(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 399 745**

(51) Int. Cl.:

***G07C 9/00*** (2006.01)
***G06F 15/00*** (2006.01)
***G06Q 20/00*** (2012.01)
***G07F 7/10*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.09.2002** **E 02797558 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.11.2012** **EP 1434140**

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

(30) Prioridad:

**03.09.2001 JP 2001265929**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**03.04.2013**

(73) Titular/es:

**KABUSHIKI KAISHA EIGHTING (100.0%)**
**20-14, Minamioui 6-chome, Shinagawa-ku**
**Tokyo , JP**

(72) Inventor/es:

**FUJISAWA, TOMONORI y**
**SATOU, SHOJI**

(74) Agente/Representante:

**FÚSTER OLAGUIBEL, Gustavo Nicolás**

**ES 2 399 745 T3**

## 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.

### TÉCNICA ANTERIOR

Convencionalmente la autenticación individual se ha realizado principalmente usando una tarjeta de plástico con una banda magnética adherida a ella, como representa 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 es conocido, como procedimiento de autenticación individual utilizando 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 lo que respecta a 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.

En el documento WO 01/41081 se dan 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. La invención permite al usuario pedir una credencial de un sistema de emisión de credenciales, recibir la credencial 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.

### DESCRIPCIÓN DE LA INVENCIÓN

La presente invención proporciona un procedimiento de autenticación individual seguro y rápido usando un terminal de telefonía móvil, en el que se utiliza temporalmente entre redes en las que no se ha establecido la seguridad información de señal sin sentido y no fija.

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

Preferentemente, el código de verificación recibido por el terminal de telefonía móvil se lee con un lector de imágenes que tiene un medio para analizar un patrón de puntos con colores específicos, y que está conectado al servidor de gestión de ventas. Preferentemente, cada punto con un color específico proporción información acerca de coordenadas. 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. Más 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.

### 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 de la presente invención;

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 ampliada de una pantalla de autenticación de un terminal 30 de telefonía móvil 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 509 de generación de datos de visualización del servidor 10 de autenticación en la que se genera una señal de imagen; y

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

**REALIZACIONES DE LA INVENCIÓN**

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

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 22 de venta automática o similar, y un servidor 23 de gestión de ventas para gestionar la máquina y los 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 31 de telefonía móvil 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 31 de telefonía móvil 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 23 de gestión de ventas a través de una línea 60 dedicada.

En el procedimiento según la 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 30 de telefonía móvil 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 30 de telefonía móvil al servidor 10 de autenticación (a través de una ruta 201), el servidor 10 de autenticación transmite el código de verificación para la autenticación al terminal 30 de telefonía móvil (a través de una ruta 202). El terminal 30 de telefonía móvil envía el código de verificación mediante el lector 21 o similar al servidor 23 de gestión de ventas (a través de una ruta 203). Este lector 21 es un tipo de lector sin contacto. El servidor 23 de gestión de ventas transmite el código de verificación al servidor 10 de autenticación para solicitar la autenticación (a través de una ruta 204). El servidor 10 de autenticación 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 23 de gestión de ventas al servidor 23 de gestión de ventas (a través de una ruta 205).

El código de verificación para autenticación es un código temporal y sin sentido generado de nuevo cada vez que se recibe una petición desde el terminal 30 de telefonía móvil, y nunca se usa de nuevo no solamente en respuesta a otros terminales 30 de telefonía móvil, sino tampoco aunque el mismo terminal 30 de telefonía móvil envíe una petición de autenticación la próxima vez. La expresión “código sin sentido” utilizada 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 el propio proveedor de un producto o servicio puede autenticar al propietario del terminal 30 de telefonía móvil como un usuario y el procesamiento por parte del servidor 10 de autenticación y el procesamiento por parte del servidor 23 de gestión de ventas se realizan en el mismo servidor.

El 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 22 de venta automática, 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 30 de telefonía móvil, que pertenece al usuario, al servidor 10 de autenticación. Esta señal de solicitud es transmitida en forma de ondas 32 eléctricas bajo el control de la empresa de servicios de telefonía móvil, y llega al servidor 10 de autenticación a través el servidor 31 de terminal de telefonía móvil que es un servidor de conversión de señales para la conexión a la red 50.

El servidor 10 de autenticación 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 el sentido inverso. El terminal 30 de telefonía móvil 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 23 de gestión de ventas.

El servidor 23 de gestión de ventas transmite el código de verificación al servidor 10 de autenticación 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 60 dedicada, que no permite el acceso ilegal a ella.

El servidor 10 de autenticación 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 23 de gestión de ventas. Con esta etapa de retorno, se establece la autenticación individual, y el procedimiento posterior cambia al procedimiento ordinario específico para cada 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 10 de autenticación. En la figura 3, un archivo 310 de datos para autenticación individual que comprende un grupo de registros de datos, cada uno para autenticación individual, se registra en un medio 300 de registro de datos dispuesto en el servidor 10 de autenticación. Comprendiendo cada registro 320 de datos 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 un elemento de los datos presente como un campo en el registro 320 de datos para autenticación individual en el archivo 310 de datos para autenticación individual que comprende un grupo de registros de datos almacenados en el medio 300 de registro de datos en el servidor 10 de autenticación.

Debe observarse que estos datos son datos temporales que se generan en primer lugar cuando se recibe una señal de solicitud procedente del terminal 30 de telefonía móvil, presente dentro de un periodo de tiempo especificado previamente, y se suprimen cuando no se requiere una señal de verificación dentro de un periodo de tiempo especificado previamente desde el servidor 23 de gestión de ventas. 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 operaciones desde la generación del "código de verificación" hasta la supresión del mismo en el servidor 10 de autenticación se describe en referencia a la figura 4.

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

Una vez se ha establecido la autenticación del miembro, el servidor 10 de autenticación genera el "código de verificación" (402), y este código de verificación es verificado inmediatamente con los datos del historial (403) de generación de códigos de verificación para comprobar si el código de verificación ya se ha generado en el pasado o no (404). Cuando el código de verificación coincide con los datos correspondientes generados en el pasado, se genera de nuevo un código de verificación (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 30 de telefonía móvil (407). A continuación, el código de verificación se pone bajo control mediante un temporizador o similar, y se suprime cuando la comprobación de una petición de verificación es recibida del servidor 23 de gestión de ventas (408) y se determina mediante un temporizador o similar que una petición de verificación para el código de verificación no se ha recibido dentro de un periodo de tiempo especificado previamente (412). Cuando se determina que una petición de verificación se ha recibido desde el servidor 23 de gestión de ventas dentro del 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 10 de autenticación. 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 520 de control para controlar las operaciones del servidor 10 de autenticación como un todo, una sección 530 de procesamiento para procesar datos, una interfaz 510 de entrada / salida conectada a diversos tipos de dispositivos de entrada / salida así como a la red 50 y similares, una sección 550 de entrada para recibir datos de la interfaz 510 de entrada / salida, una sección 560 de salida para emitir datos, una sección 540 de almacenamiento para almacenar temporalmente en su interior datos durante el procesamiento de los datos, una sección 570 de recepción para recibir diversos tipos de datos, y una sección 580 de transmisión para transmitir diversos tipos de datos.

