



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 334 157**

51 Int. Cl.:
G06K 9/32 (2006.01)
G06K 9/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **06252422 .8**
96 Fecha de presentación : **08.05.2006**
97 Número de publicación de la solicitud: **1780657**
97 Fecha de publicación de la solicitud: **02.05.2007**

54 Título: **Sistema biométrico y método biométrico.**

30 Prioridad: **27.10.2005 JP 2005-313092**

45 Fecha de publicación de la mención BOPI:
05.03.2010

45 Fecha de la publicación del folleto de la patente:
05.03.2010

73 Titular/es: **Fujitsu Ltd.**
1-1, Kamikodanaka 4-chome
Nakahara-ku, Kawasaki-shi
Kanagawa 211-8588, JP
Fujitsu Frontech Limited

72 Inventor/es: **Kamata, Hideo y**
Tanaka, Hiroyuki

74 Agente: **Ungría López, Javier**

ES 2 334 157 T3

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

DESCRIPCIÓN

Sistema biométrico y método biométrico.

5 Esta solicitud se basa y reivindica el beneficio de prioridad de la solicitud de patente japonesa anterior número 2005-313092, presentada el 27 de octubre de 2005.

10 La presente invención se refiere a un sistema biométrico y método biométrico utilizando características de una porción del cuerpo humano para realizar autenticación individual, y en particular se refiere a un sistema biométrico y método biométrico que guía una parte del cuerpo a un estado de registro al detectar información biométrica para uso en verificación contra información biométrica registrada.

15 Hay numerosas porciones del cuerpo humano, tal como las huellas dactilares y las huellas de las puntas de los pies, las retinas de los ojos, características faciales, y vasos sanguíneos, que pueden ser usadas para distinguir individuos. Los avances en tecnología biométrica en los últimos años han ido acompañados de la aparición de varios dispositivos para reconocer las características de tales porciones del cuerpo humano y realizar la autenticación individual.

20 Se han facilitado métodos de autenticación individual a través de biometría que utilizan las características faciales, el iris del ojo, los vasos sanguíneos de la palma y dedos, las huellas dactilares y las marcas de la palma de la mano, y análogos. Estos métodos se han usado en varios campos como métodos de autenticación individual proporcionando un nivel alto de seguridad.

25 Por ejemplo, se obtienen cantidades comparativamente grandes de información de características individuales de los vasos sanguíneos en la palma y el reverso de la mano, y las configuraciones de los vasos sanguíneos (venas) no cambian durante toda la vida desde la infancia y se considera que son completamente únicas, y por ello son adecuadas para la autenticación individual. Aquí se explican dichos métodos de autenticación individual. Al tiempo del registro o de la autenticación, el usuario pone su palma cerca de un dispositivo de captura de imagen. El dispositivo de captura de imagen emite infrarrojos cercanos, que son incidentes en la palma de la mano. El dispositivo de captura de imagen usa un sensor para capturar los infrarrojos cercanos que rebotan de la palma de la mano.

30 La hemoglobina de los corpúsculos rojos que fluyen en las venas ha perdido oxígeno. Esta hemoglobina (hemoglobina reducida) absorbe rayos infrarrojos cercanos. En consecuencia, cuando los rayos infrarrojos cercanos inciden en la palma de una mano, la reflexión se reduce solamente en las zonas en que hay venas, y la intensidad de los infrarrojos cercanos reflejados puede ser usada para identificar las posiciones de las venas.

35 Al tiempo del registro biométrico, el usuario utiliza primero un dispositivo de captura de imagen para registrar datos de la imagen de las venas de la palma de su propia mano en un servidor y en una tarjeta.

40 Entonces, con el fin de realizar autenticación individual, el usuario utiliza un dispositivo de captura de imagen para leer datos de la imagen de las venas para su propia palma. La imagen de venas registrada recuperada usando la ID del usuario es verificada contra la configuración de vena de la imagen de verificación de venas así leída para realizar autenticación individual (véase, por ejemplo, la Publicación de Patente japonesa número 2004-062826).

45 En dicha detección de información biométrica, la parte del cuerpo se puede mover libremente con respecto al dispositivo de captura de imagen, y en particular, la mano, la cara y los dedos se pueden mover libremente. Por otra parte, para la verificación precisa es necesario que la parte del cuerpo para detección se coloque dentro del rango de captura de imagen del dispositivo de captura de imagen. Como tal método, se han propuesto (véase, por ejemplo, WO 04/021884 (figura 3) y la Publicación de Patente japonesa número 2001-273948) un método para detectar, al tiempo de la autenticación, la posición y orientación de la mano en cada captura de imagen, y usando una visualización o salida de voz para notificar al usuario que la posición u orientación de la mano es inapropiada (véase por ejemplo WO 04/021884), y un método de presentar una forma de la mano u otra configuración estándar de la mano, y para guiar el usuario en el modo de captura de imagen.

55 También se han propuesto métodos que incluyen la forma de la mano en la verificación basada en imágenes de los vasos sanguíneos. Es decir, se han propuesto métodos en los que, al tiempo del registro, la forma de la mano también se registra con anterioridad, y al tiempo de la verificación se determina si la forma de la mano de la que se captura una imagen, es similar a la forma de la mano al tiempo del registro, y si el grado de semejanza es bajo, no se realiza verificación de la imagen de los vasos sanguíneos, pero si el grado de semejanza es alto, se realiza verificación de la imagen de los vasos sanguíneos (véase, por ejemplo, WO04/021884).

60 En la primera tecnología de la técnica anterior, se visualiza una forma estándar, y el usuario es guiado a un modo apropiado de captura de imagen; o se usa una imagen de detección de la parte del cuerpo en el análisis para determinar si la parte del cuerpo detectada está en el rango apropiado de captura de imagen, y se ofrecen indicaciones de guía. Sin embargo, cuando se lleva a cabo dicha guía, si las circunstancias de la detección de la parte del cuerpo al tiempo del registro difieren de las circunstancias de la captura de imagen de la parte del cuerpo al tiempo de la autenticación 65 a pesar de esta guía al rango de captura de imagen, no se pueden obtener resultados de verificación satisfactorios.

ES 2 334 157 T3

Los ejemplos en los que las circunstancias de captura de imagen de una parte del cuerpo son diferentes durante el registro y durante la autenticación incluyen, por ejemplo, en el caso de autenticación usando la palma de la mano, un grado de diferencia en la extensión de los dedos al tiempo del registro y al tiempo de la autenticación; y en el caso de autenticación usando características faciales, las diferentes orientaciones de la cara, o la presencia y ausencia de gafas, al tiempo del registro y al tiempo de la autenticación. Así, incluso cuando la posición y la orientación de la mano o la cara son similares, a menudo los resultados de la verificación no concuerdan.

En la última tecnología de la técnica anterior, la forma de una mano se usa conjuntamente con un algoritmo de autenticación, de modo que cuando hay fallo de autenticación, el usuario no entiende directamente la causa, y a menudo no es posible determinar cómo se deberá guiar la parte del cuerpo con respecto al dispositivo de captura de imagen. En concreto, las personas con poca experiencia con el dispositivo, y los ancianos y otras personas, tenderá a tener inconvenientes.

En general, el usuario no recuerda el estado de captura de imagen de la parte del cuerpo al tiempo del registro, y además el usuario tendrá una fuerte aversión a ponerse en un estado estrictamente definido (posición o similar) de la parte del cuerpo para captura de imagen al tiempo del registro. En consecuencia, desde el punto de vista del fabricante del dispositivo, dado que hay casos en que se producen eventos imprevistos y pueden surgir errores de verificación, se espera que en tales casos, el usuario, es decir el individuo en cuestión, pierda confianza en dicha autenticación biométrica. En particular cuando se usa en equipo automatizado (cajeros automáticos de transacciones en efectivo, máquinas vendedoras automáticas, en puertas de entrada a viviendas, y análogos), porque no hay allí personal dedicado, surgen problemas al determinar la causa del problema, dando origen a más pérdida de confianza en la autenticación biométrica.

US 5054090 describe un método y aparato para procesar en paralelo datos de huellas dactilares “en vivo” y “de referencia” prerregistrados a efectos de comparación. Un sensor de matriz toma imágenes de una porción seleccionada de una huella dactilar en vivo y unos medios vídeo producen datos de imagen en vivo digitales correspondientes. Los datos de referencia prerregistrados y los datos de imagen son explorados uno con relación a otro mediante memorias intermedias recirculantes primero en entrar primero en salir (FIFO) y medios de desplazamiento de fila y columna.

US 2005/047632 describe un dispositivo de identificación personal que incluye un dispositivo de toma de imágenes que toma una imagen de la configuración de las venas de los dedos, una fuente de luz que emite luz adaptada para ser transmitida a través del dedo, una unidad operativa de imagen compara la imagen, unas guías indican la posición de toma de la imagen del dedo, un detector detecta el contacto entre el dedo y las guías, otra fuente de luz que irradia luz reflejada del grosor del dedo, un interruptor que es pulsado por la punta del dedo, otra fuente de luz que emite luz transmitida a través de la punta del dedo, y un sensor de luz que recibe la luz de la otra fuente de luz a través del dedo.

US 2005/148876 describe un dispositivo de identificación individual que incluye un dispositivo de formación de imágenes para formación de imágenes de vasos sanguíneos de una mano del usuario sin contacto incluyendo una unidad de instrucción de posición/dirección/forma para indicar al usuario que coloque su mano, una o más unidades radiantes para irradiar la mano con radiación infrarroja cercana, y una o varias unidades de formación de imágenes para producir una imagen por radiación infrarroja cercana; una unidad de extracción de imagen de vasos sanguíneos para extraer la imagen de los vasos sanguíneos de la imagen producida; una unidad de almacenamiento de imagen de los vasos sanguíneos para almacenar la imagen de los vasos sanguíneos de la mano de cada usuario; y una unidad de identificación para identificar el usuario comparando la imagen extraída de los vasos sanguíneos con la imagen registrada de los vasos sanguíneos.

EP 1385116 describe un sistema en que el usuario introduce una tarjeta de chip en un lector, para comprobar si el usuario está registrado en una base de datos. La base de datos contiene un registro de datos de referencia acerca de la estructura de los vasos sanguíneos y la dirección de flujo de sangre en el pulgar del usuario. Si el usuario está en la base de datos, entonces el usuario ofrece el pulgar para verificar los datos biométricos comparando la disposición espacial de los vasos sanguíneos y la dirección y la velocidad de sangre con los datos almacenados.

DE 4421237 describe un sistema de identificación que tiene un dispositivo detector para adquirir los datos de una configuración de los vasos sanguíneos de una sección predeterminada de una mano de una persona. Los datos de la configuración de los vasos sanguíneos son almacenados en un banco de datos durante una fase de registro y durante una fase de verificación posterior, se lleva a cabo una prueba para ver si los datos adquiridos de una configuración de los vasos sanguíneos corresponden a los datos almacenados en el banco de datos.

Consiguientemente, es deseable proporcionar un sistema biométrico y método biométrico para guiar efectivamente una parte del cuerpo al tiempo de la autenticación de manera que coincida con las circunstancias de la captura de imagen de la parte del cuerpo al tiempo del registro, con el fin de mejorar la eficiencia de la verificación.

También es deseable guiar una parte del cuerpo a las circunstancias de captura de imagen de la parte del cuerpo al tiempo del registro sin imponer una carga al usuario, y acortar el tiempo requerido para la verificación.

También es deseable, en caso de error de verificación, guiar la parte del cuerpo a las circunstancias de la captura de imagen de la parte del cuerpo al tiempo de registro sin confundir al usuario, con el fin de hacer conveniente el uso de autenticación biométrica para el usuario.

Según un primer aspecto, un sistema biométrico de esta invención, que verifica datos característicos de una parte del cuerpo registrados en una unidad de almacenamiento contra datos característicos de la parte del cuerpo obtenidos a través de captura de imagen para realizar autenticación individual, incluye: un dispositivo de captura de imagen que captura imágenes de la parte del cuerpo, por ejemplo, en modo sin contacto; un dispositivo de control que extrae datos característicos de la parte del cuerpo a partir de la imagen capturada de la parte del cuerpo, y verifica los datos característicos extraídos contra los datos característicos registrados para realizar autenticación individual; un dispositivo de visualización, que, al tiempo de la autenticación individual, indica una forma de la parte del cuerpo obtenida a partir de una captura de imagen al tiempo del registro de los datos característicos de parte del cuerpo almacenados en la unidad de almacenamiento, por ejemplo, presentando un contorno de la parte del cuerpo; y una unidad de entrada para introducir un número de identificación, con el fin de recuperar, de la unidad de almacenamiento, datos de la forma de la parte del cuerpo del usuario cuya autenticación individual se ha de realizar, donde la unidad de almacenamiento guarda, al tiempo del registro de los datos característicos de parte del cuerpo, datos de la forma de la parte del cuerpo obtenidos en la captura de imagen de la parte del cuerpo y datos característicos de la parte del cuerpo, el dispositivo de control lee, al tiempo de la autenticación biométrica, los datos de la forma de la parte del cuerpo y los datos característicos de la parte del cuerpo de la unidad de almacenamiento, y el dispositivo de control visualiza, en el dispositivo de visualización, la forma de la parte del cuerpo al tiempo de la verificación, obtenida en la captura de imagen por el dispositivo de captura de imagen, conjuntamente con la forma de la parte del cuerpo al tiempo del registro, caracterizado porque el dispositivo de captura de imagen incluye una unidad de captura de imagen que captura imágenes de al menos una porción de una mano del usuario, y el dispositivo de control extrae datos de imagen de vasos sanguíneos de la porción de la mano a partir de la imagen capturada y visualiza, en el dispositivo de visualización, una forma de la mano del mismo usuario al tiempo de la verificación, obtenida en la captura de imagen por el dispositivo de captura de imagen, junto a y paralela con la forma de la mano al tiempo del registro.

