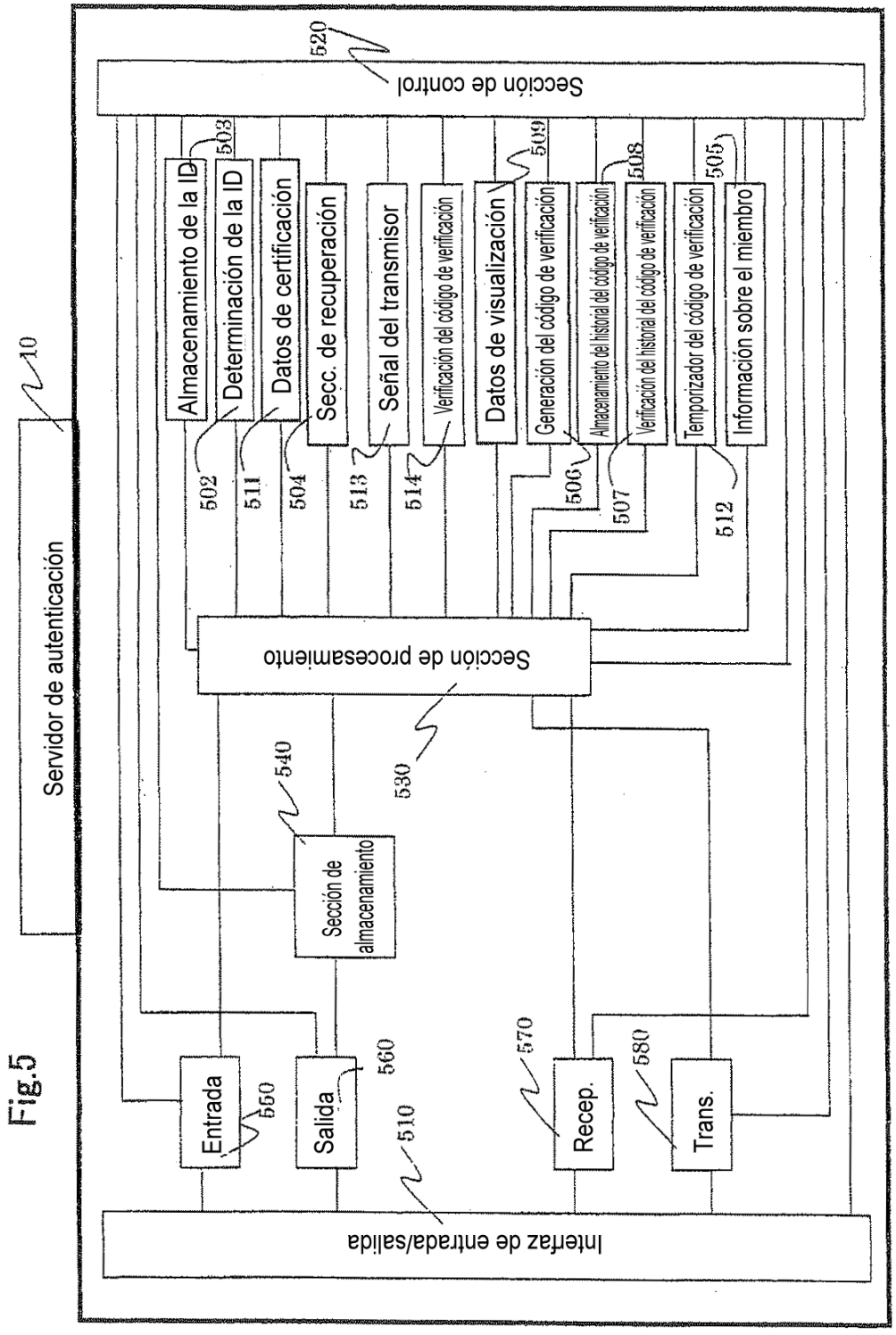

INICIO
401
Señal de petición de código de verificación
402
Generación sucesiva de código de verificación
403
Verificación del código de verificación generado
404
¿Duplicado?
SÍ
405
Generar de nuevo
NO
406
Emisión del código de verificación
407
Transmisión a un terminal portátil
408
¿Petición de verificación en un periodo especificado previamente?
No
Sí
410
Verificación
411
Transmisión de datos de verificación
412
Supresión del código de verificación
FIN