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

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

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

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

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

El “código de verificación” sin sentido y no fijo que se ha descrito anteriormente debe eliminarse cada vez que se usa el código, y se requiere un gran número de códigos de verificación para llevar a cabo las realizaciones de la presente invención. Sin embargo, en la pantalla que comprende letras y figuras, aunque esto depende de la capacidad de representación de datos 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 30 de telefonía móvil como la sección 509 de generación de datos de visualización del servidor 10 de autenticación, y esta imagen mostrada se lee con el lector 21.

A continuación, se describe el procedimiento según la presente realización haciendo referencia al caso en el que autenticación individual realizada con el terminal 30 de telefonía móvil 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 30 de telefonía móvil intenta pasar a través de una puerta 63 de embarque, el propietario 62 tiene una pantalla de autenticación mostrada en el terminal 30 de telefonía móvil portado por el propietario 62. Como una imagen de la cara del propietario registrada previamente por el propietario en el servidor 10 de autenticación se muestra en colores, de modo que, cuando la

pantalla 61 de autenticación 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 30 de telefonía móvil para la verificación, siendo de este modo identificado el propietario.

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

Cuando la comprobación se realiza por partida doble, concretamente de forma visual y con cualquier equipo, es posible salvar los límites de seguridad que dependen solamente de un sistema, tales como los causados por la pérdida o el robo del terminal 30 de telefonía móvil, o el chantaje. La imagen de visualización provista en la pantalla 61 de autenticación puede ser, además de una imagen de la cara del propietario, otra imagen, una ilustración, una foto o similares. Es admisible una configuración en que una pantalla de cristal líquido o similar (no se muestra) esté dispuesta en la puerta 63 de embarque y la pantalla 61 de autenticación en el terminal 30 de telefonía móvil 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 30 de telefonía móvil comprende una fina zona cuadrada (punto) como una unidad, y se muestra una imagen generando diversos colores en los puntos respectivamente. En esta realización, se generan colores específicos en una pluralidad de puntos especificados previamente que se disponen según 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,… constituye 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 71 de partida, un segundo punto 72 que define un borde que es una línea de base horizontal que incluye el punto 71 de partida, un tercer punto 73 que define otro borde que es una línea de base vertical que incluye el punto 71de partida, 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 71 de partida y un punto 75 de medición de la distancia horizontal en la línea de base horizontal, se mide en la pantalla de cristal líquido una distancia entre puntos que varía para cada parte. Análogamente, en el punto 71 de partida y en un punto 76 de medición de la distancia vertical en la línea de base vertical, en la pantalla de cristal líquido se mide una distancia vertical entre puntos. 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 71de partida, 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 75 de medición de la distancia horizontal y el punto 76 de medición de la distancia vertical 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 71 de partida, 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 75 de medición de la distancia horizontal y el punto 76 de medición de la distancia vertical 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 mediante referencia a la información sobre la distancia entre puntos almacenada en la sección de almacenamiento de información sobre la distancia entre puntos (86). Los valores de coordenadas analizados se comprueban mediante referencia a la información sobre coordenadas almacenada en la sección de almacenamiento de coordenadas de campo especificada 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 dentro del 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 509 de generación de datos de visualización en el servidor 10 de autenticación, y la sección

comprende una sección 91 de generación de información sobre puntos para generar una imagen de organización de puntos con un color específico, una sección 92 de almacenamiento de información sobre imágenes con, por ejemplo, datos de una foto de la cara registrados previamente por cada usuario almacenados en su interior, y una sección 93 de síntesis de información sobre imágenes para sintetizar los dos tipos de imágenes.

En la figura 9, el código de verificación generado en la 506 sección de generación de un código de verificación en el servidor 10 de autenticación se pone bajo control mediante la sección 520 de control según una orden procedente de la sección 530 de procesamiento, y es enviado a la sección 91 de generación de información sobre puntos. La sección 91 de generación de información sobre puntos 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 93 de síntesis de información sobre imágenes busca una imagen de una foto de la cara de un miembro que ha solicitado la verificación desde la sección 92 de almacenamiento de información sobre imágenes 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 530 de procesamiento según una orden procedente de la sección 520 de control. 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 102 de análisis de información sobre puntos se describe en referencia a un diagrama de bloques del lector 21 mostrado en la figura 10.

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

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

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

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

La sección 530 de procesamiento que ha recibido la ID 311 de miembro ordena a la sección 511 de generación de datos de autenticación que extraiga y genere datos personales requeridos por la señal de verificación transferida desde la sección 505 de almacenamiento de información sobre afiliación. Estos datos personales son transferidos por la sección 530 de procesamiento que ha recibido la orden de la sección 520 de control a la sección 540 de almacenamiento. Los datos personales en la sección 540 de almacenamiento se convierten, después de una orden procedente de la sección 530 de procesamiento que ha recibido una orden procedente de la sección 520 de control, en datos con un formato de señal previamente decidido por la sección 513 de generación de señal de transmisión tal como, por ejemplo, un formato especificado previamente tal como aquellos basados en el sistema de encriptado de claves publicadas o el sistema de encriptado de claves común, y son transferidos a la sección 580 de transmisión, donde los datos se transmiten al servidor 23 de gestión de ventas que solicita los datos personales mediante la sección 510 de interfaz de entrada / salida.

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 realizaciones de la invención, 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.

Con realizaciones de la invención, 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 nunca se produzcan problemas tales como daños físicos al terminal de telefonía móvil.

Con realizaciones de la invención, es posible mejorar adicionalmente la seguridad.

**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 un terminal de telefonía móvil de un usuario;

generar en el servidor (10) de autenticación un código de verificación representado por una imagen de una organización de puntos con una pluralidad de colores específicos, buscar una imagen de una foto de la cara del usuario registrada previamente por el usuario y almacenada en el servidor de autenticación, y sintetizar la imagen de la foto de la cara con la imagen de puntos;

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

mostrar la imagen sintetizada en el terminal de telefonía móvil de modo que la imagen de la foto de la cara se muestre con dicho código de verificación, donde es posible verificar visualmente la cara del usuario con la imagen de la foto de la cara mostrada en el terminal de telefonía móvil para verificación;

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

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

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

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

2. El procedimiento de autenticación individual según la reivindicación 1, en el que el código de verificación recibido por dicho terminal (30) de telefonía móvil es leído con un lector de imágenes que tiene un medio para analizar una visualización de puntos con colores específicos y conectarse a dicho servidor de gestión de ventas.