Además, un método biométrico de esta invención para verificar datos característicos de parte del cuerpo registrados en una unidad de almacenamiento contra datos característicos de parte del cuerpo obtenidos por la captura de imagen para realizar autenticación individual, incluye: un paso de captura de imagen que consiste en capturar una imagen, por ejemplo en modo sin contacto, de la parte del cuerpo por un dispositivo de captura de imagen; un paso de extraer datos característicos de la parte del cuerpo a partir de la imagen capturada de la parte del cuerpo; un paso de almacenar en la unidad de almacenamiento, al tiempo del registro de los datos característicos de parte del cuerpo, datos de forma de la parte del cuerpo y datos característicos de la parte del cuerpo obtenidos en la captura de imagen de la parte del cuerpo; un paso de entrada consistente en introducir un número de identificación, con el fin de recuperar, de la unidad de almacenamiento, datos de forma de la parte del cuerpo del usuario para quien se ha de llevar a cabo la autenticación individual; un paso de lectura, al tiempo de la autenticación biométrica, de los datos de forma de la parte del cuerpo y los datos característicos de la parte del cuerpo de la unidad de almacenamiento; un paso de autenticación consistente en verificar los datos característicos extraídos de la parte del cuerpo contra los datos característicos registrados; y un paso de visualización, al tiempo de la autenticación individual, de presentar en un dispositivo de visualización una forma de la parte del cuerpo obtenida a través de captura de imagen por el dispositivo de captura de imagen al tiempo de la verificación, conjuntamente con la forma de la parte del cuerpo al tiempo del registro, caracterizado porque el paso de captura de imagen incluye un paso de captura de imagen que consiste en capturar una imagen de al menos una porción de la mano del usuario, el paso de autenticación incluye un paso de extraer datos de imagen de vasos sanguíneos de la mano de la imagen capturada, y el paso de visualización incluye un paso de presentar en el dispositivo de visualización una forma de la mano del mismo usuario al tiempo de la verificación, obtenida a través de la captura de imagen por el dispositivo de captura de imagen, junto a y paralela con la forma de la mano al tiempo del registro.

En esta invención, es preferible que el sistema biométrico tenga además un dispositivo de registro de datos biométricos, que captura una imagen de la parte del cuerpo, extrae datos de la forma de la parte del cuerpo y datos característicos de la parte del cuerpo de la imagen capturada, y guarda los datos en la unidad de almacenamiento.

En esta invención, es preferible que la unidad de entrada sea una unidad portátil propiedad del usuario.

En esta invención, es preferible que la unidad de almacenamiento esté dispuesta en un dispositivo de nivel superior conectado al dispositivo de control.

En esta invención, es preferible que la unidad de almacenamiento esté dispuesta en una unidad portátil propiedad del usuario.

En esta invención, es preferible que la unidad de almacenamiento tenga un dispositivo de nivel superior que esté conectado al dispositivo de control y guarde datos de la forma de la parte del cuerpo, y una unidad portátil propiedad del usuario y guarda datos característicos de la parte del cuerpo.

En esta invención, es preferible que el sistema biométrico tenga una unidad de comunicaciones por medio de la que, al tiempo de la autenticación individual, el usuario llame a un centro de llamadas, y un dispositivo terminal que lea la forma de la parte del cuerpo del usuario en la unidad de almacenamiento, visualice la forma de parte del cuerpo en la pantalla del centro de llamadas, y proporcione indicaciones de guía al usuario.

En esta invención, es preferible que la unidad portátil verifique los datos característicos de parte del cuerpo, extraídos por la unidad portátil de la imagen capturada de la parte del cuerpo, contra datos característicos registrados en la unidad de almacenamiento, y que realice autenticación individual.

ES 2 334 157 T3

En esta invención, la imagen capturada para autenticación es registrada antes del tiempo del registro biométrico, y al tiempo de la autenticación biométrica la imagen capturada es visualizada y proporcionada al usuario para uso en la captura de imagen; por lo tanto, se incrementa la conveniencia del usuario, con ventajas para la operación por parte del usuario no familiarizado con el sistema de autenticación y para mejorar la velocidad de autenticación.

5

Se hace referencia, a modo de ejemplo solamente, a los dibujos acompañantes en los que:

La figura 1 representa la configuración del sistema biométrico de una primera realización de la invención.

10

La figura 2 representa la configuración del terminal de zona de servicio de la figura 1.

La figura 3 es una vista oblicua del CA de la figura 1.

15

La figura 4 es un diagrama de bloques del CA de la figura 3.

La figura 5 es un diagrama de bloques funcionales del procesado de registro de información biométrica de la figura 2.

20

La figura 6 es un diagrama de bloques funcionales del procesado de autenticación de información biométrica de la figura 4.

La figura 7 explica la forma registrada de parte del cuerpo de la figura 5.

25

La figura 8 explica la imagen de vasos sanguíneos de la figura 5.

La figura 9 representa el flujo de procesado de registro de información biométrica en una realización de la invención.

30

La figura 10 representa el flujo de procesado de autenticación biométrica en una realización de la invención.

La figura 11 representa el flujo de procesado de autenticación biométrica en otra realización de la invención.

La figura 12 explica un ejemplo de visualización de la forma de parte del cuerpo de la figura 11.

35

La figura 13 representa la configuración del sistema biométrico de una segunda realización de la invención.

La figura 14 representa la configuración del sistema biométrico de una tercera realización de la invención.

40

Y la figura 15 representa la configuración del sistema biométrico de una cuarta realización de la invención.

A continuación se explican realizaciones de la invención siguiendo el orden de una primera realización de un sistema biométrico, configuración del procesado de autenticación biométrica, procesado del registro biométrico, procesado de autenticación biométrica, otro procesado de autenticación biométrica, segunda realización de un sistema biométrico, tercera realización de un sistema biométrico, cuarta realización de un sistema biométrico, y otras realizaciones.

45

Primera realización de un sistema biométrico

50

La figura 1 representa la configuración de una primera realización de un sistema biométrico de esta invención, la figura 2 representa la configuración del dispositivo de zona de servicio de la figura 1, la figura 3 es una vista exterior de la máquina de transacciones automáticas de la figura 1, y la figura 4 representa la configuración de la máquina de transacciones automáticas de la figura 3.

55

La figura 1 representa un sistema de autenticación de venas de la palma en una institución financiera, como un ejemplo de un sistema biométrico. Un terminal de sucursal 2 está dispuesto en una zona de servicio de la institución financiera. Como se explica en la figura 2, el terminal de sucursal 2 está provisto de un dispositivo de captura de imagen de la palma 1, un ordenador de terminal de sucursal (por ejemplo, un ordenador personal) 2-1 conectado al dispositivo de captura de imagen 1, un teclado 2-2, una pantalla 2-3, y un dispositivo de lectura/escritura de tarjetas CI 2-4. El dispositivo de captura de imagen de la palma 1 puede estar configurado integralmente con el dispositivo de lectura/escritura de tarjetas CI 2-4.

60

Como se ha indicado en la figura 2, el dispositivo de captura de imagen de la palma 1 tiene una unidad sensora 18, guía delantera 14 para soportar la muñeca del usuario, y una guía trasera 13 para guiar los dedos del usuario. El usuario, que ha pedido autenticación de venas, pone la mano sobre este dispositivo de captura de imagen de la palma 1. El dispositivo de captura de imagen de la palma (a continuación "dispositivo de captura de imagen") 1 lee la imagen de la palma, y envía la imagen al ordenador 2-1.

65

ES 2 334 157 T3

El dispositivo de lectura/escritura de tarjetas CI 2-4 lee y escribe datos de y a una tarjeta CI 5 que tiene el usuario. La tarjeta CI 5 es una tarjeta conocida del tamaño de una tarjeta de crédito, que incorpora un chip CI con memoria y una CPU, y que tiene terminales externos.

5 El dispositivo de captura de imagen 1, el dispositivo de lectura/escritura de tarjetas CI 2-4, el teclado 2-2, y la pantalla 2-3 están conectados al ordenador 2-1, y realizan la extracción de imagen de vasos sanguíneos, registro de forma y otro procesado, descritos más adelante.

10 El terminal 2 está conectado a un servidor 4 mediante una LAN (red de área local) 80. El servidor 4 tiene un archivo temporal 4-1, y está conectado al host 7. El servidor 4 también está conectado a una pluralidad de máquinas de transacciones automáticas (CAs) 6 mediante una segunda LAN 82.

15 Dicho CA 6 puede ser usado para realizar transacciones en base a la autenticación de venas. Con el fin de usar un CA 6 para realizar transacciones de extracción y otras transacciones financieras, el usuario pone su mano sobre el dispositivo de captura de imagen 1-1 dispuesto en el CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma. El CA 6 tiene un dispositivo de lectura/escritura de tarjetas CI 60, que lee y escribe datos en una tarjeta CI 5 que tiene el usuario.

20 La figura 3 y la figura 4 muestran la configuración del CA 6 de la figura 1. Como se representa en la figura 3, el CA 6 tiene, en su cara delantera, una ranura de introducción/expulsión de tarjetas 6-4; una ranura de introducción/expulsión de libreta 6-5; una ranura de introducción/dispensación de billetes 6-3; una ranura de introducción/dispensación de monedas 6-2; y un panel de operación del cliente (POU) 6-1 para operación y visualización.

25 En este ejemplo, el dispositivo de captura de imagen 1-1 está dispuesto en el lado del panel de operación del cliente 6-1. La unidad sensora 18 explicada en la figura 4 y la figura 6 está montada en el lado delantero de la unidad principal 10 del dispositivo de captura de imagen 1-1. Además, la unidad sensora 18 de la unidad principal 10 mira hacia atrás y está inclinada hacia arriba, y se ha dispuesto una porción plana 22 detrás.

30 Este dispositivo de captura de imagen 1-1 difiere del dispositivo de captura de imagen 1 de la figura 2 en que no se han previsto las guías de palma 14, 13. Esto es porque, en el registro, es suficiente una sola operación, pero en el caso de una transacción basada en autenticación, se realizan docenas de operaciones; por lo tanto, con el fin de aliviar la aversión del usuario, no se han dispuesto guías 14, 13 en el dispositivo de captura de imagen 1-1 del CA 6. Otra razón es que la existencia de guías 14, 13 plantea problemas para operación por parte del usuario. Naturalmente se pueden disponer las guías 14, 13.

35 Como se representa en la figura 4, el CA 6 tiene una unidad CIP (impresora de lector de tarjetas) 60 con una ranura de introducción/expulsión de tarjetas 6-4; una unidad de libreta de banco 64 que tiene una ranura de introducción/expulsión de libreta 6-5; una unidad de recuento de billetes/monedas 66 que tiene una ranura de introducción/dispensación de billetes 6-3 y una ranura de introducción/dispensación de monedas 6-2; una unidad de operación de encargado 65; una unidad de control 67; un panel de operación del cliente (POU) 6-1 para operación y visualización; y un dispositivo de captura de imagen (sensor de venas) 1-1.

40 La unidad CIP 60 tiene un dispositivo de lectura/escritura de tarjetas CI 61 que lee y escribe la banda magnética y el chip CI de una tarjeta CI 5; una impresora de resguardos 63 que registra transacciones en un resguardo; y una impresora de diario 62 que imprime la historia de transacciones en forma de diario.

45 La unidad de libreta de banco 64 registra transacciones en las páginas de una libreta de banco, y cuando es necesario pasa las páginas. La unidad de operación de encargado 65 es para operaciones realizadas por un encargado, que puede ver el estado y realizar operaciones a la aparición de un fallo o durante las inspecciones. La unidad de recuento de billetes/monedas 66 valida, cuenta, y guarda billetes y monedas introducidos, y cuenta y dispensa billetes y monedas en las cantidades requeridas.

50 La unidad de control 67 comunica con el servidor 4, y tiene una aplicación CA 68 que controla la operación CA y una librería de autenticación 69 para procesado de autenticación. Una porción de esta aplicación de CA 68 actúa en concierto con la librería de autenticación 69 para controlar las pantallas de guía de autenticación biométrica del POU 6-1

55 En el sistema de la figura 1, un archivo de imágenes de vasos sanguíneos (venas) 7-1 y la base de datos de cliente 7-2 están dispuestos en el host 7. El archivo de imágenes de vasos sanguíneos 7-1 guarda datos de venas 70 y datos de forma de la palma 72 de los usuarios que han completado el registro de autenticación de venas.

60 Se explica el proceso de registro de este sistema. El usuario, que ha pedido autenticación de venas, pone la mano sobre el dispositivo de captura de imagen de la palma 1 del terminal de zona de servicio 2. El dispositivo de captura de imagen 1 lee la imagen de la palma y envía la imagen al ordenador 2-1. El ordenador 2-1 extrae la imagen de vasos sanguíneos para la palma, crea datos de imagen de vasos sanguíneos 70, también crea datos de forma exterior de la mano 72, y transfiere al servidor 4 el número de identificación (por ejemplo, número de cuenta) leído de la tarjeta CI 5 así como los datos de imagen de vasos sanguíneos 70 y datos de forma externa 72. El servidor 4 convierte los datos transferidos a un formato preestablecido, y transfiere el resultado al host 7. El host 7 guarda, en el archivo de imágenes

ES 2 334 157 T3

de vasos sanguíneos 7-1, el número de identificación transferido (por ejemplo, el número de cuenta), datos de imagen de vasos sanguíneos 70, y datos de forma externa 72.