Fig.5


10
Servidor de autenticación
520
Sección de control
503
Almacenamiento de la ID
Determinación de la ID
Datos de certificación
Secc. de recuperación
Señal del transmisor
Verificación del código de verificación
Datos de visualización
Generación del código de verificación
Almacenamiento del historial del código de verificación
Verificación del historial del código de verificación
Temporizador del código de verificación
Información sobre el miembro
502
511
504
513
514
509
506
507
508
505
512
Sección de procesamiento
530
540
Sección de almacenamiento
Entrada
550
Salida
560
510
Recep.
570
Trans.
580
Interfaz de entrada/salida

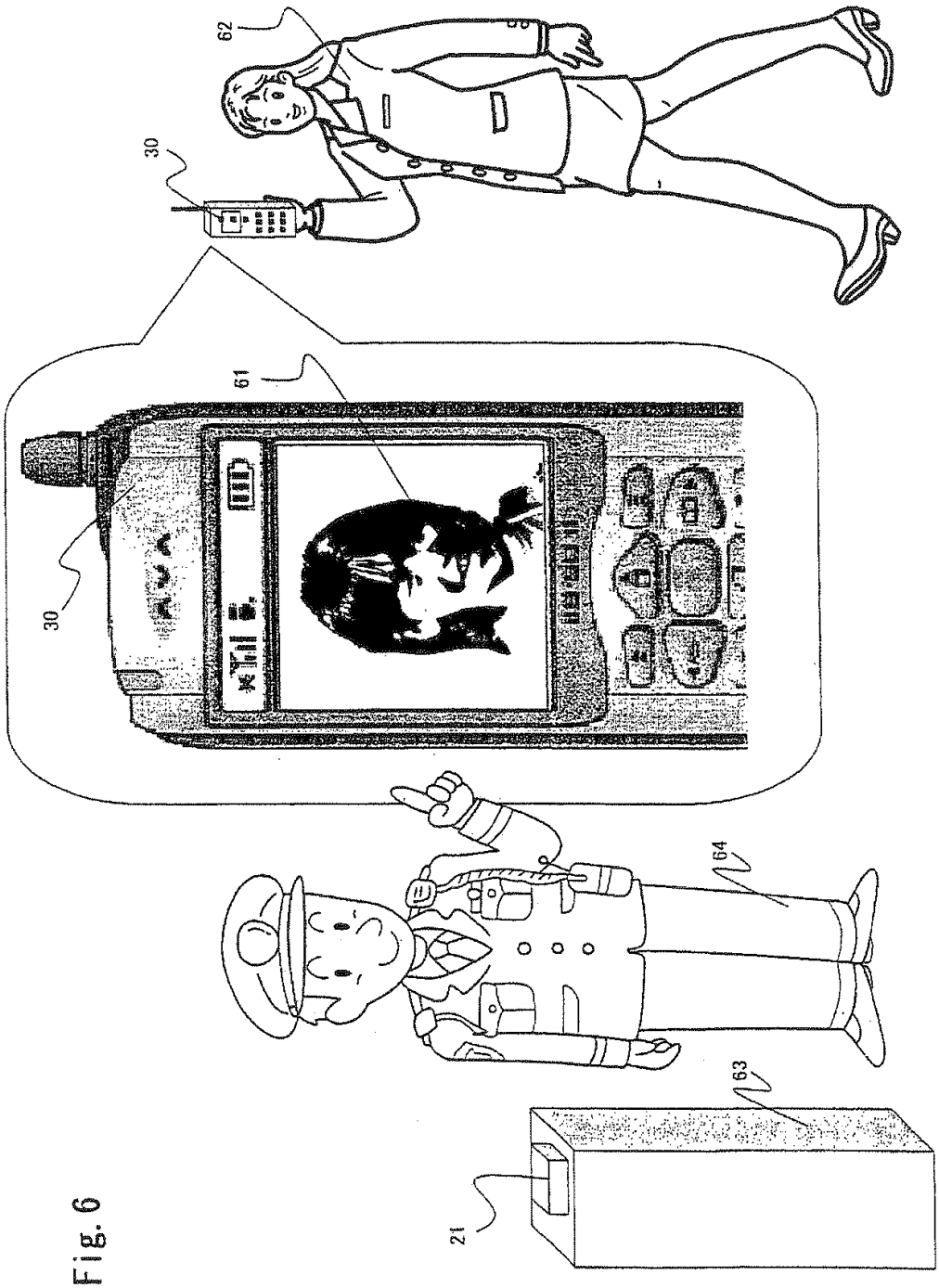


Fig. 6

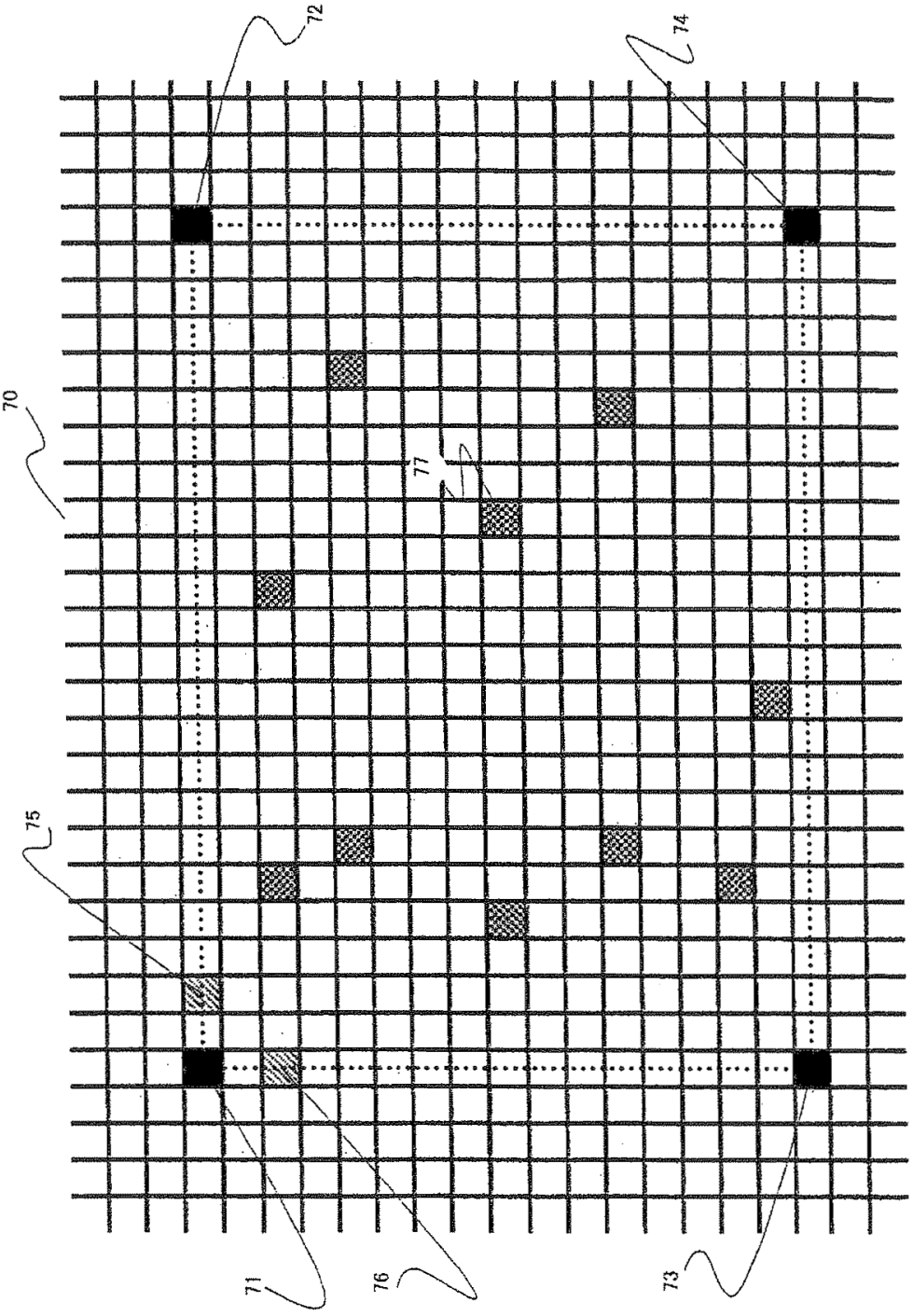
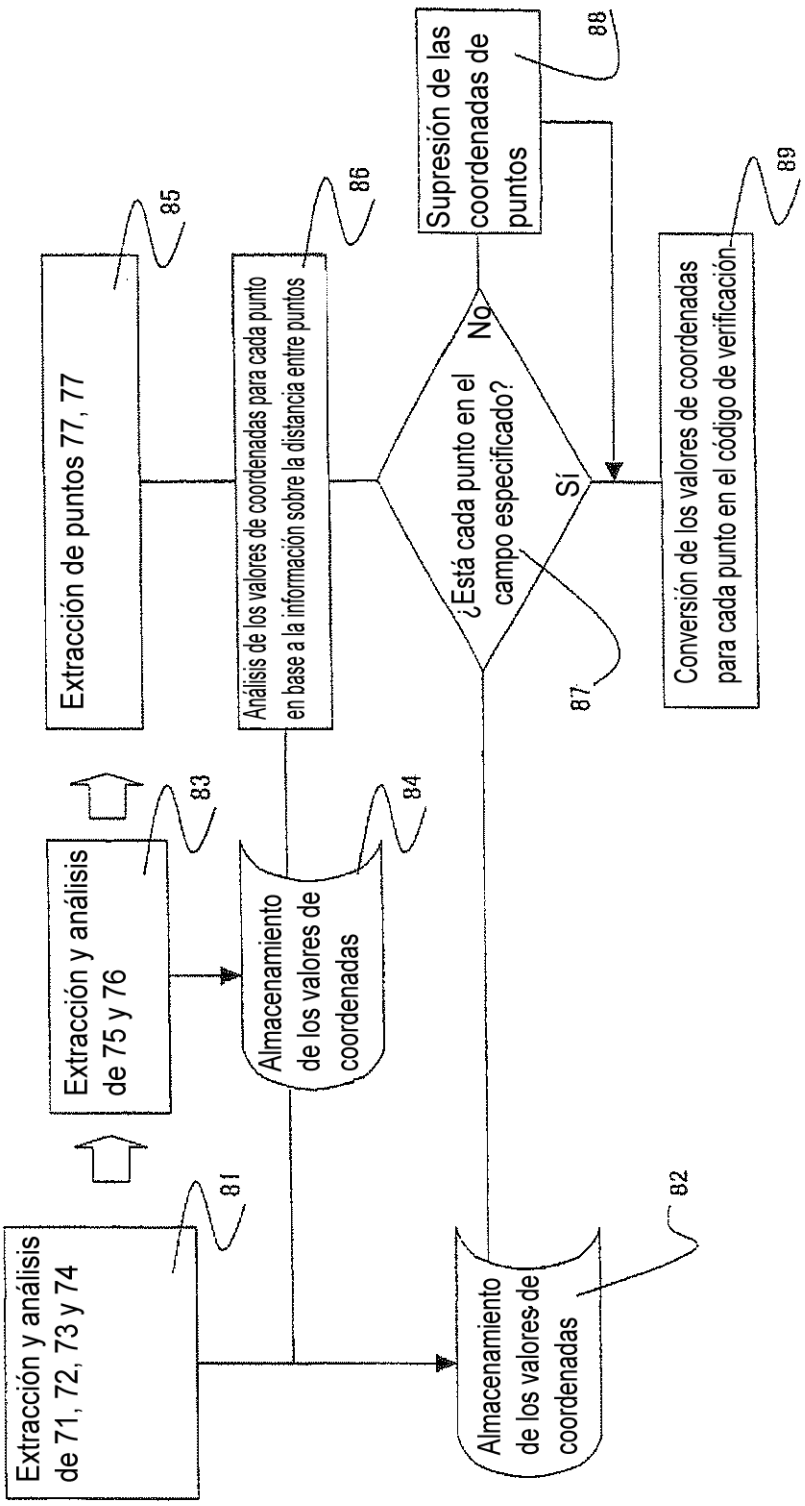