3. El procedimiento de autenticación individual según la reivindicación 1, en el que cada dicho punto con un color específico proporciona información sobre coordenadas.

4. El procedimiento de autenticación individual según una cualquiera de las reivindicaciones 1 – 3, en el que la imagen de organización de puntos incluye puntos que comprenden un punto (71) de partida, un segundo punto (72), un tercer punto (73) y un cuarto punto (74) que definen un campo de visualización rectangular,

5. El procedimiento de autenticación individual según la reivindicación 4, en el que la imagen de organización de puntos incluye, además, puntos que definen un punto (75) de medición de la distancia horizontal y un punto (76) de medición de la distancia vertical.

6. El procedimiento de autenticación individual según la reivindicación 5, en el que puntos (77) dentro del campo de visualización constituyen el código de verificación y, midiendo las distancias entre puntos (77), los puntos (77) pueden analizarse y convertirse en el código de verificación.

7. El procedimiento de autenticación individual según la reivindicación 6, en el que el color mostrado en el punto (71) de partida, el segundo punto (72), el tercer punto (73), el cuarto punto (74), los puntos (75, 76) de medición y los puntos (77) del código de verificación se diferencian todos entre sí.

8. 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.

9. 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 (10) de autenticación.

10. 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.

11. El procedimiento de autenticación individual según cualquier reivindicación anterior, en el que el código de verificación es un código sin sentido.