5 A continuación, en una transacción basada en autenticación biométrica, el usuario introduce la tarjeta CI 5 en el dispositivo de lectura/escritura de tarjetas CI 60 del CA 6, y hace que se lean los datos. Estos datos son transmitidos al host 7 mediante la LAN 82 y el servidor 4. El host 7 busca el archivo de imágenes de vasos sanguíneos 7-1, lee los datos de imagen de vasos sanguíneos 70 y datos de forma externa 72 correspondientes al número de identificación transmitido del archivo 7-1, y transmite estos datos al CA 6 mediante el servidor 4 y la LAN 82. En el CA 6, estos datos de forma son visualizados en el POU 6-1, que reproduce el estado de captura de imagen para el usuario al tiempo del registro.
10

Mediante esto, el usuario puede identificar el estado de captura de imagen al tiempo del registro. Consiguientemente, el usuario pone la mano de manera similar sobre el dispositivo de captura de imagen 1-1 del CA 6. El dispositivo de captura de imagen 1-1 lee la imagen de la palma de la mano, y transmite la imagen a la unidad de control 67 del CA 6. La unidad de control 67 extrae la imagen de vasos sanguíneos de la palma, crea datos de imagen de vasos sanguíneos 70, verifica los datos contra los datos de imagen de vasos sanguíneos transmitidos desde el host 7, y realiza la autenticación individual. Si la persona queda confirmada satisfactoriamente, el CA 6 permite entonces una transacción automatizada ordinaria.
15

20 *Configuración del procesado de autenticación biométrica*

La figura 5 es un diagrama de bloques de procesado de autenticación biométrica en el terminal de zona de servicio en la figura 1 y la figura 2, la figura 6 es un diagrama de bloques de procesado de autenticación biométrica por el CA 6 en la figura 1, la figura 3, y la figura 4, y la figura 7 y la figura 8 explican esta operación.
25

Como se representa en la figura 5, el dispositivo de captura de imagen de la palma 1 de la figura 1 tiene una unidad sensora 18 instalada sustancialmente en el centro de la unidad principal 10. En la porción delantera (en el lado del usuario) de la unidad sensora 18 se ha dispuesto una guía delantera 14; en el lado trasero se ha dispuesto una guía trasera 13. La guía delantera 14 incluye una hoja de resina sintética, transparente o sustancialmente transparente.
30

La guía delantera 14 cumple la finalidad de guiar la mano del usuario en la parte delantera y de soportar la muñeca; la guía trasera 13 soporta las puntas de los dedos. Por lo tanto, se ofrece guía y soporte al usuario, guiando la guía delantera 14 la muñeca encima de la unidad sensora 18. Como resultado, se puede controlar la postura de la palma de la mano, es decir, la posición, la inclinación y el tamaño sobre la unidad sensora 18. La forma en sección transversal de la guía delantera 14 tiene un cuerpo vertical y, en la porción superior, una porción horizontal 14-1 para soportar la muñeca. Se ha formado una depresión 14-2 de forma continua en el centro de la porción horizontal 14-1, para facilitar la colocación de la muñeca.
35

La unidad sensora 18 está provista de un sensor de captura de imagen bidimensional (sensor de infrarrojos) y lente de enfoque 16 y un sensor de distancia 15 en el centro; en su periferia se ha dispuesto una pluralidad de elementos emisores de luz infrarroja cercana (LEDs) 12. Por ejemplo, elementos emisores de luz infrarroja cercana están dispuestos en ocho lugares en la periferia, para emitir rayos infrarrojos cercanos hacia arriba.
40

La región legible V de esta unidad sensora 18 es regulada por la relación entre el sensor, lente de enfoque, y región de emisión de luz infrarroja cercana. Por lo tanto, la posición y altura de la guía delantera 14 se ponen de tal manera que la palma soportada se coloque en la región legible V.
45

Como se ha indicado en la figura 5, la librería de autenticación del ordenador 2-1 conectado al dispositivo de captura de imagen 1 ejecuta una serie de procesado de registro 30 a 36, 44 y 46.
50

El procesado de detección de distancia/contorno de la mano 30 recibe la distancia medida por el sensor de distancia 16 de los dispositivos de captura de imagen 1, determina si la palma de la mano u otro objeto está a una distancia en un rango preestablecido de la unidad sensora 18, y también detecta el contorno de la mano a partir de la imagen capturada por la unidad sensora 18 y determina a partir del contorno si la imagen puede ser usada en el registro y el procesado de verificación. Por ejemplo, la palma puede no aparecer suficientemente en la imagen.
55

El procesado de salida de mensajes de guía 32 envía, al POU 6-1 del CA 6, un mensaje para guiar la palma a la izquierda o a la derecha, hacia delante o hacia atrás, hacia arriba o hacia abajo, cuando la distancia medida por el sensor de distancia 16 indica que la mano está fuera del rango de captura de imagen, o cuando la imagen no puede ser usada en el registro y el procesado de verificación. Mediante esto, la palma de la mano del usuario es guiada a posición sobre el dispositivo de captura de imagen 1.
60

El procesado de extracción de imagen de vasos sanguíneos 34 extrae una imagen de venas de la imagen de la mano cuando el procesado de detección del contorno de la mano 30 determina que una imagen ha sido capturada con la mano mantenida correctamente. Es decir, se extraen datos de vasos sanguíneos (venas) 70 de la imagen de la palma, como en la figura 8, a través de diferencias de reflectividad. La figura 8 representa la imagen de venas de vasos sanguíneos como una imagen, pero los datos correspondientes son datos en escala de grises de esta imagen.
65

ES 2 334 157 T3

El procesado de registro/salida de la forma de la mano 36 guarda en la porción de almacenamiento (en la figura 1, el archivo de imágenes de vasos sanguíneos 7-1 en el host 7), conjuntamente con un número de cuenta, datos de forma externa 72 de la mano (véase la figura 7) cuando se captura una imagen con la mano mantenida correctamente en el procesado de detección del contorno de la mano 30. Estos datos de forma de la mano pueden ser un mapa de bits de una imagen capturada, como en la figura 7, o pueden ser datos de contorno de la mano, extraídos de una imagen capturada.

El proceso de registro/búsqueda de imagen registrada de vasos sanguíneos 46 guarda datos de imagen de vasos sanguíneos detectados en el procesado de detección de imagen de vasos sanguíneos 34, conjuntamente con el número de cuenta, en la porción de almacenamiento (en la figura 1, en el archivo de imágenes de vasos sanguíneos 7-1 del host 7). Con el fin de realizar verificación de ensayo al tiempo del registro, los conjuntos de datos registrados de imagen de vasos sanguíneos R1, R2, R3 correspondientes a la ID individual (número de cuenta) leídos de la tarjeta CI 5 indicada en la figura 1 y la figura 2 son recuperados de la porción de almacenamiento 7-1. En el procesado de verificación 44, los datos de imagen de vasos sanguíneos N1 detectados en procesado de detección de imagen de vasos sanguíneos 34 y los datos registrados de imagen de vasos sanguíneos N2 son comparados, se realiza el procesado de verificación, y se envía el resultado de la verificación.

Igualmente, en el procesado de registro/salida de la forma de la mano 36, los datos de forma externa registrados correspondientes a la ID individual (número de cuenta) leídos de la tarjeta CI 5 de la figura 1 y la figura 2 son recuperados de la porción de almacenamiento 7-1 y presentados en la pantalla 2-3.

A continuación, se usa la figura 6 para explicar el mecanismo de autenticación biométrica del CA 6. El dispositivo de captura de imagen 1-1 de la figura 1 y la figura 3 tiene una unidad sensora 18 instalada sustancialmente en el centro de la unidad principal 10. Como se ha explicado anteriormente, este dispositivo de captura de imagen 1-1 difiere del dispositivo de captura de imagen 1 de la figura 5 en que no se facilitan una guía delantera 14 y una guía trasera 13.

La unidad sensora 18 está provista de un sensor de captura de imagen bidimensional (sensor de infrarrojos) y lente de enfoque 16 y un sensor de distancia 15 en el centro; en su periferia se ha dispuesto una pluralidad de elementos emisores de luz infrarroja cercana (LEDs) 12. Por ejemplo, los elementos emisores de luz infrarroja cercana están dispuestos en ocho lugares en la periferia, para emitir rayos infrarrojos cercanos hacia arriba. La región legible V de esta unidad sensora 18 es regulada por la relación entre el sensor, la lente de enfoque, y la región de emisión de luz infrarroja cercana.

A continuación se explica la librería de autenticación 69 del CA 6. La librería de autenticación 69 de la unidad de control 67 del CA 6 conectada al dispositivo de captura de imagen 1-1 ejecuta la serie de procesado de verificación 30 a 34, 38, 44, 46. La unidad de control 67 del CA 6 tiene, por ejemplo, una CPU y varios tipos de memoria, un circuito de interface, y otra circuitería necesaria para el procesado de datos. Esta CPU ejecuta la serie de procesado de registro 30 a 34, 38, 44 y 46.

En la figura 6 a las porciones idénticas a las de la figura 5 se les han asignado los mismos símbolos. Es decir, en la figura 6, el procesado de detección de distancia/contorno 30, el procesado de salida de mensajes de guía 32, y el procesado de extracción de imagen de vasos sanguíneos 34 son los mismos que en la figura 5.

El procesado de búsqueda de imagen registrada de vasos sanguíneos 46 recupera conjuntos de datos registrados de imagen de vasos sanguíneos R1, R2, R3 correspondientes a la ID individual (número de cuenta) de la tarjeta CI 5 de la porción de almacenamiento 7-1. El procesado de verificación 44 compara el conjunto de datos de imagen de vasos sanguíneos N1 recuperado en el procesado de detección de imagen de vasos sanguíneos 34 con el conjunto de datos registrados de imagen de vasos sanguíneos N2, realiza el procesado de verificación, y envía el resultado de la verificación.

El procesado de salida de forma de mano 38 recupera los datos de forma registrados 72 correspondientes a la ID individual (número de cuenta) de la tarjeta CI 5 de la porción de almacenamiento antes descrita 7-1, y visualiza los datos en el POU 6-1. La imagen visualizada puede ser un mapa de bits de la imagen al tiempo del registro, como en la figura 7, o puede ser datos de contorno de la mano, extraídos de la imagen capturada.

En tal sistema de autenticación biométrica, la imagen capturada antes descrita para uso en autenticación al tiempo del registro es registrada, y la visualización de esta imagen para el usuario al tiempo de la autenticación es conveniente para el usuario, y es ventajosa con respecto a la operación realizada por usuarios no familiarizados con el sistema de autenticación, y con respecto al procesado de autenticación rápida.

60 *Procesado del registro biométrico*

A continuación se explica el procesado del registro biométrico de la figura 5. La figura 9 representa el flujo de procesado del registro biométrico en una realización de la invención. A continuación se explica el procesado del registro biométrico de la figura 9, con referencia a la figura 2 y la figura 5.

(S10) El usuario, que ha pedido autenticación de venas, pone la mano sobre el dispositivo de captura de imagen de la palma 1 del terminal de zona de servicio 2. El dispositivo de captura de imagen 1 lee una imagen de la palma, y envía la imagen al ordenador 2-1.

ES 2 334 157 T3

(S12) El ordenador 2-1 extrae una imagen de vasos sanguíneos de la palma de la imagen leída, y crea datos de imagen de vasos sanguíneos 70. Estos datos de imagen de vasos sanguíneos son el resultado de extraer características específicas de la imagen de vasos sanguíneos representada en la figura 8 (las direcciones y el número de troncos y bifurcaciones de vasos sanguíneos, y análogos).

5

(S14) El procesado de estos pasos S10 y S12 se repite una pluralidad de veces (por ejemplo, n veces), y después de repetirse n veces (por ejemplo, tres veces), se obtiene una pluralidad de conjuntos de datos de imagen de vasos sanguíneos.

10 (S16) El ordenador determina si la semejanza de la pluralidad de conjuntos de datos de imagen de vasos sanguíneos es igual o excede de un valor umbral. Si la semejanza no es igual o mayor que el valor umbral, se puede producir reconocimiento erróneo, y así se presenta un mensaje de guía, tal como “por favor, extiende de nuevo la mano”, en el POU 6-1, y el procesado vuelve al paso S10.

15 (S18) Si la semejanza de la pluralidad de conjuntos de datos de imagen de vasos sanguíneos es igual o mayor que el valor umbral, estos conjuntos de datos de imagen de vasos sanguíneos son transferidos al servidor 4, conjuntamente con el número de identificación (por ejemplo, el número de cuenta) leído en la tarjeta CI 5.

20 (S20) Además, la imagen leída por el dispositivo de captura de imagen 1 (véase la figura 7), que era la base para la creación de los datos de imagen de vasos sanguíneos, es transferida al servidor 4. El servidor 4 convierte los datos transferidos a un formato preestablecido, y transfiere el resultado al host 7. El host 7 guarda el número de identificación transferido (por ejemplo, número de cuenta), los datos de imagen de vasos sanguíneos 70, y los datos de forma externa (imagen leída) 72 al archivo de imágenes de vasos sanguíneos 7-1.

25 De esta forma, la imagen capturada al tiempo del registro se almacena conjuntamente con los datos de imagen de vasos sanguíneos.

Procesado de autenticación biométrica

30 A continuación se explica el procesado de autenticación biométrica en el CA 6 de la figura 3 y la figura 4. La figura 10 representa el flujo de procesado de autenticación biométrica en una realización de la invención. A continuación, el procesado de autenticación biométrica de la figura 10 se explica con referencia a la figura 3, la figura 4, y la figura 6.

35 (S30) En un estado de espera de cliente, la unidad de control 67 del CA 6 detecta si se ha pulsado una tecla de transacción en el POU 6-1. Si se ha pulsado una tecla de transacción, y se introduce una tarjeta CI 5 en el dispositivo de lectura/escritura de tarjetas CI 60 del CA 6, el dispositivo de lectura/escritura de tarjetas CI 60 lee datos de la tarjeta CI 5.