Fig. 7

Fig. 8


Extracción y análisis de 71, 72, 73 y 74
81
Extracción y análisis de 75 y 76
83
Extracción de puntos 77, 77
85
Almacenamiento de los valores de coordenadas
84
Análisis de los valores de coordenadas para cada punto en base a la información sobre la distancia entre puntos
86
Almacenamiento de los valores de coordenadas
82
¿Está cada punto en el campo especificado?
No
Sí
87
Supresión de las coordenadas de puntos
88
Conversión de los valores de coordenadas para cada punto en el código de verificación
89

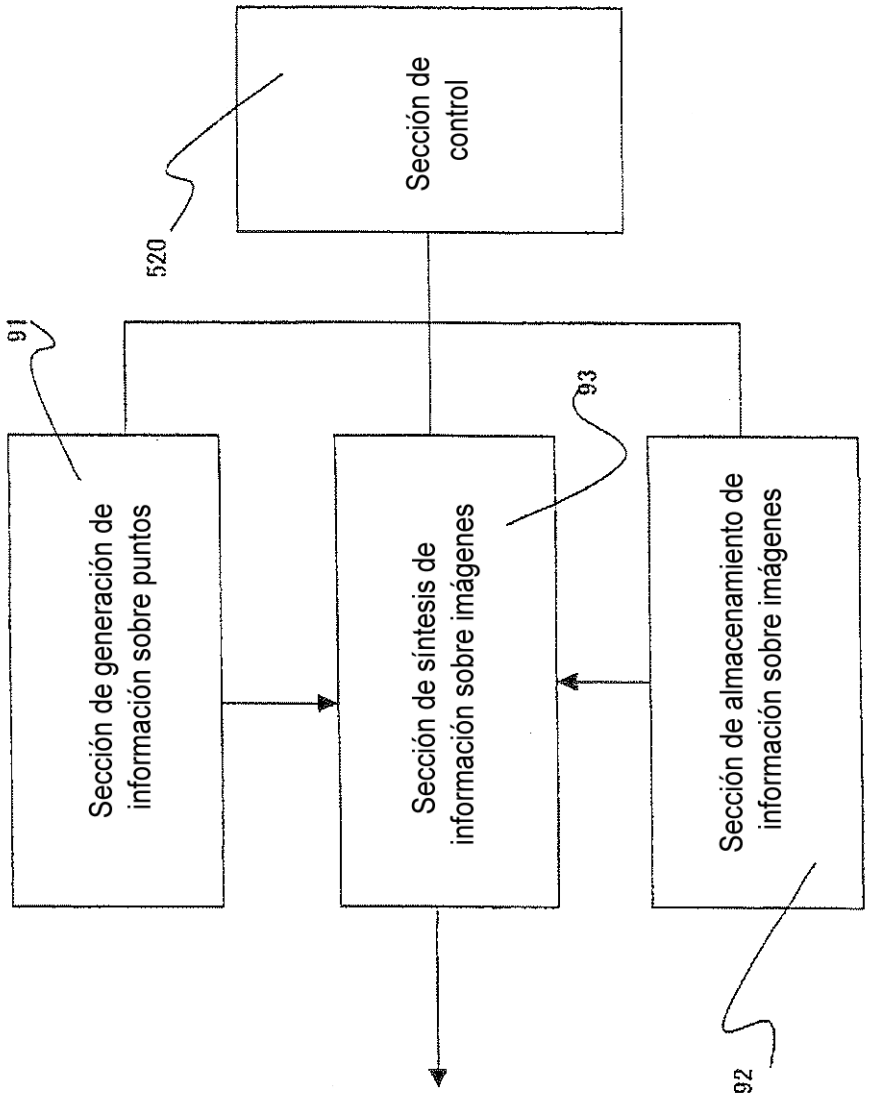

Sección de control
520
91
93
Sección de generación de información sobre puntos
Sección de síntesis de información sobre imágenes
Sección de almacenamiento de información sobre imágenes
92

Fig. 9

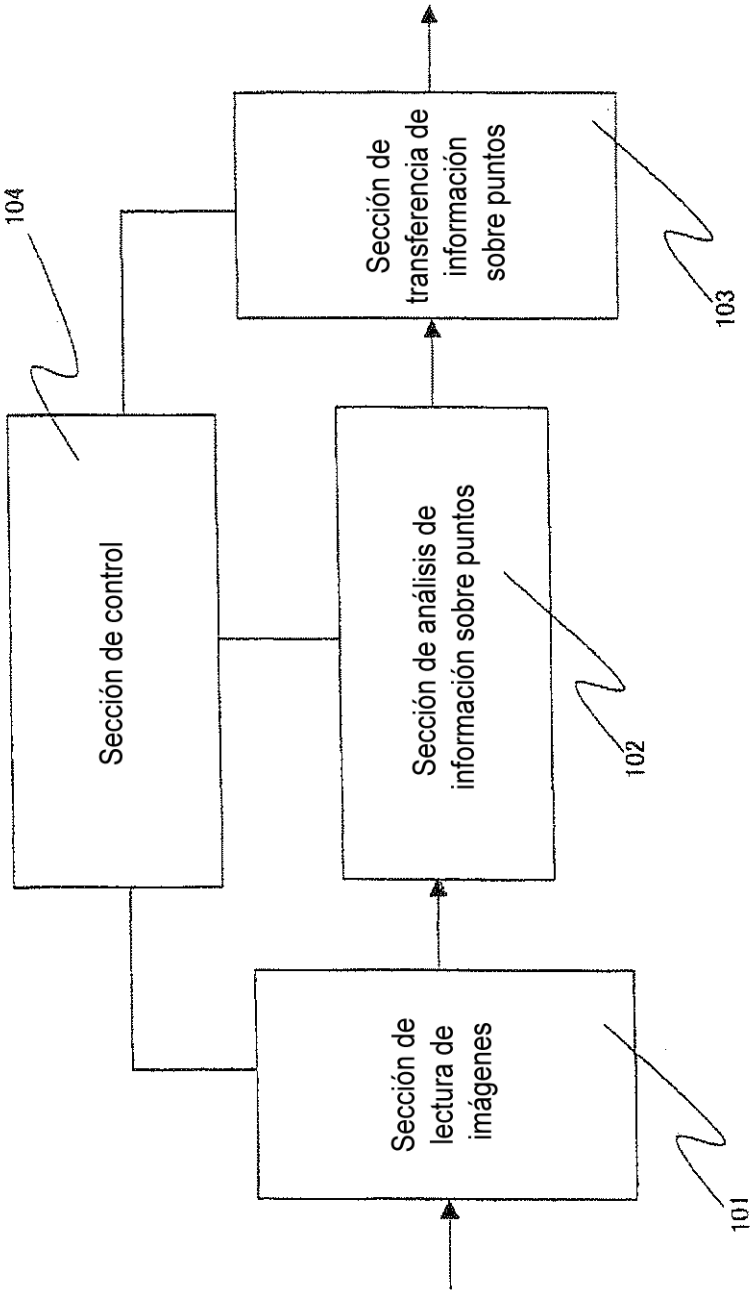

Sección de transferencia de información sobre puntos
103
104
Sección de control
Sección de análisis de información sobre puntos
102
Sección de lectura de imágenes
101

Fig. 10