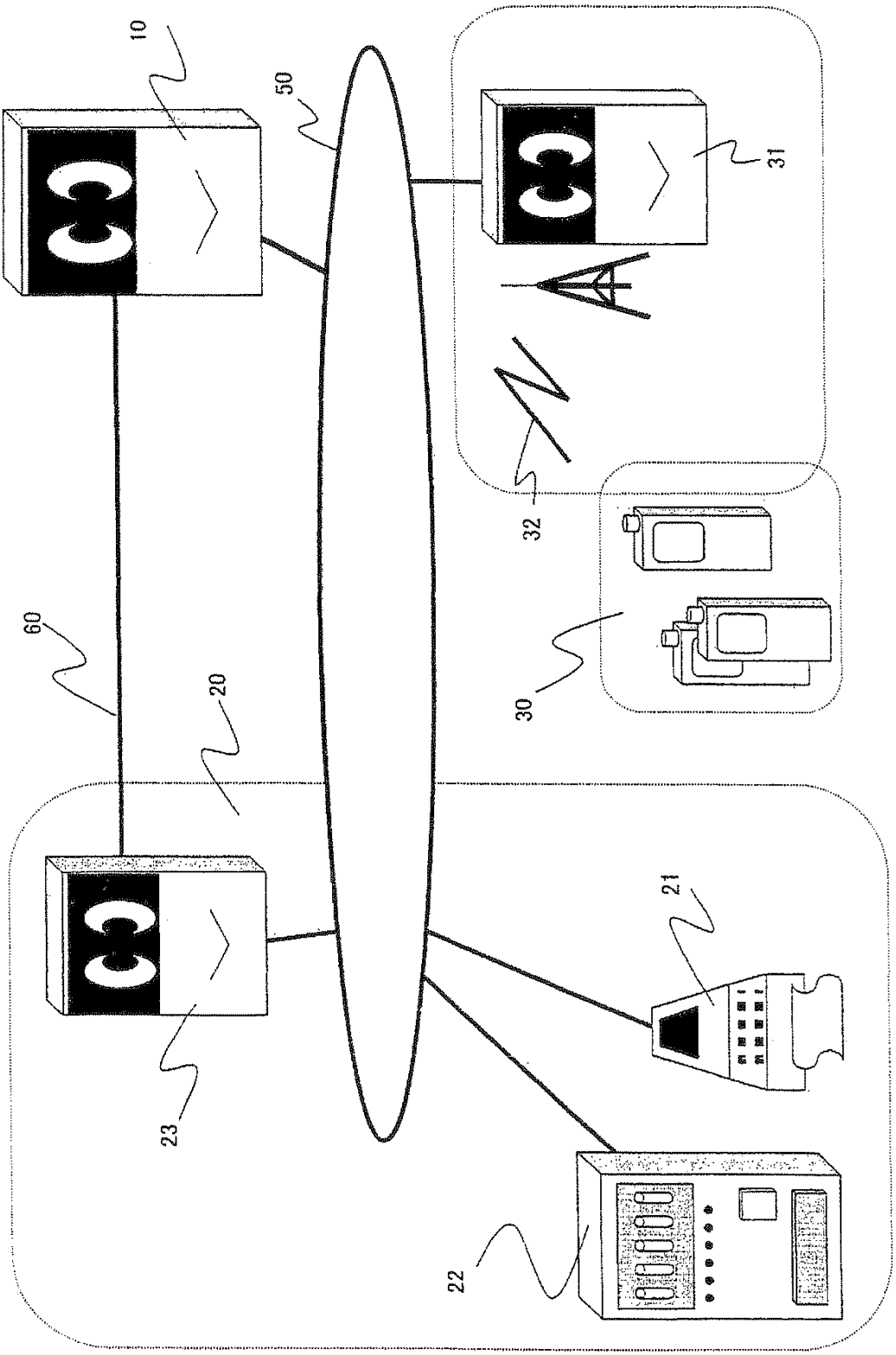



Fig.1

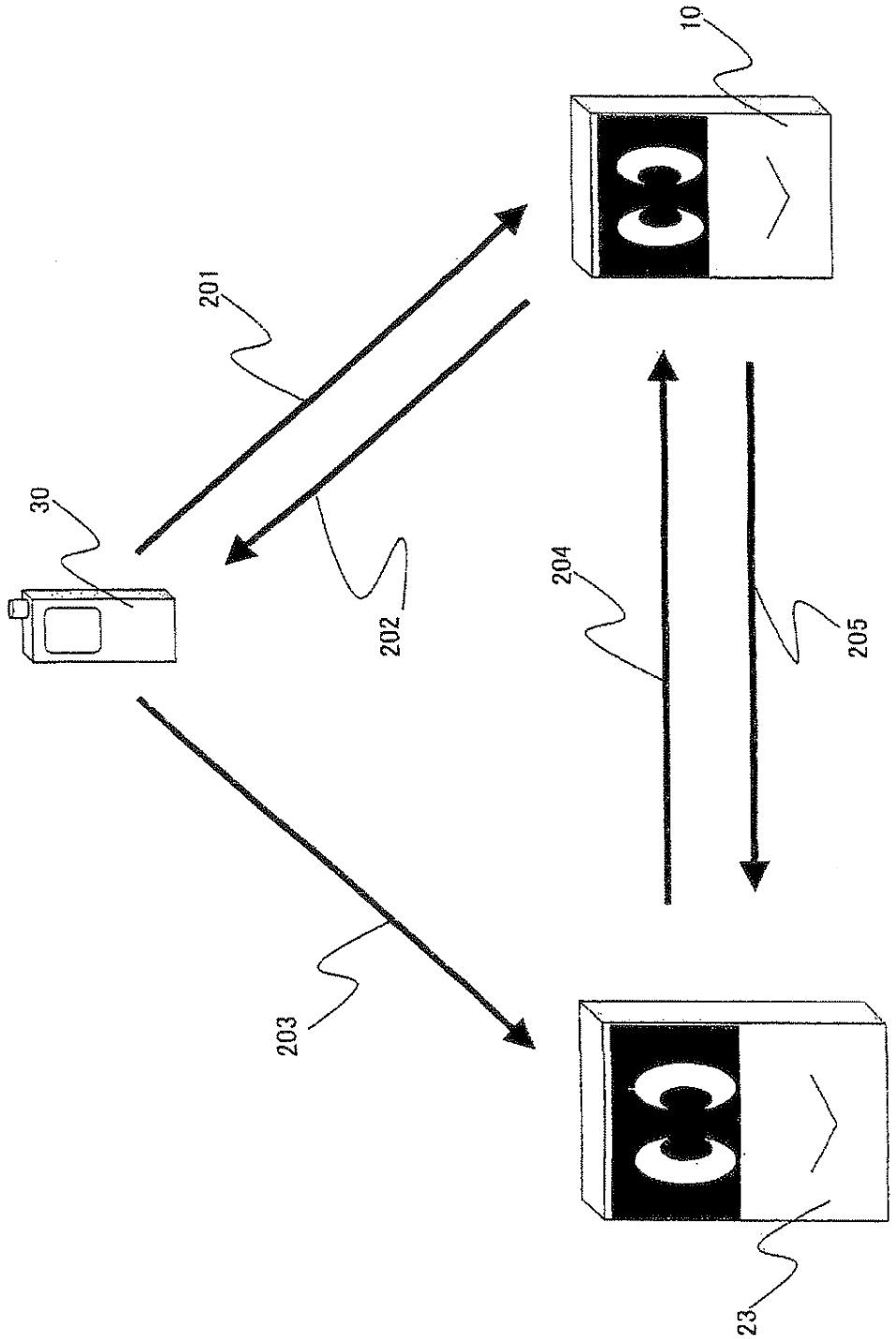



Fig.2

Fig.3

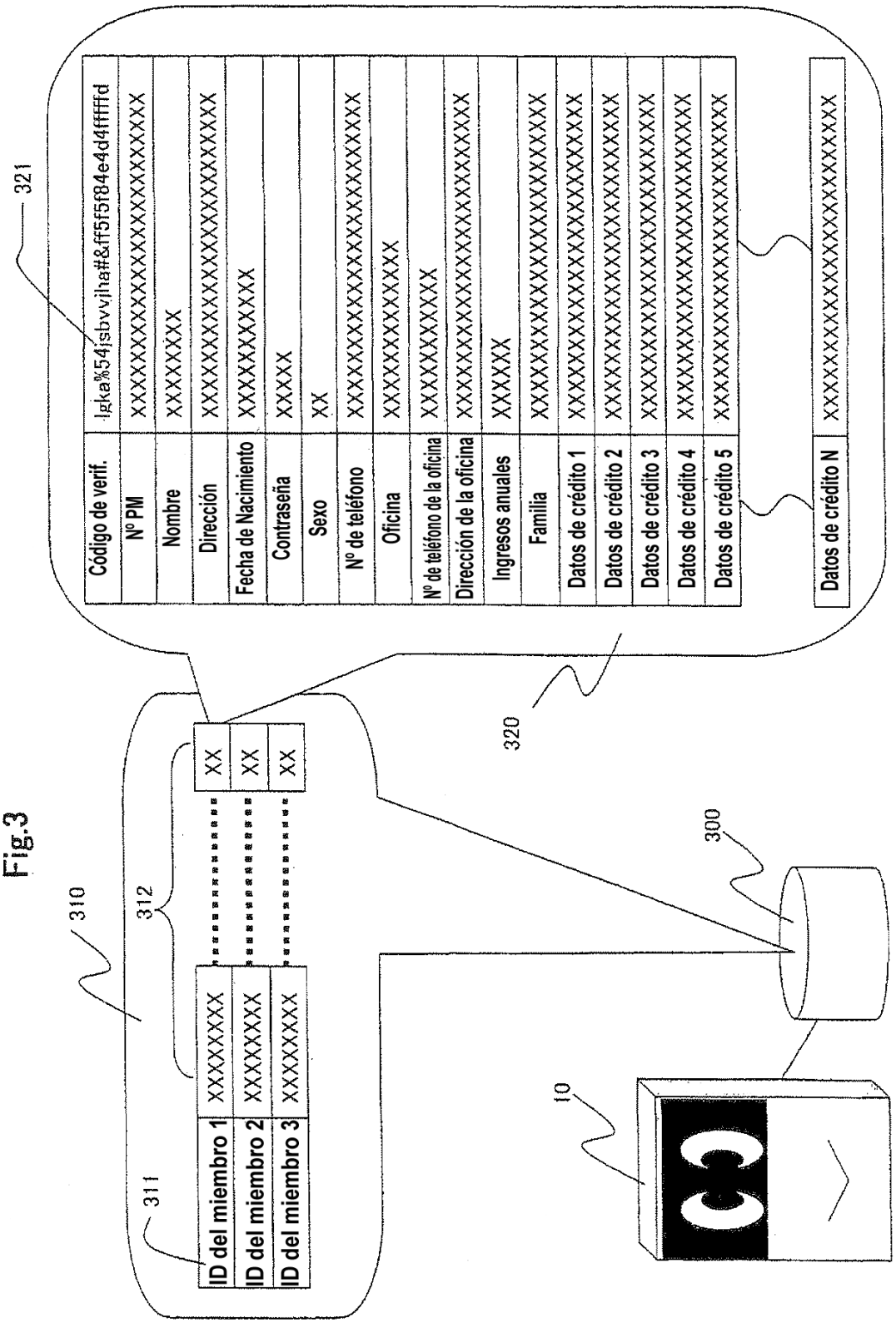

321
Código de verif.
lgka%54jsbvvjlha#&ff5f5f84e4d4ffffd
Nº PM
XXXXXXXXXXXXXXXXXXXXXXXX
Nombre
XXXXXXXX
Dirección
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Fecha de Nacimiento
XXXXXXXXXXX
Contraseña
XXXXX
Sexo
XX
Nº de teléfono
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Oficina
XXXXXXXXXXXXXX
Nº de teléfono de la oficina
XXXXXXXXXX
Dirección de la oficina
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Ingresos anuales
XXXXXX
Familia
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 1
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 2
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 3
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 4
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito 5
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Datos de crédito N
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
320
300
10
310
312
311
ID del miembro 1
XXXXXXXX
XX
ID del miembro 2
XXXXXXXX
XX
ID del miembro 3
XXXXXXXX
XX