40 (S32) Estos datos son transmitidos al host 7 mediante la LAN 82 y el servidor 4. El host 7 busca el archivo de imágenes de vasos sanguíneos 7-1 y lee los datos de imagen de vasos sanguíneos 70 y los datos de forma externa 72 correspondientes al número de identificación transmitido desde el archivo 7-1, y transmite los datos al CA 6 mediante el servidor 4 y la LAN 82.

45 (S34) En el CA 6, la forma externa al tiempo del registro de los datos de forma externa transmitidos 72 es visualizada en el POU 6-1, para reproducir el estado de captura de imagen para el usuario al tiempo del registro. El contenido visualizado es el mismo que el representado en la figura 7.

50 (S36) Al ver esto, el usuario extiende la mano sobre el dispositivo de captura de imagen 1-1 del CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma, adquiere información de verificación de parte del cuerpo, y envía la información a la unidad de control 67 del CA 6. La unidad de control 67 detecta los datos de imagen de vasos sanguíneos (información de verificación de parte del cuerpo) para la palma.

55 (S38) Además, la unidad de control 67 extrae datos característicos de parte del cuerpo (por ejemplo, las direcciones y el número de troncos y longitudes de las bifurcaciones de vasos sanguíneos, y análogos) de los datos de imagen de vasos sanguíneos.

60 (S40) Además, la unidad de control 67 verifica los datos característicos de parte del cuerpo extraídos contra los datos característicos de la imagen de vasos sanguíneos transmitidos desde el host 7, y confirma la identidad del individuo.

(S42) Si la confirmación del individuo es satisfactoria, entonces la unidad de control 67 envía un resultado de autenticación OK, y el CA 6 permite transacciones automáticas ordinarias. Por otra parte, si la confirmación del individuo no es satisfactoria, la unidad de control 67 visualiza un mensaje de guía en el POU 6-1, y el procesado vuelve al paso S36. Como el mensaje de guía, se presenta la causa de la no coincidencia de verificación estándar. Por ejemplo, se puede presentar “Por favor, extiende la palma”, “Se ha desplazado la posición de la mano”, u otro texto, y una imagen de orden de operación estándar.

ES 2 334 157 T3

De esta forma se registra una imagen de la forma de parte del cuerpo capturada del usuario al tiempo del registro de datos biométricos, y al tiempo de la autenticación del usuario, presentando esta forma de parte del cuerpo, el usuario puede identificar directamente el estado de captura de imagen de la parte del cuerpo al tiempo del registro. Como resultado, al usuario se le pueden dar instrucciones de guía relativas a un estado de captura de imagen de la parte del cuerpo similares a las del tiempo del registro, de modo que, al tiempo de la autenticación, se pueden dar indicaciones de guía efectivas relativas a la posición de la parte del cuerpo con el fin de adaptarla a las circunstancias de captura de imagen de la parte del cuerpo durante el registro, con el fin de mejorar la eficiencia de verificación.

Además, incluso cuando la autenticación biométrica no tiene éxito, se pueden dar instrucciones de guía para mover la parte del cuerpo a las circunstancias de captura de imagen de la parte del cuerpo al tiempo del registro sin confundir al usuario, facilitando así la autenticación biométrica del usuario. En particular cuando se usa en equipo automatizado, puede no haber personal dedicado *in situ*, sino que el usuario puede recibir indicaciones de guía fiables, mejorando así la eficiencia de verificación y contribuyendo a acortar el tiempo requerido para la verificación.

15 *Otro procesado de autenticación biométrica*

A continuación, se explica otro procesado de autenticación biométrica en el CA 6 de la figura 3 y la figura 4. La figura 11 representa el flujo de procesado de autenticación biométrica en otra realización de la invención; la figura 12 explica el ejemplo de visualización de la forma de parte del cuerpo. A continuación, el procesado de autenticación biométrica de la figura 11 se explica con referencia a la figura 3, la figura 4, la figura 6, y la figura 12. A los pasos que son idénticos a los de la figura 10 se les asignan los mismos símbolos.

(S30) En un estado de espera de cliente, la porción de control 67 del CA 6 detecta si se ha pulsado una tecla de transacción en el POU 6-1. Si se ha pulsado una tecla de transacción, y se introduce una tarjeta CI 5 en el dispositivo de lectura/escritura de tarjetas CI 60 del CA 6, el dispositivo de lectura/escritura de tarjetas CI 60 lee datos de la tarjeta CI 5.

(S32) Estos datos son transmitidos al host 7 mediante la LAN 82 y el servidor 4. El host 7 busca el archivo de imágenes de vasos sanguíneos 7-1 y lee los datos de imagen de vasos sanguíneos 70 y los datos de forma externa 72 correspondientes al número de identificación transmitido desde el archivo 7-1, y transmite los datos al CA 6 mediante el servidor 4 y la LAN 82.

(S34) En el CA 6, la forma externa al tiempo del registro de los datos de forma externa transmitido 72 es visualizada en el POU 6-1, para reproducir el estado de captura de imagen del usuario al tiempo del registro. El contenido visualizado es el mismo que el representado en la figura 7.

(S36) Al ver esto, el usuario extiende la mano sobre el dispositivo de captura de imagen 1-1 del CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma, adquiere información de verificación de parte del cuerpo, y envía la información a la porción de control 67 del CA 6. La unidad de control 67 detecta los datos de imagen de vasos sanguíneos (información de verificación de parte del cuerpo) de la palma.

(S37) La unidad de control 67 extrae la información de verificación de parte del cuerpo (datos de forma de parte del cuerpo) adquiridos en el paso S36, visualiza esta forma de parte del cuerpo al tiempo de la verificación en paralelo con la forma externa al tiempo del registro visualizada en el paso S34 en el POU 6-1. Como se representa en la figura 12, la forma externa al tiempo de la verificación (forma de verificación) se combina con la forma externa al tiempo del registro (forma de registro), y ambas son visualizadas en el POU 6-1. En este ejemplo, la forma externa de la mano al tiempo del registro (forma de registro) es visualizada conjuntamente con la forma externa de la mano al tiempo de la verificación (forma de verificación).

(S38) Además, la unidad de control 67 extrae datos característicos de parte del cuerpo (por ejemplo, las direcciones y el número de troncos y longitudes de bifurcaciones de vasos sanguíneos, y análogos) de los datos de imagen de vasos sanguíneos.

(S40) Además, la unidad de control 67 verifica los datos característicos de parte del cuerpo extraídos contra los datos característicos de la imagen de vasos sanguíneos transmitidos desde el host 7, y confirma la identidad del individuo.

(S42) Si la confirmación del individuo es satisfactoria, entonces la unidad de control 67 envía un resultado de autenticación OK, y el CA 6 permite transacciones automáticas ordinarias. Por otra parte, si la confirmación del individuo no es satisfactoria, la unidad de control 67 visualiza un mensaje de guía en el POU 6-1, y el procesado vuelve al paso S36. Como el mensaje de guía, se presenta la causa de no coincidencia de verificación estándar. Por ejemplo, se puede presentar "Por favor, extienda la palma", "Se ha desplazado la posición de la mano", u otro texto, y una imagen de orden de operación estándar.

De esta forma, se registra la forma de parte del cuerpo capturado para el usuario al tiempo del registro de datos biométricos, y al tiempo de la autenticación del usuario, presentando esta forma de parte del cuerpo y la forma de parte del cuerpo durante la verificación, el usuario puede identificar directamente el estado de captura de imagen de la parte del cuerpo al tiempo del registro y el estado de captura de imagen de la parte del cuerpo al tiempo de la verificación. Como resultado, cuando la autenticación biométrica no tiene éxito, el usuario puede ser guiado a un estado de captura

de imagen de la parte del cuerpo similar a la del tiempo del registro, de modo que, al tiempo de la autenticación, se pueden ofrecer indicaciones de guía efectivas relativas a la posición de la parte del cuerpo con el fin de adaptarla a las circunstancias de captura de imagen de la parte del cuerpo durante registro, con el fin de mejorar la eficiencia de verificación.

5 Además, se pueden dar indicaciones de guía para mover la parte del cuerpo a las circunstancias de captura de imagen de la parte del cuerpo al tiempo del registro sin confundir al usuario, facilitando así la autenticación biométrica del usuario. En particular, cuando se usa en equipo automatizado, no tiene que haber personal dedicado *in situ*, sino que al usuario se le pueden ofrecer indicaciones de guía fiables, mejorando así la eficiencia de verificación y contribuyendo a acortar el tiempo requerido para la verificación.

Segunda realización de un sistema biométrico

15 La figura 13 representa la configuración del sistema biométrico de una segunda realización de la invención. En la figura 13, al igual que en la figura 1, se representa un sistema de autenticación de venas de la palma en una institución financiera como un ejemplo de un sistema de autenticación biométrica. En la figura 13, a las porciones que son idénticas a las de la figura 1 se les asignan los mismos símbolos.

20 En la figura 13, el terminal de sucursal 2 explicado en la figura 2 está dispuesto en una zona de servicio de la institución financiera. Como se ha explicado en la figura 2, el terminal de sucursal 2 está provisto de un dispositivo de captura de imagen de la palma 1, y, conectado a él, un ordenador de terminal de sucursal (por ejemplo, un ordenador personal) 2-1, teclado 2-2, pantalla 2-3, y dispositivo de lectura/escritura de tarjetas CI 2-4.

25 Al igual que en la figura 2, el dispositivo de captura de imagen de la palma 1 tiene una unidad sensora 18, guía delantera 14 para soportar la muñeca del usuario, y una guía trasera 13 para guiar los dedos del usuario. El usuario, que ha pedido autenticación de venas, pone la mano sobre este dispositivo de captura de imagen de la palma 1. El dispositivo de captura de imagen (a continuación "dispositivo de captura de imagen") 1 lee la imagen de la palma, y envía la imagen al ordenador 2-1.

30 El dispositivo de lectura/escritura de tarjetas CI 2-4 lee y escribe datos de y a una tarjeta CI 5 que tiene el usuario. La tarjeta CI 5 es una tarjeta conocida del tamaño de una tarjeta de crédito, que incorpora un chip CI con memoria y una CPU, y que tiene terminales externos.

35 El dispositivo de captura de imagen 1, el dispositivo de lectura/escritura de tarjetas CI 2-4, el teclado 2-2 y la pantalla 2-3 están conectados al ordenador 2-1, y realizan la extracción de imagen de vasos sanguíneos, registro de forma y otro procesado, descritos anteriormente.

40 Este terminal 2 está conectado, mediante una LAN (red de área local) 80, al servidor 4. El servidor 4 tiene un archivo temporal 4-1, y está conectado a un host (el host 7 de la figura 1), no representado. El servidor 4 está conectado, mediante una segunda LAN 82, a una pluralidad de máquinas de transacciones automáticas (CAs) 6.

45 Este CA 6 puede ser usado para realizar transacciones basadas en la autenticación de venas. Cuando el usuario usa un CA 6 para realizar extracción u otra transacción con dinero en efectivo, extiende su mano sobre un dispositivo de captura de imagen 1-1, dispuesto en el CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma. El CA 6 tiene un dispositivo de lectura/escritura de tarjetas CI 60, y lee y escribe los datos de y sobre la tarjeta CI 5 que tiene el usuario.

50 En esta realización, al tiempo del registro, el terminal 2 guarda datos característicos de vasos sanguíneos 70 y datos de forma externa 72 en la tarjeta CI 5 del usuario. En el CA 6, el dispositivo de lectura/escritura de tarjetas CI 60 lee los datos de forma externa en la tarjeta CI 5 y visualiza la forma externa en el POU 6-1.

55 Además, la tarjeta CI 5 está provista de las funciones para procesado de verificación 44 y procesado de búsqueda de imagen registrada de vasos sanguíneos 46 de la figura 6. Los datos característicos de la imagen de vasos sanguíneos al tiempo de la verificación, leídos por el dispositivo de captura de imagen 1-1 del CA 6 y extraídos, son transmitidos a la tarjeta CI 5 mediante el dispositivo de lectura/escritura de tarjetas CI 60. La tarjeta CI 5 verifica los datos característicos registrados de la imagen de vasos sanguíneos contra datos característicos de la imagen de vasos sanguíneos de verificación a través del procesado de verificación antes descrito 44 y el procesado de búsqueda de imagen registrada de vasos sanguíneos 46, y notifica a la unidad de control 67 en el CA 6 el resultado de la verificación.

60 Como resultado, los datos registrados de imagen de vasos sanguíneos 70 permanecen en la tarjeta CI 5, y no son leídos por el CA 6, de modo que se puede evitar una réplica ilícita y análogos, contribuyendo a una mayor seguridad.

65 Como se ha explicado en la figura 11 y la figura 12, la forma externa al tiempo de la verificación (forma de verificación) también puede ser visualizada en el POU 6-1 conjuntamente con la forma externa al tiempo del registro (forma de registro). Es decir, como se representa en la figura 12, la forma externa de la mano al tiempo de la verificación (forma de verificación) es visualizada conjuntamente con la forma externa de la mano al tiempo del registro (forma de registro).

ES 2 334 157 T3

También en esta realización, además de resultados ventajosos similares a los de la figura 1, la verificación se realiza dentro de la tarjeta CI 5, contribuyendo a una mayor seguridad; además, dado que la comunicación con el host 7 y el servidor 4 no es necesaria para la visualización de formas externas, se alivia la carga del host 7 y del servidor 4, y la base de datos de vena 7-1 en el host 7 puede ser de tamaño reducido.

5

Tercera realización de un sistema biométrico

La figura 14 representa la configuración de una tercera realización de un sistema de autorización biométrica de esta invención. En la figura 14, al igual que en la figura 1 y la figura 13, se representa un sistema de autenticación de venas de la palma en una institución financiera, como un ejemplo de un sistema biométrico. En la figura 14, a las porciones que son idénticas a las de la figura 1 y la figura 13 se les asignan los mismos símbolos.

En la figura 14, un terminal de sucursal 2 explicado en la figura 2 está dispuesto en una zona de servicio de la institución financiera. Como se ha explicado en la figura 2, el terminal de sucursal 2 está provisto de un dispositivo de captura de imagen de la palma 1, un ordenador de terminal de sucursal (por ejemplo, un ordenador personal) 2-1 conectado al dispositivo de captura de imagen 1, un teclado 2-2, una pantalla 2-3, y un dispositivo de lectura/escritura de tarjetas CI 2-4.

Al igual que en la figura 2, el dispositivo de captura de imagen de la palma 1 tiene una unidad sensora 18, una guía delantera 14 para soportar la muñeca del usuario, y una guía trasera 13 para guiar los dedos del usuario. El usuario, que ha pedido autenticación de venas, pone la mano sobre este dispositivo de captura de imagen de la palma 1. El dispositivo de captura de imagen (a continuación "dispositivo de captura de imagen") 1 lee la imagen de la palma, y envía la imagen al ordenador 2-1.

25

El dispositivo de lectura/escritura de tarjetas CI 2-4 lee y escribe datos de y a una tarjeta CI 5 que tiene el usuario. La tarjeta CI 5 es una tarjeta conocida del tamaño de una tarjeta de crédito, que incorporan un chip CI con memoria y una CPU, y que tiene terminales externos.

El dispositivo de captura de imagen 1, el dispositivo de lectura/escritura de tarjetas CI 2-4, el teclado 2-2 y la pantalla 2-3 están conectados al ordenador 2-1, y realizan la extracción de imagen de vasos sanguíneos, registro de forma y otro procesado, descritos anteriormente.

30

El terminal 2 está conectado a un servidor 4 mediante una LAN (red de área local) 80. El servidor 4 tiene un archivo temporal 4-1, y está conectado al host 7. El servidor 4 también está conectado a una pluralidad de máquinas de transacciones automáticas (CAs) 6 mediante una segunda LAN 82.

35

Dicho CA 6 puede ser usado para realizar transacciones basadas en la autenticación de venas. Con el fin de usar un CA 6 para realizar transacciones de extracción y otras transacciones financieras, el usuario pone la mano sobre el dispositivo de captura de imagen 1-1 dispuesto en el CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma. El CA 6 tiene un dispositivo de lectura/escritura de tarjetas CI 60, que lee y escribe datos en una tarjeta CI 5 que tiene el usuario.

En esta realización, al tiempo del registro, el terminal 2 guarda datos característicos de la imagen de vasos sanguíneos 70 en la tarjeta CI 5 del usuario, y guarda datos de forma externa 72 en la base de datos de vena 7-1 del host 7. En el CA 6, la tarjeta CI 5 del usuario se introduce en el dispositivo de lectura/escritura de tarjetas CI 60, se lee un número de identificación, se leen datos de forma externa de la base de datos de vena 7-1 del host 7 mediante el servidor 4, y se presenta la forma externa en el POU 6-1.

45

La tarjeta CI 5 está provista de las funciones para el procesado de verificación 44 y procesado de búsqueda de imagen registrada de vasos sanguíneos 46 de la figura 6. Los datos característicos de la imagen de vasos sanguíneos al tiempo de la verificación, que son leídos y extraídos por el dispositivo de captura de imagen 1-1 del CA 6, son transmitidos a la tarjeta CI 5 mediante el dispositivo de lectura/escritura de tarjetas CI 60. Por medio del procesado de verificación antes descrito 44 y el procesado de búsqueda de imagen registrada de vasos sanguíneos 46, la tarjeta CI 5 verifica los datos característicos registrados de la imagen de vasos sanguíneos contra los datos característicos de verificación de la imagen de vasos sanguíneos, y notifica a la unidad de control 67 del CA 6 el resultado de la verificación.

50

Como resultado de lo anterior, los datos registrados de imagen de vasos sanguíneos 70 permanecen en la tarjeta CI 5, y no son leídos por el CA 6, de modo que se puede evitar la reproducción ilícita, contribuyendo a una mayor seguridad.

60

Además, como se ha explicado en la figura 11 y la figura 12, además de la forma externa al tiempo del registro (forma de registro), también se puede visualizar en el POU 6-1 la forma externa al tiempo de la verificación (forma de verificación). Es decir, como se representa en la figura 12, la forma externa de la mano al tiempo del registro (forma de registro) se combina con la forma externa de la mano al tiempo de la verificación (forma de verificación) y se visualiza.

65

ES 2 334 157 T3

También en esta realización, además de resultados ventajosos similares a los de la figura 1, la verificación se realiza dentro de la tarjeta CI 5, contribuyendo a una mayor seguridad; además, dado que no se usan formas externas directamente en autenticación biométrica, se puede evitar la degradación de la seguridad incluso cuando tales formas son almacenadas en el host 7, y se puede mitigar la carga impuesta a la tarjeta CI 5.

5

Cuarta realización de un sistema biométrico

La figura 15 representa la configuración del sistema de autenticación biométrica de una cuarta realización de la invención. En la figura 15, al igual que en la figura 1, la figura 13 y la figura 14, un sistema de autenticación de venas de la palma en una institución financiera se representa como un ejemplo de un sistema de autenticación biométrica. En la figura 15, a las porciones que son idénticas a las de la figura 1, la figura 13, y la figura 14 se les asignan los mismos símbolos.

En la figura 15, el terminal de sucursal 2 explicado en la figura 2 está dispuesto en una zona de servicio de la institución financiera. Como se ha explicado en la figura 2, el terminal de sucursal 2 está provisto de un dispositivo de captura de imagen de la palma 1, y, conectado a él, un ordenador de terminal de sucursal (por ejemplo, un ordenador personal) 2-1, teclado 2-2, pantalla 2-3, y dispositivo de lectura/escritura de tarjetas CI 2-4.

Al igual que en la figura 2, el dispositivo de captura de imagen de la palma 1 tiene una unidad sensora 18, guía delantera 14 para soportar la muñeca del usuario, y una guía trasera 13 para guiar los dedos del usuario. El usuario, que ha pedido autenticación de venas, pone la mano sobre este dispositivo de captura de imagen de la palma 1. El dispositivo de captura de imagen (a continuación "dispositivo de captura de imagen") 1 lee la imagen de la palma, y envía la imagen al ordenador 2-1.

25

El dispositivo de lectura/escritura de tarjetas CI 2-4 lee y escribe datos de y a una tarjeta CI 5 que tiene el usuario. La tarjeta CI 5 es una tarjeta conocida del tamaño de una tarjeta de crédito, que incorpora un chip CI con memoria y una CPU, y que tiene terminales externos.

El dispositivo de captura de imagen 1, el dispositivo de lectura/escritura de tarjetas CI 2-4, el teclado 2-2 y la pantalla 2-3 están conectados al ordenador 2-1, y realizan la extracción de imagen de vasos sanguíneos, registro de forma y otro procesado, descritos anteriormente.

El terminal 2 está conectado a un servidor 4 mediante una LAN (red de área local) 80. El servidor 4 tiene un archivo temporal 4-1, y está conectado al host 7. El servidor 4 también está conectado a una pluralidad de máquinas de transacciones automáticas (CAs) 6 mediante una segunda LAN 82.

Dicho CA 6 puede ser usado para realizar transacciones basadas en autenticación de venas. Con el fin de usar un CA 6 para realizar transacciones de extracción y otras transacciones financieras, el usuario pone la mano sobre el dispositivo de captura de imagen 1-1 dispuesto en el CA 6. El dispositivo de captura de imagen 1-1 lee una imagen de la palma. El CA 6 tiene un dispositivo de lectura/escritura de tarjetas CI 60, que lee y escribe datos en una tarjeta CI 5 que tiene el usuario.

Además, un teléfono 6-6 para comunicación telefónica mediante un centro de llamadas 8 y red de circuito público 9 están dispuestos en el CA 6. Un terminal 80 conectado al host 7 está dispuesto en el centro de llamadas 8. Cuando hay una consulta del usuario mediante el teléfono 6-6 del CA 6, el personal dedicado presente en el centro de llamadas 8 opera el terminal 80, y mientras ve la pantalla del terminal 80, responde a la consulta del usuario por el teléfono.

En esta realización, al tiempo del registro, el terminal 2 guarda datos característicos de la imagen de vasos sanguíneos 70 en la tarjeta CI 5 del usuario, y guarda datos de forma externa 72 en la base de datos de vena 7-1 del host 7. En el CA 6, el usuario introduce la tarjeta CI 5 en el dispositivo de lectura/escritura de tarjetas CI 60, se lee el número de identificación, y se le notifica al host 7 el número de identificación mediante el servidor 4. Mediante esto, el host 7 lee los datos de forma externa de la base de datos de vena 7-1, y visualiza la forma externa en la pantalla del terminal 80 en el centro de llamadas 8.

Además, la tarjeta CI 5 está provista de las funciones para el procesado de verificación 44 y el procesado de búsqueda de imagen registrada de vasos sanguíneos 46 de la figura 6. Los datos característicos de la imagen de vasos sanguíneos al tiempo de la verificación, que son leídos y extraídos por el dispositivo de captura de imagen 1-1 del CA 6, son transmitidos a la tarjeta CI 5 mediante el dispositivo de lectura/escritura de tarjetas CI 60. Por medio del procesado de verificación antes descrito 44 y el procesado de búsqueda de imagen registrada de vasos sanguíneos 46, la tarjeta CI 5 verifica los datos característicos registrados de la imagen de vasos sanguíneos contra los datos característicos de verificación de la imagen de vasos sanguíneos, y notifica a la unidad de control 67 del CA 6 el resultado de la verificación.

65

En caso de verificación no exitosa, en el CA 6 el usuario llama al personal dedicado situado en el centro de llamadas 8 por el teléfono 6-6 mediante la red de circuito público 9, y consulta la causa del fallo de verificación. El personal dedicado en el centro de llamadas 8 ve la forma externa registrada en el terminal 80 y responde al usuario.

ES 2 334 157 T3

Este personal dedicado conoce las causas del fallo de verificación, y así, al ver la forma externa registrada, puede dar indicaciones e instrucciones de guía apropiadas al usuario.

5 Por ejemplo, en autenticación de la palma, se puede ver una forma externa registrada de la mano, y se pueden
indicar las porciones en que el estado de captura de imagen es diferente al tiempo de la verificación. Es decir, se
pueden dar instrucciones relativas a que la distancia entre la mano y el dispositivo de captura de imagen 1-1, la
extensión de los dedos, prolapso de los dedos, y las posiciones de los dedos con relación al dispositivo de captura de
imagen son diferentes del estado de captura de imagen al tiempo del registro. Mediante esto, el usuario puede seguir las
instrucciones del personal dedicado, alterar el estado de captura de imagen, y puede obtener un resultado satisfactorio
10 de la verificación.

Además, los datos registrados de imagen de vasos sanguíneos 70 permanecen en la tarjeta CI 5, y no son leídos por
el CA 6, de modo que se pueda evitar la reproducción ilícita, contribuyendo a una mayor seguridad.

15 Además, como se ha explicado en la figura 11 y la figura 12, la forma externa al tiempo de la verificación es
transmitida al terminal 80 del centro de llamadas 8 desde el CA 6, mediante el servidor 4 y el host 7. Mediante esto, la
forma externa al tiempo de la verificación (forma de verificación) puede ser visualizada, conjuntamente con la forma
externa al tiempo del registro (forma de registro), en la pantalla del terminal 80 del centro de llamadas 8. Es decir,
como se representa en la figura 12, la forma externa de la mano al tiempo de la verificación (forma de verificación) es
20 visualizada conjuntamente con la forma externa de la mano al tiempo del registro (forma de registro).

Así, el personal dedicado puede ver la forma externa al tiempo del registro (forma de registro) y la forma externa al
tiempo de la verificación (forma de verificación), y puede proporcionar indicaciones de guía e instrucción apropiadas.

25 También en esta realización, la verificación se realiza dentro de la tarjeta CI 5, contribuyendo a una mayor se-
guridad; además, dado que no se usan formas externas directamente en autenticación biométrica, se puede evitar la
degradación de la seguridad incluso cuando dichas formas se almacenan en el host 7, y se puede aliviar la carga
impuesta a la tarjeta CI 5.

30 *Otras realizaciones*

En las realizaciones antes descritas, se explicó la autenticación biométrica sin contacto en términos de autentica-
ción de la configuración de las venas de la palma; sin embargo, también es posible la aplicación a la autenticación de
configuraciones de venas en el reverso de la mano o los dedos, así como a las huellas de la palma u otras características
35 de la mano, y a huellas digitales, características faciales, y autenticación usando otras partes del cuerpo. Además, el
sistema de autenticación biométrica se explicó aplicado a equipo automatizado en empresas financieras; pero también
es posible la aplicación a máquinas automáticas de emisión de billetes, máquinas vendedoras automáticas, y otro equi-
po automatizado en varios campos, así como a ordenadores y a la apertura/cierre de puertas y otras tareas, implicando
la sustitución de una clave, que requieran autenticación individual.

40 Además, en el CA 6 se pueden registrar configuraciones de venas (datos biométricos), y los medios que lleva el
usuario no se limitan a tarjetas CI, sino que pueden ser teléfonos portátiles u otro equipo portátil. Además, también es
posible la aplicación a sistemas de autenticación biométrica que no emplean medios. Además, la visualización de la
forma de registro y forma de verificación en la figura 11 y la figura 12 no se limita a la disposición lateral; es posible
45 la disposición vertical, y también es posible una visualización de solapamiento.