Fig.4

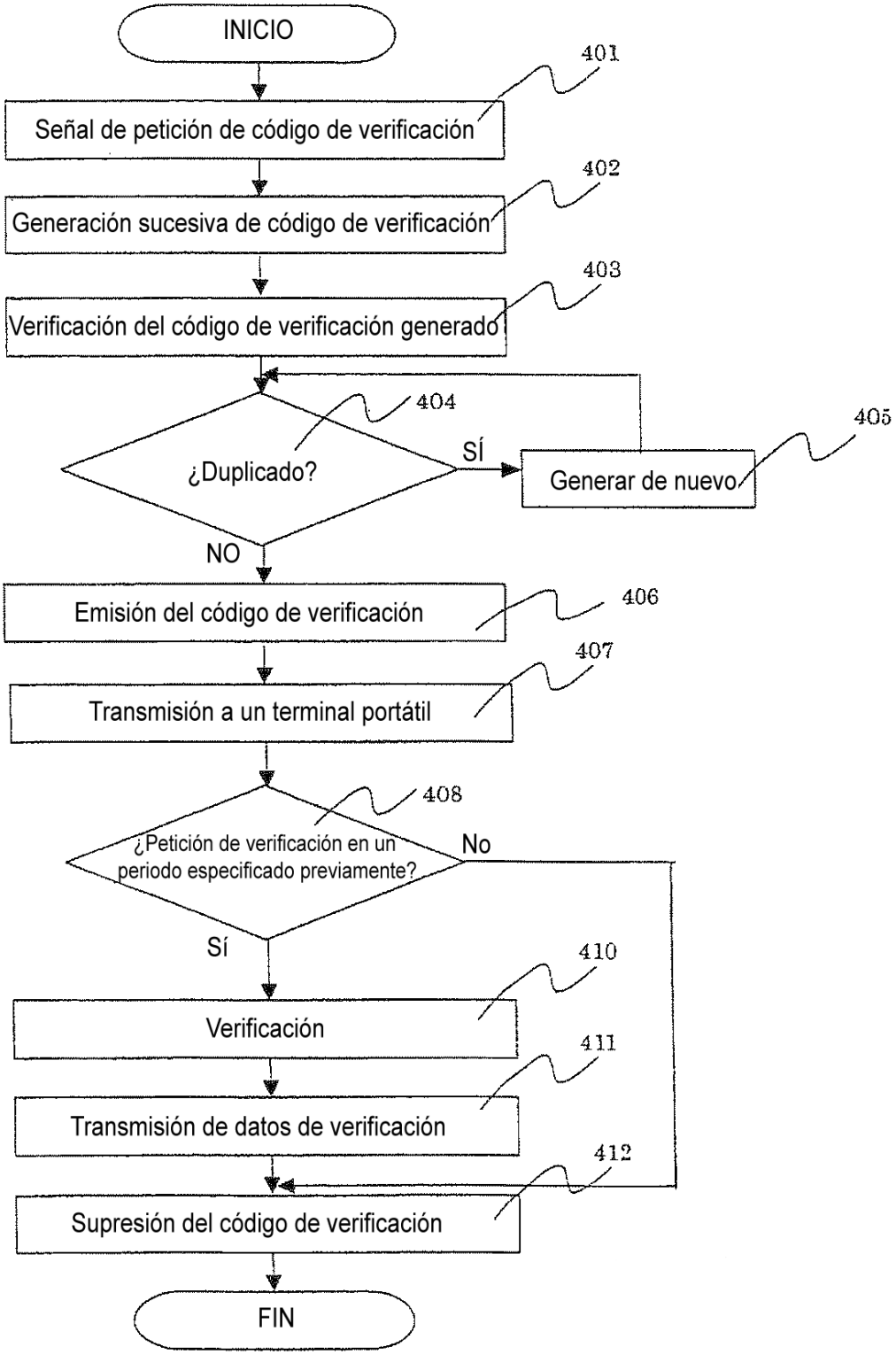
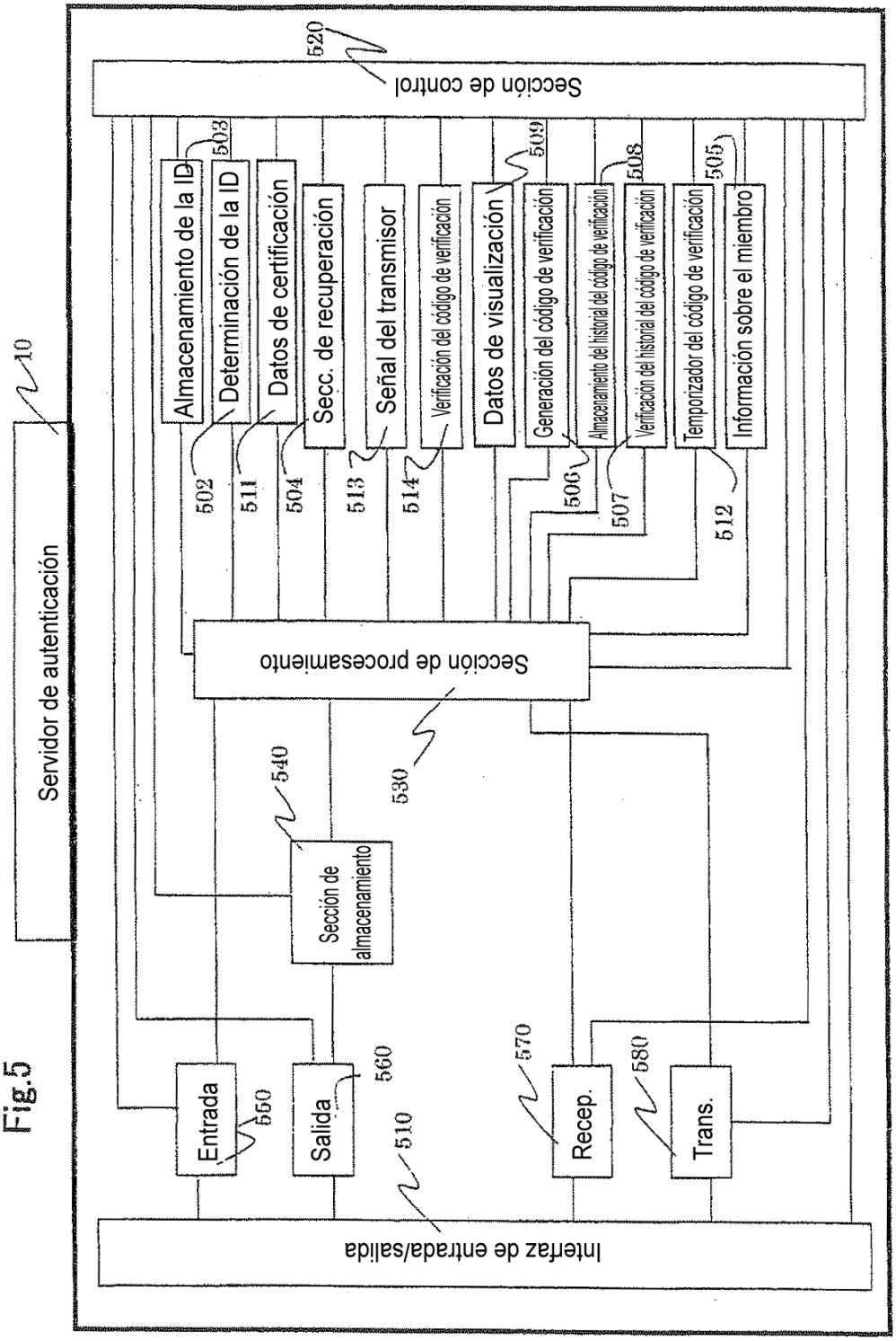