Registrando la forma de la parte del cuerpo del usuario para captura de imagen al tiempo del registro de datos
de la parte del cuerpo, y presentando la forma de parte del cuerpo al usuario al tiempo de la verificación, el usuario
puede identificar directamente el estado de captura de imagen de la parte del cuerpo al tiempo del registro. Como
50 resultado, el usuario puede ser guiado a un estado de captura de imagen de la parte del cuerpo de forma similar a la del
tiempo del registro, de modo que se mejora la eficiencia de la verificación. Además, incluso cuando la autenticación
biométrica no tiene éxito, la parte del cuerpo puede ser guiada a las circunstancias de captura de imagen al tiempo
del registro sin confundir al usuario, aumentando así la conveniencia del usuario en autenticación biométrica. En
particular, cuando se usa en equipo automatizado, no tiene que haber personal dedicado *in situ*, sino que al usuario se
55 le pueden ofrecer indicaciones de guía fiables, mejorando así la eficiencia de la verificación y contribuyendo a acortar
el tiempo requerido para verificación.

60

65

REIVINDICACIONES

1. Un sistema biométrico, que verifica datos característicos de una parte del cuerpo registrados en una unidad de almacenamiento (5, 7-1) contra datos característicos de la parte del cuerpo obtenidos a través de captura de imagen para realizar autenticación individual, incluyendo:

un dispositivo de captura de imagen (1, 1-1) que captura imágenes de la parte del cuerpo;

un dispositivo de control (2, 4, 67) que extrae datos característicos de la parte del cuerpo de la imagen capturada de la parte del cuerpo, y verifica los datos característicos extraídos contra los datos característicos registrados para realizar autenticación individual;

un dispositivo de visualización (2-3, 6-1, 80), que, al tiempo de la autenticación individual, indica una forma de la parte del cuerpo obtenida de una captura de imagen al tiempo del registro de los datos característicos de parte del cuerpo almacenados en la unidad de almacenamiento (5, 7-1), y

una unidad de entrada (2-4, 60) para introducir un número de identificación, con el fin de recuperar, de la unidad de almacenamiento (5, 7-1), datos de forma de la parte del cuerpo del usuario para quien se ha de llevar a cabo la autenticación individual,

donde la unidad de almacenamiento (5, 7-1) guarda, al tiempo del registro de los datos característicos de parte del cuerpo, datos de forma de la parte del cuerpo obtenidos en la captura de imagen de la parte del cuerpo y datos característicos de la parte del cuerpo,

el dispositivo de control (2, 4, 67) lee, al tiempo de la autenticación biométrica, los datos de forma de la parte del cuerpo y los datos característicos de la parte del cuerpo en la unidad de almacenamiento (5, 7-1), y

el dispositivo de control (2, 4, 67) visualiza, en el dispositivo de visualización (2-3, 6-1, 80), una forma de la parte del cuerpo al tiempo de la verificación, obtenida en la captura de imagen por el dispositivo de captura de imagen (1, 1-1), junto con la forma de la parte del cuerpo al tiempo del registro, siendo la mano del usuario la parte del cuerpo en cuestión,

caracterizado porque el dispositivo de captura de imagen (1, 1-1) incluye una unidad de captura de imagen que captura imágenes de al menos una porción de una mano del usuario,

y el dispositivo de control (2, 4, 67) extrae datos de imagen de vasos sanguíneos de la porción de la mano a partir de la imagen capturada, y visualiza, en el dispositivo de visualización (2-3, 6-1, 80), una forma de la mano del mismo usuario al tiempo de la verificación, obtenida en la captura de imagen por el dispositivo de captura de imagen (1, 1-1), junto a y paralela con la forma de la mano al tiempo del registro.

2. El sistema biométrico según la reivindicación 1, incluyendo además un dispositivo de registro de datos biométricos (1, 2), que captura una imagen de la parte del cuerpo, extrae datos de forma de la parte del cuerpo y datos característicos de la parte del cuerpo a partir de la imagen capturada, y guarda los datos en la unidad de almacenamiento (5, 7-1).

3. El sistema biométrico según la reivindicación 1, donde la unidad de entrada es una unidad portátil propiedad del usuario.

4. El sistema biométrico de cualquier reivindicación precedente, donde la unidad de almacenamiento (7-1) está dispuesta en un dispositivo de nivel superior (7) conectado al dispositivo de control (2, 4, 67).

5. El sistema biométrico de cualquiera de las reivindicaciones 1 a 3, donde la unidad de almacenamiento (5) está dispuesta en una unidad portátil propiedad del usuario.

6. El sistema biométrico de cualquiera de las reivindicaciones 1 a 3, donde la unidad de almacenamiento (5, 7-1) incluye:

un dispositivo de nivel superior (7), que está conectado al dispositivo de control (2, 4, 67) y guarda datos de forma de la parte del cuerpo; y

una unidad portátil, que es propiedad del usuario y guarda datos característicos de la parte del cuerpo.

7. El sistema biométrico según la reivindicación 1, incluyendo además:

una unidad de comunicaciones (6-6) por medio de la que, al tiempo de la autenticación individual, el usuario llama a un centro de llamadas; y

ES 2 334 157 T3

dicha unidad de visualización incluye un dispositivo terminal (80) que lee la forma de la parte del cuerpo del usuario en la unidad de almacenamiento (7-1), y visualiza la forma de la mano al tiempo de la verificación, junto a y paralela con la forma de la mano al tiempo del registro en dicho dispositivo de visualización en el centro de llamadas, para permitir que el centro de llamadas dé indicaciones de guía al usuario.

5

8. El sistema biométrico según la reivindicación 5 o la reivindicación 6, donde la unidad portátil verifica los datos característicos de la parte del cuerpo extraídos de la imagen capturada de la parte del cuerpo contra los datos característicos registrados en la unidad de almacenamiento (5, 7-1), y realiza autenticación individual.

10 9. Un método biométrico para verificar datos característicos de parte del cuerpo registrados en una unidad de almacenamiento (5, 7-1) contra datos característicos de parte del cuerpo obtenidos por la captura de imagen para realizar autenticación individual, incluyendo:

15 un paso de captura de imagen que consiste en capturar una imagen, en modo sin contacto, de la parte del cuerpo por un dispositivo de captura de imagen (1, 1-1);

un paso de extraer datos característicos de la parte del cuerpo a partir de la imagen capturada de la parte del cuerpo;

20 un paso de almacenar en la unidad de almacenamiento (5, 7-1), al tiempo del registro de los datos característicos de parte del cuerpo, datos de forma de la parte del cuerpo y datos característicos de la parte del cuerpo obtenidos en la captura de imagen de la parte del cuerpo;

25 un paso de entrada consistente en introducir un número de identificación, con el fin de recuperar, de la unidad de almacenamiento (5, 7-1), datos de forma de la parte del cuerpo del usuario para quien se ha de llevar a cabo la autenticación individual;

un paso de lectura, al tiempo de la autenticación biométrica, de los datos de forma de la parte del cuerpo y los datos característicos de la parte del cuerpo de la unidad de almacenamiento (5, 7-1);

30 un paso de autenticación consistente en verificar los datos característicos extraídos de la parte del cuerpo contra los datos característicos registrados; y

35 un paso de visualización, al tiempo de la autenticación individual, consistente en indicar en un dispositivo de visualización (2-3, 6-1, 80) una forma de la parte del cuerpo obtenida a través de captura de imagen por el dispositivo de captura de imagen (1, 1-1) al tiempo de la verificación, conjuntamente con la forma de la parte del cuerpo al tiempo del registro, siendo la mano del usuario la parte del cuerpo en cuestión,

40 **caracterizado** porque el paso de captura de imagen incluye un paso de captura de imagen que consiste en capturar una imagen de al menos una porción de la mano del usuario,

45 el paso de autenticación incluye un paso de extraer datos de imagen de vasos sanguíneos de la mano de la imagen capturada, y el paso de visualización incluye un paso de presentar en el dispositivo de visualización (2-3, 6-1, 80) una forma de la mano del mismo usuario al tiempo de la verificación, obtenida a través de captura de imagen por el dispositivo de captura de imagen (1, 1-1), junto a y paralela con la forma de la mano al tiempo del registro.

10. El método biométrico según la reivindicación 9, incluyendo además un paso de registro consistente en capturar una imagen de la parte del cuerpo, extraer datos de forma de la parte del cuerpo y datos característicos de la parte del cuerpo de la imagen capturada, y almacenar los datos en la unidad de almacenamiento.

50 11. El método biométrico según la reivindicación 9, donde el paso de entrada incluye un paso de introducción desde una unidad portátil propiedad del usuario.

55 12. El método biométrico de cualquiera de las reivindicaciones 9 a 11, donde el paso de autenticación incluye un paso de leer, en la unidad de almacenamiento dispuesta en un dispositivo de nivel superior conectado a un dispositivo de control que realiza la autenticación, los datos de la forma de parte del cuerpo y los datos de la parte del cuerpo característicos al tiempo del registro.

60 13. El método biométrico de cualquiera de las reivindicaciones 9 a 11, donde el paso de autenticación incluye un paso de leer, en la unidad de almacenamiento dispuesta en una unidad portátil propiedad del usuario, los datos de la forma de parte del cuerpo y los datos de la parte del cuerpo característicos al tiempo del registro.

65 14. El método biométrico de cualquiera de las reivindicaciones 9 a 11, donde el paso de visualización incluye un paso de leer los datos de la forma de parte del cuerpo de un dispositivo de nivel superior conectado a un dispositivo de control que realiza la autenticación,

y donde el paso de autenticación incluye un paso de leer los datos característicos de parte del cuerpo en una unidad portátil propiedad del usuario.

ES 2 334 157 T3

15. El método biométrico según la reivindicación 9, incluyendo además:

un paso en el que el usuario llama a un centro de llamadas desde un dispositivo de comunicaciones al tiempo de la autenticación individual; y

5

un paso de leer los datos de forma de parte del cuerpo del usuario en la unidad de almacenamiento, presentar la forma de la mano al tiempo de la verificación, junto a y paralela con la forma de la mano al tiempo del registro en una unidad de visualización (80) en el centro de llamadas, y proporcionar indicaciones de guía al usuario.

10

16. El método biométrico según la reivindicación 12, donde el paso de autenticación incluye un paso de verificar, por la unidad portátil, los datos característicos de la parte del cuerpo extraídos de la imagen capturada de la parte del cuerpo contra los datos característicos registrados en la unidad de almacenamiento para realizar autenticación individual.

15

20

25

30

35

40

45

50

55

60

65

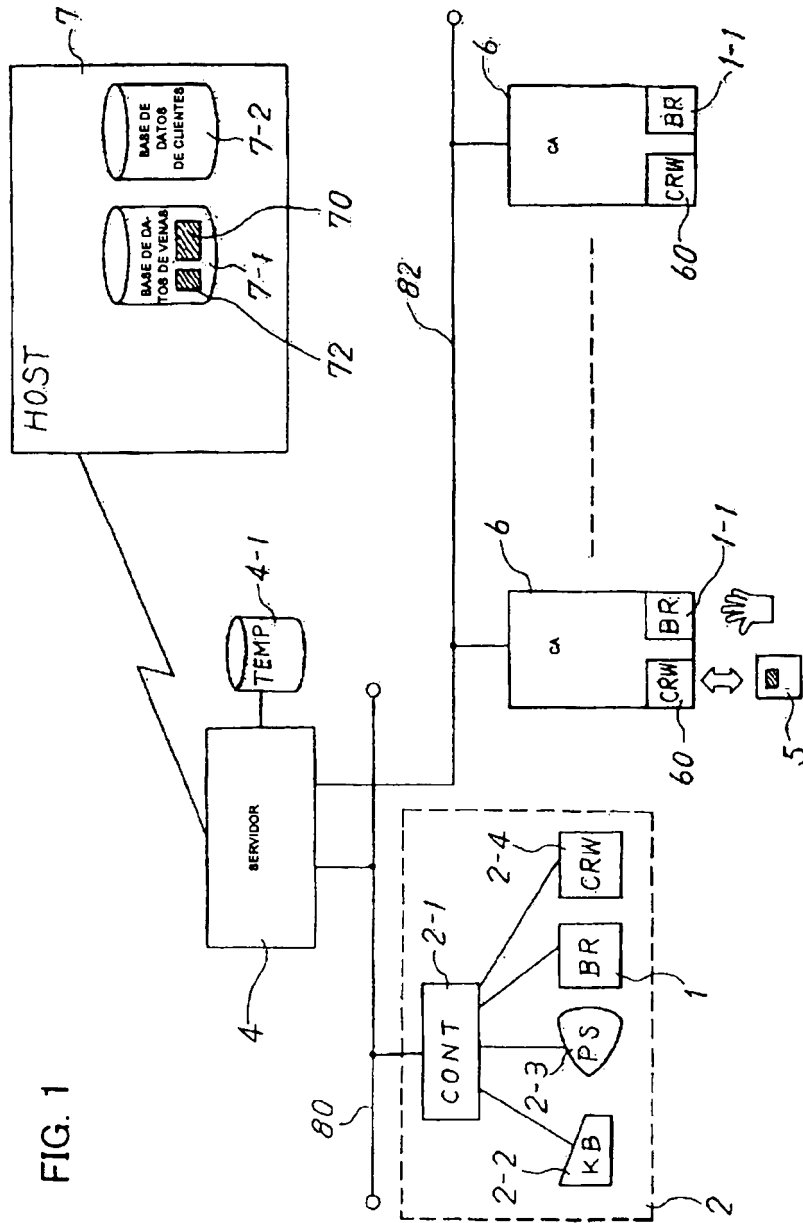


FIG. 1

FIG. 2

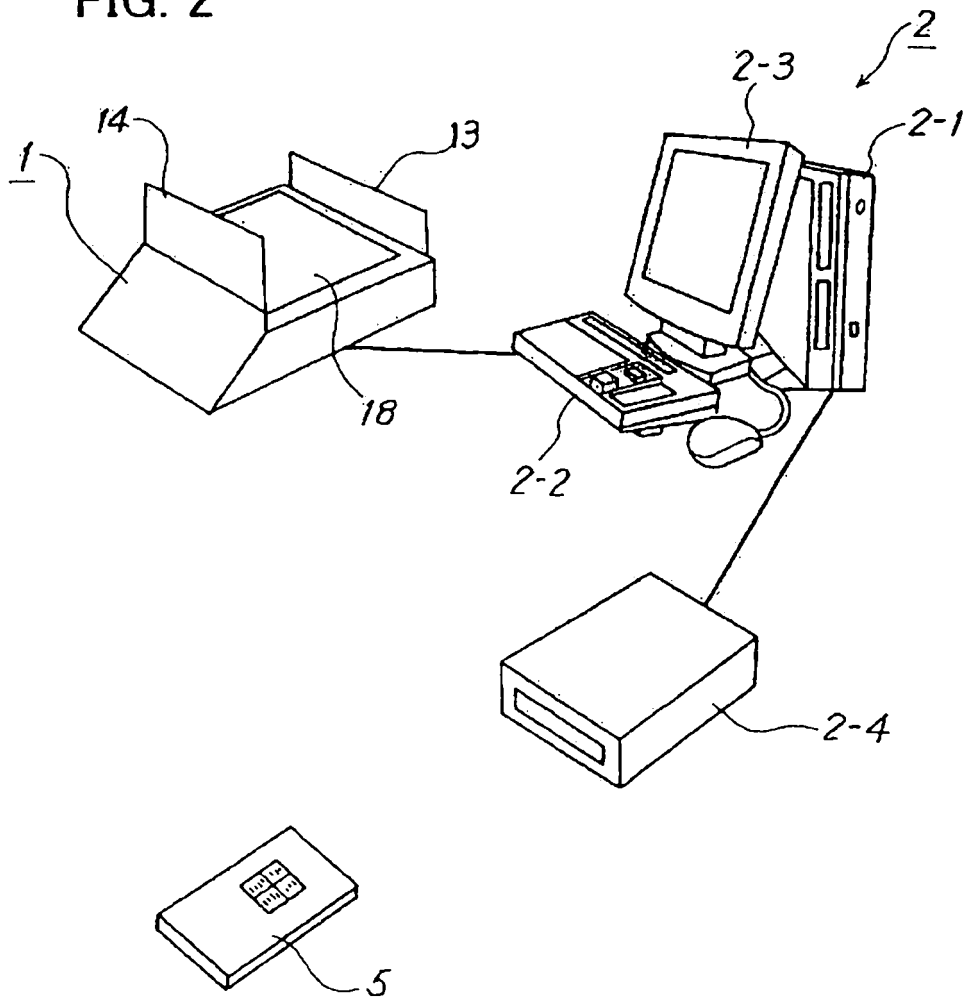


FIG. 3

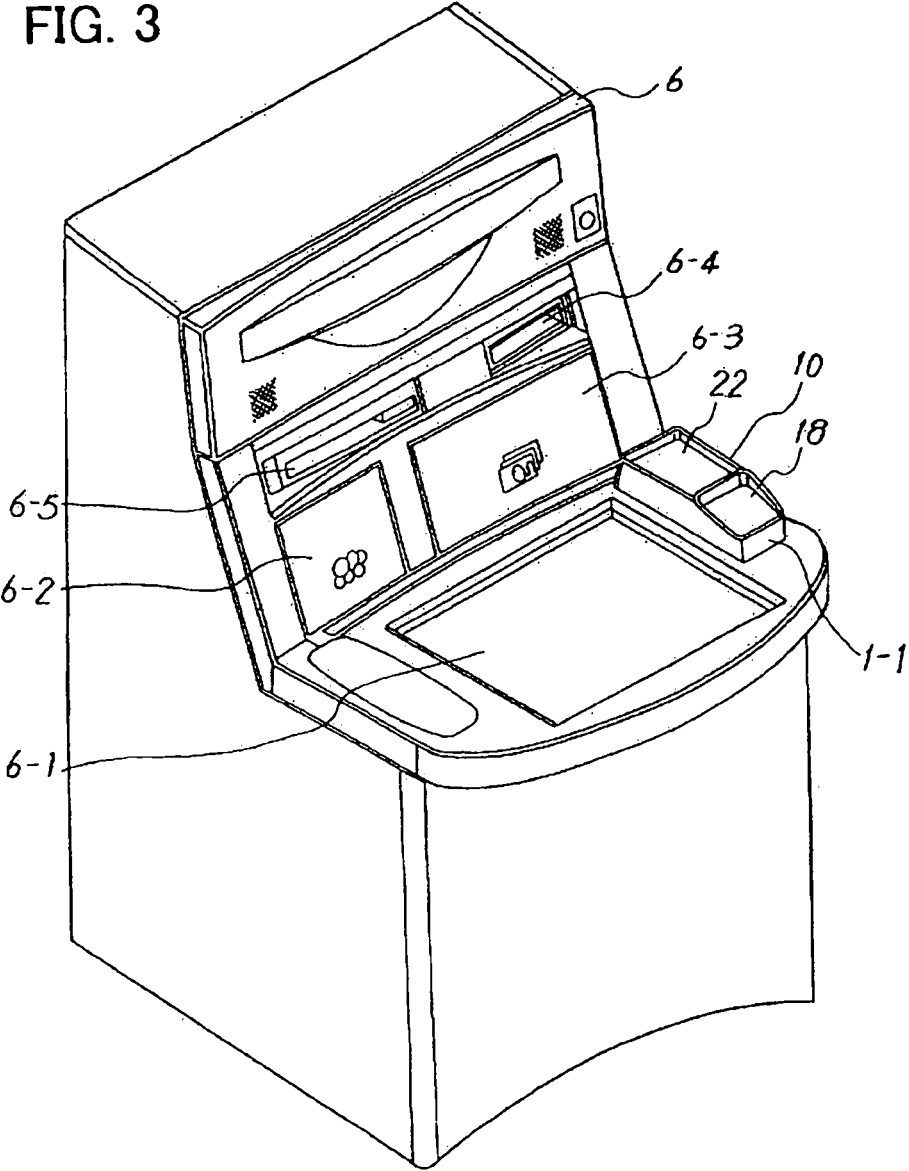


FIG. 5

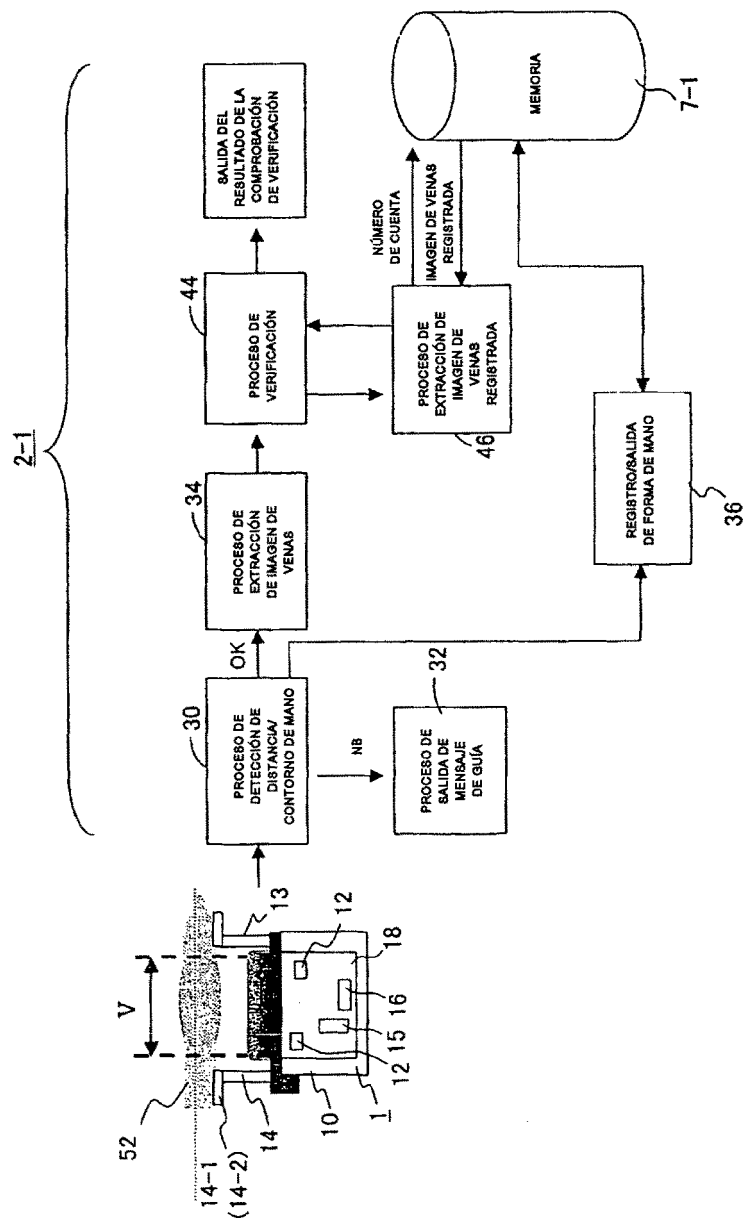


FIG. 6

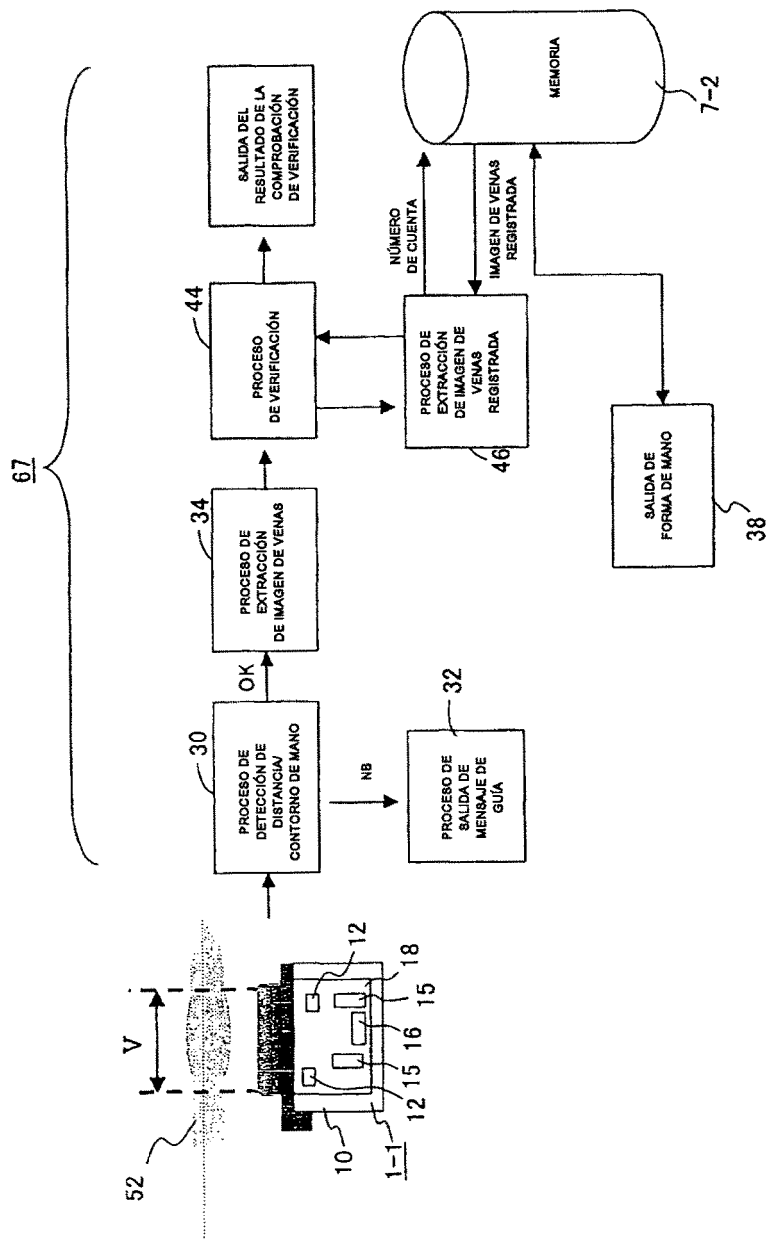


FIG. 7

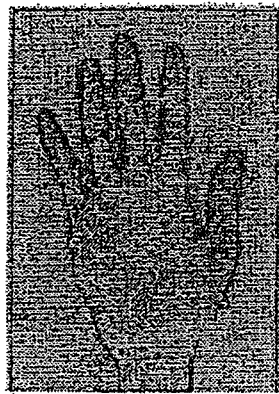