INICIO
401
Señal de petición de código de verificación
402
Generación sucesiva de código de verificación
403
Verificación del código de verificación generado
404
¿Duplicado?
SÍ
405
Generar de nuevo
NO
Emisión del código de verificación
406
407
Transmisión a un terminal portátil
408
¿Petición de verificación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

Fig.5


Servidor de autenticación
10
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
Sección de control
Sección de procesamiento
Sección de almacenamiento
Entrada
Salida
Recep.
Trans.
Interfaz de entrada/salida
502
503
504
505
506
507
508
509
510
511
512
513
514
520
530
540
550
560
570
580

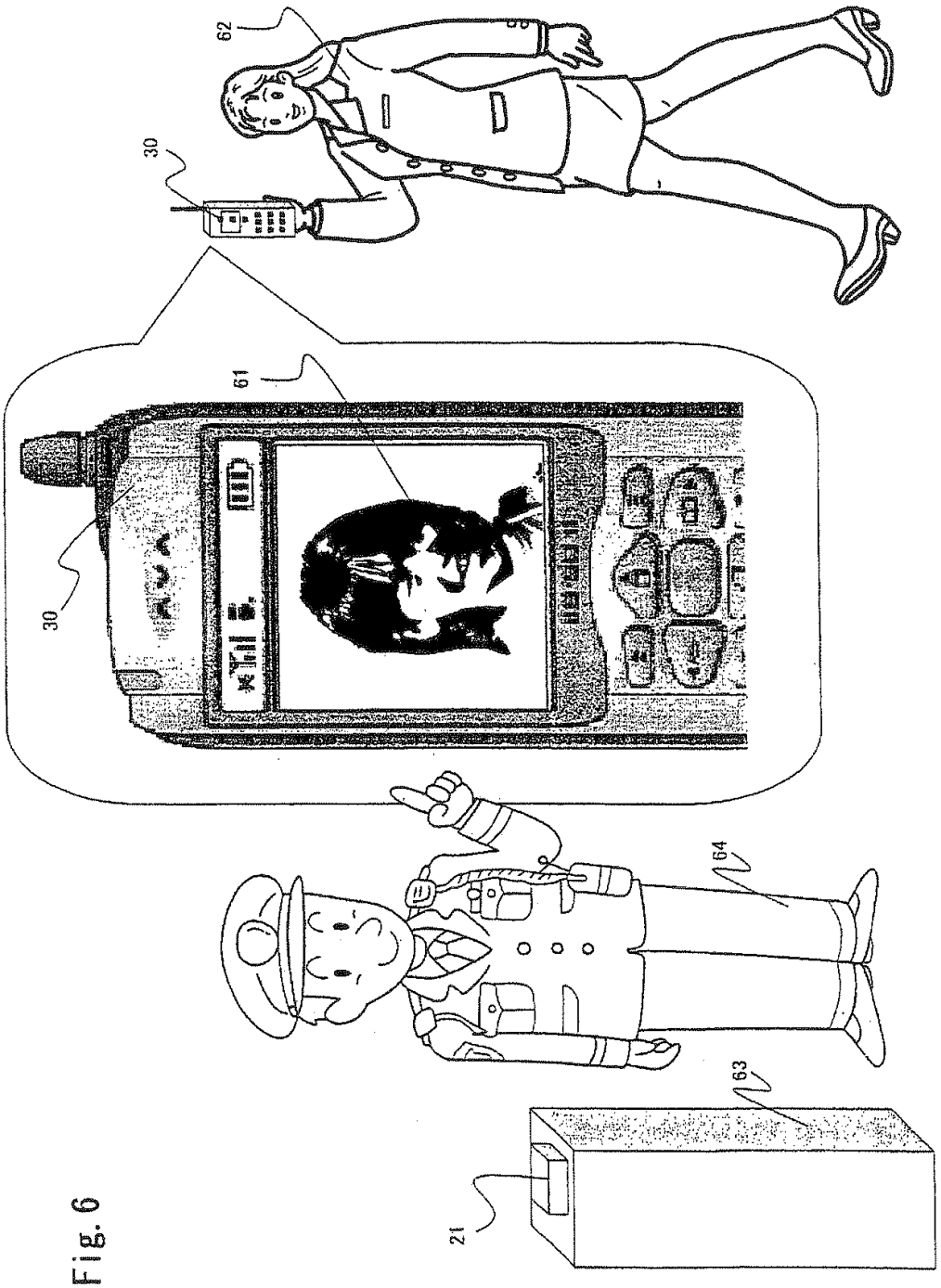



Fig. 6

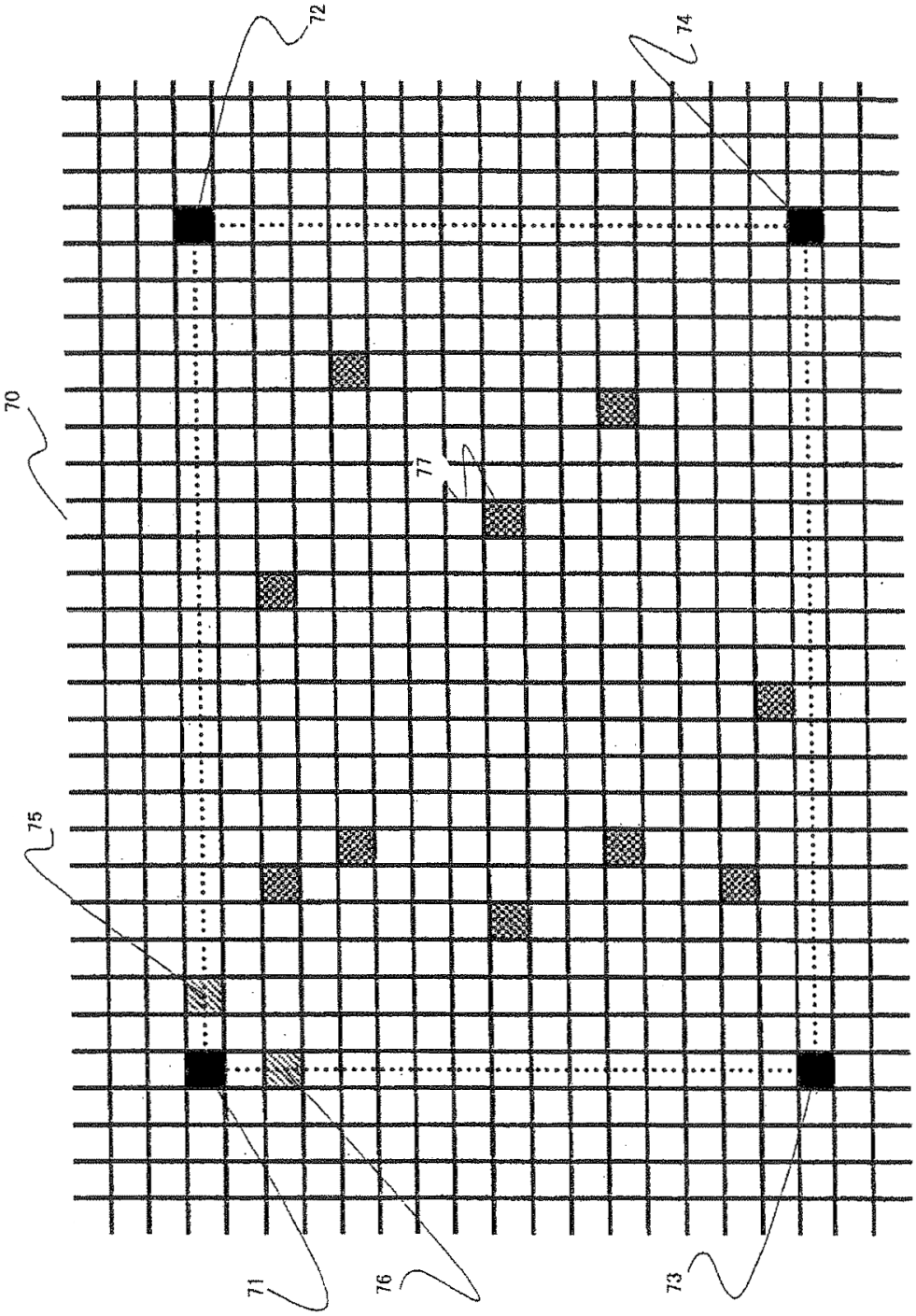
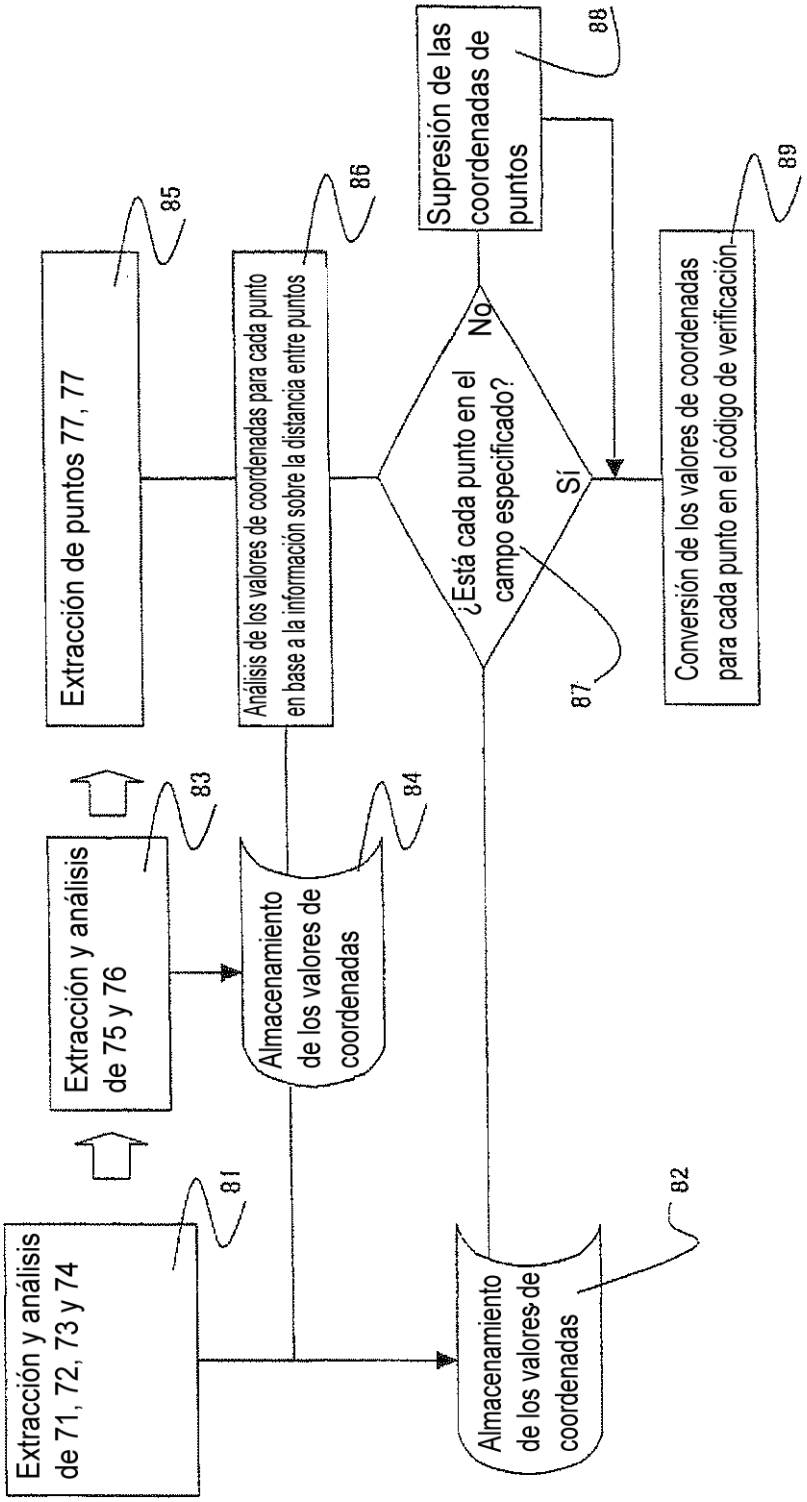



Fig. 7

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
¿Está cada punto en el campo especificado?
87
No
Sí
Supresión de las coordenadas de puntos
88
Almacenamiento de los valores de coordenadas
82
Conversión de los valores de coordenadas para cada punto en el código de verificación
89

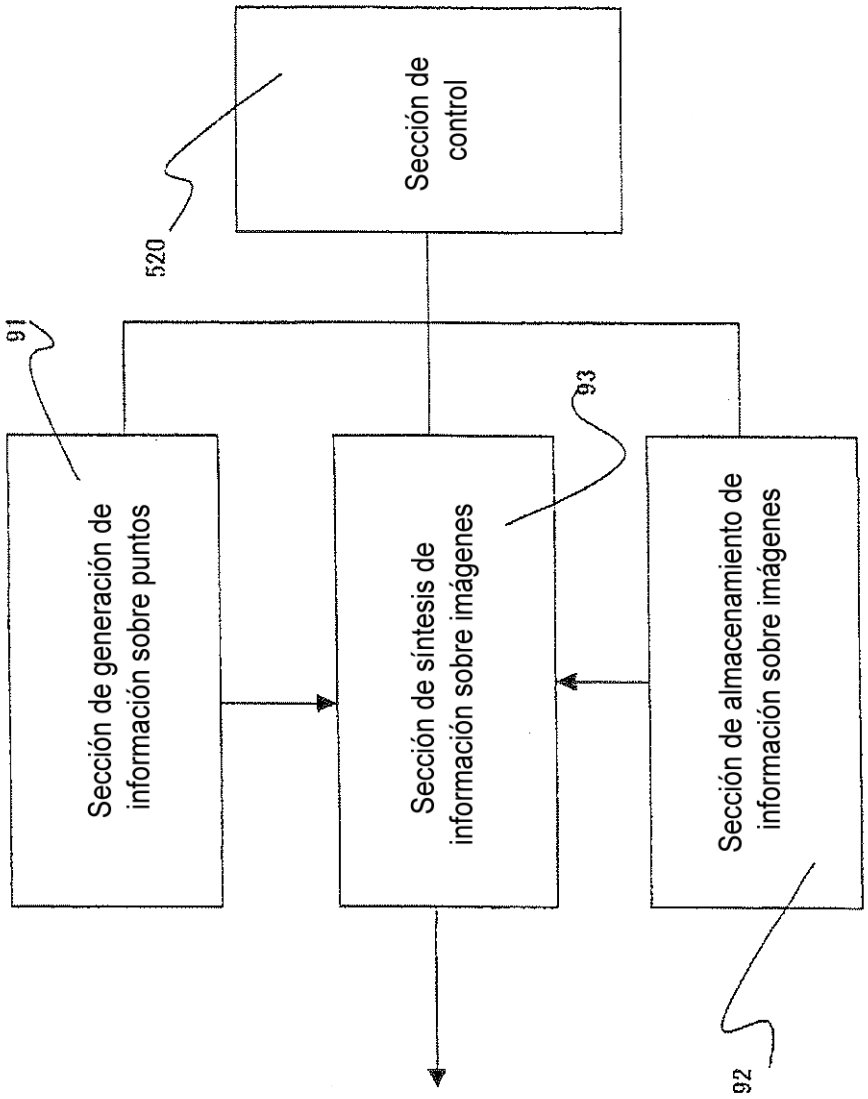
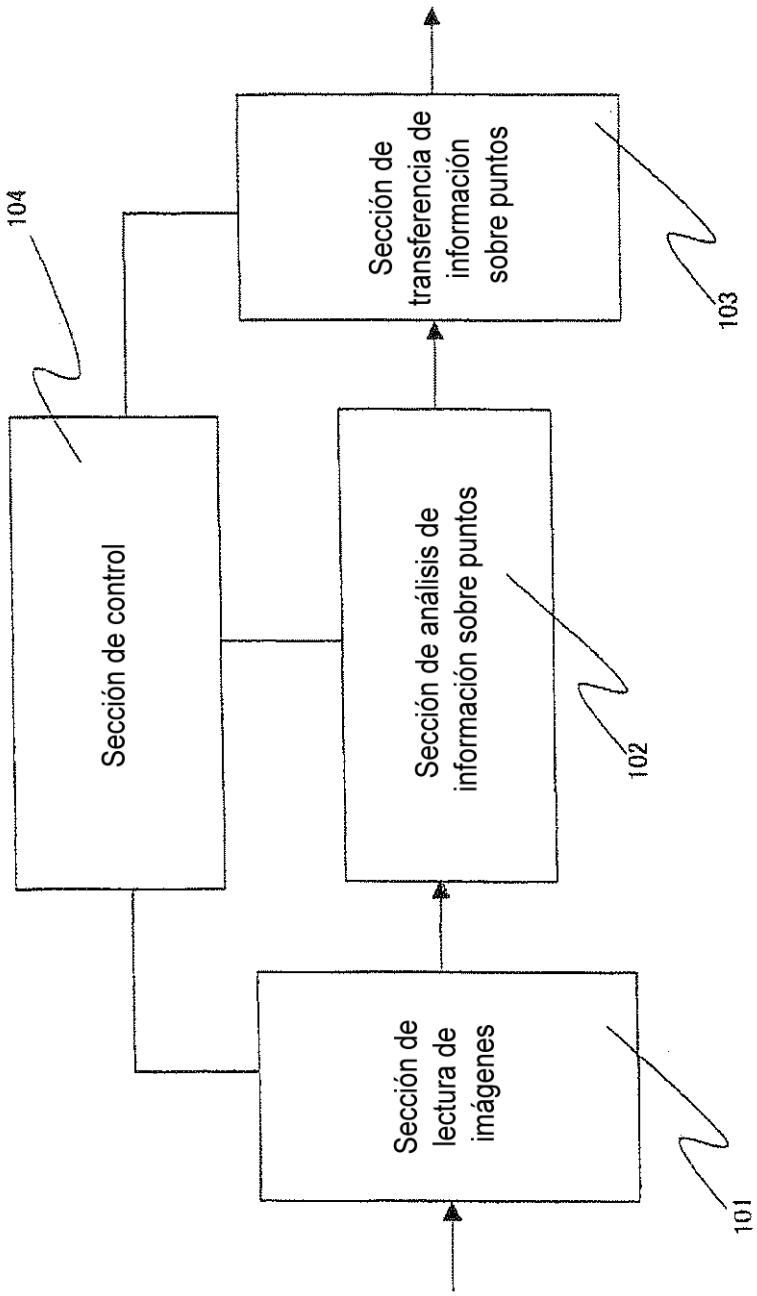

Sección de generación de información sobre puntos
91
Sección de síntesis de información sobre imágenes
93
Sección de almacenamiento de información sobre imágenes
92
Sección de control
520

Fig. 9

Fig. 10


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