FIG. 8

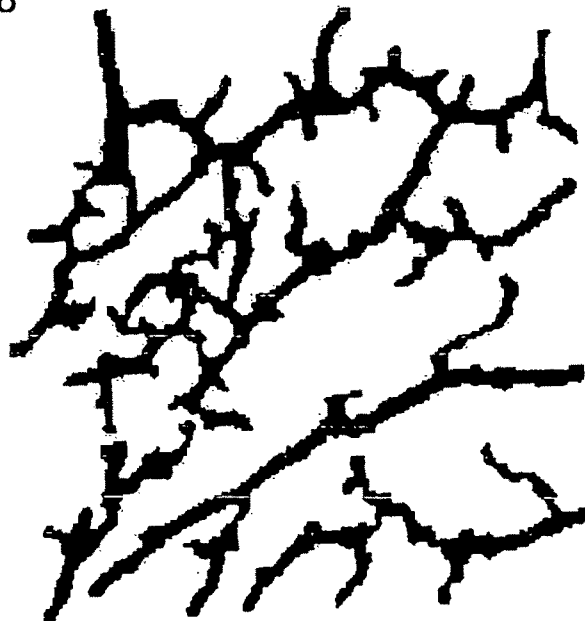


FIG. 9

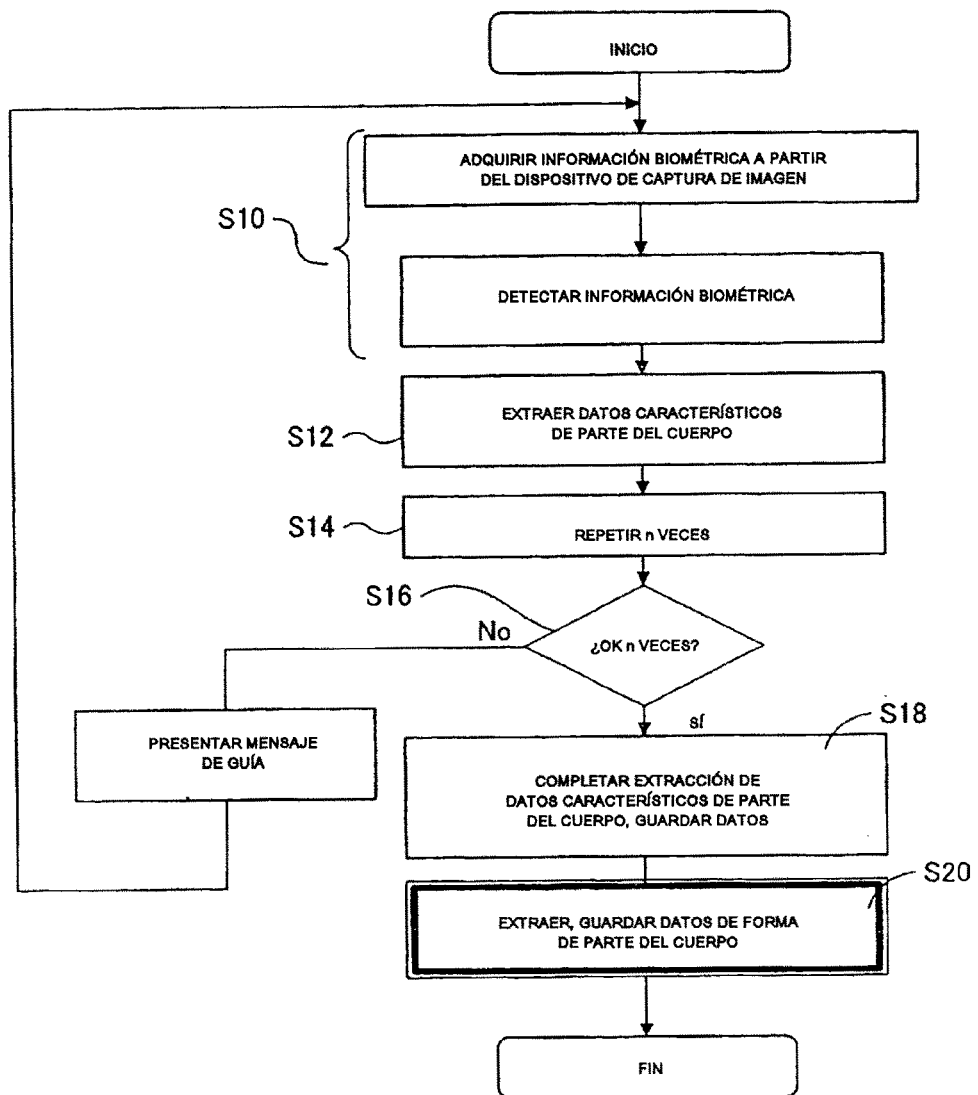


FIG. 10

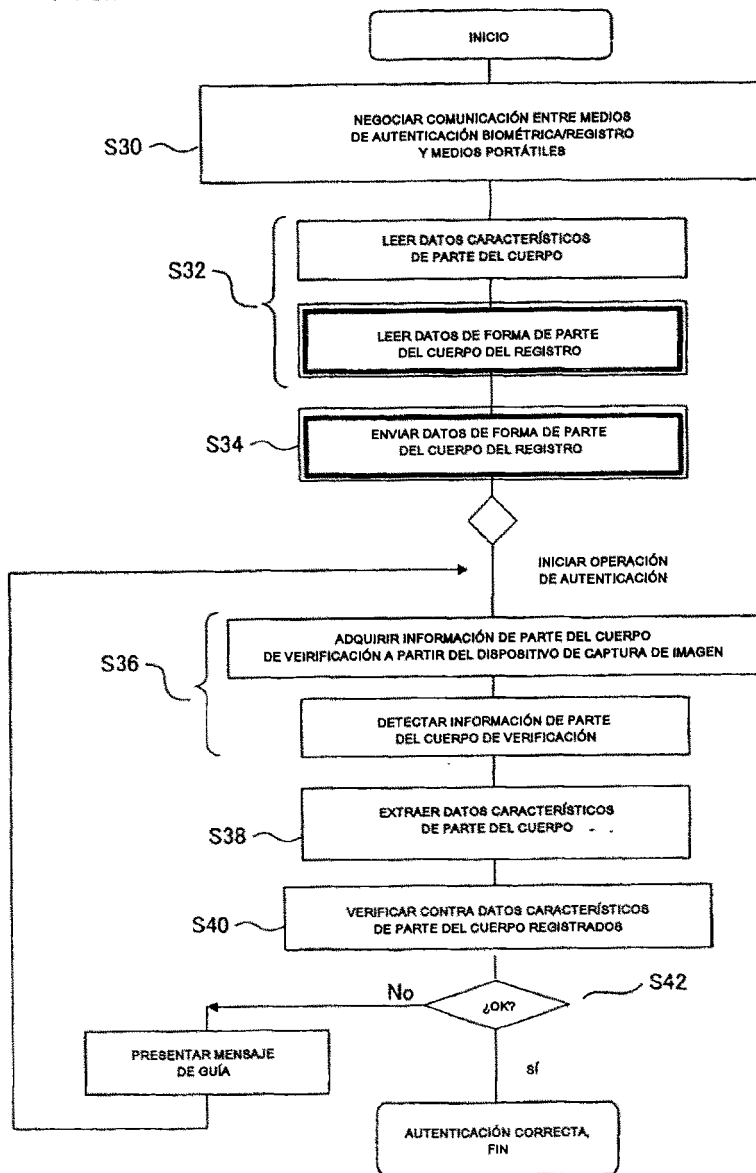


FIG. 11

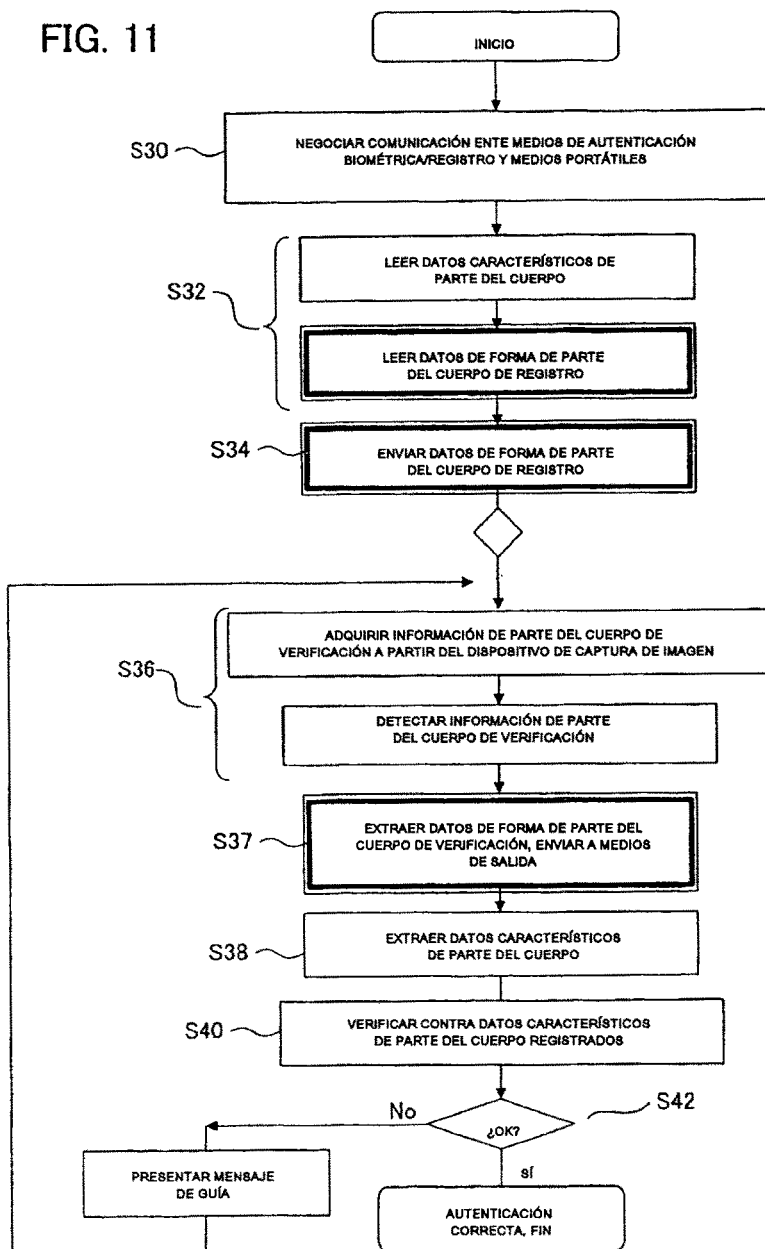


FIG. 12

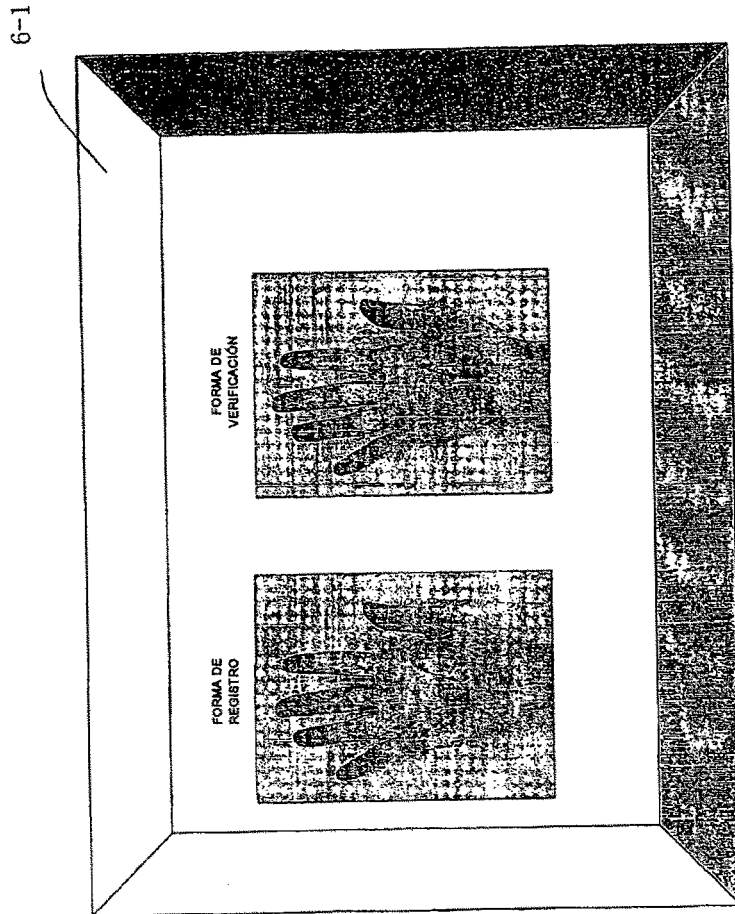
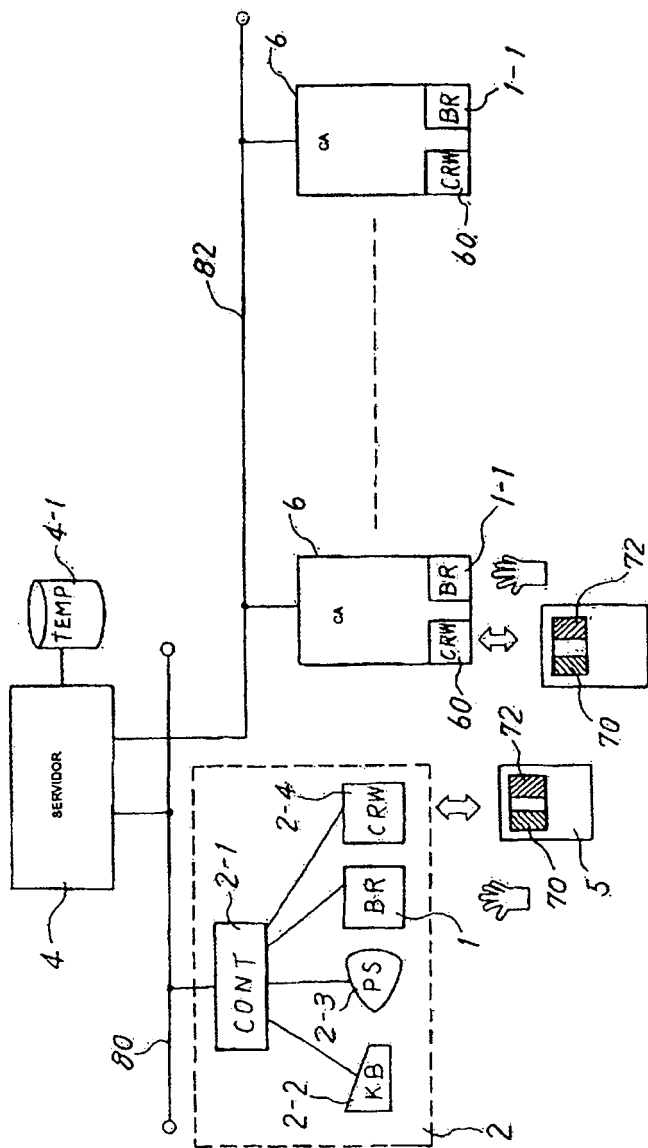


FIG. 13



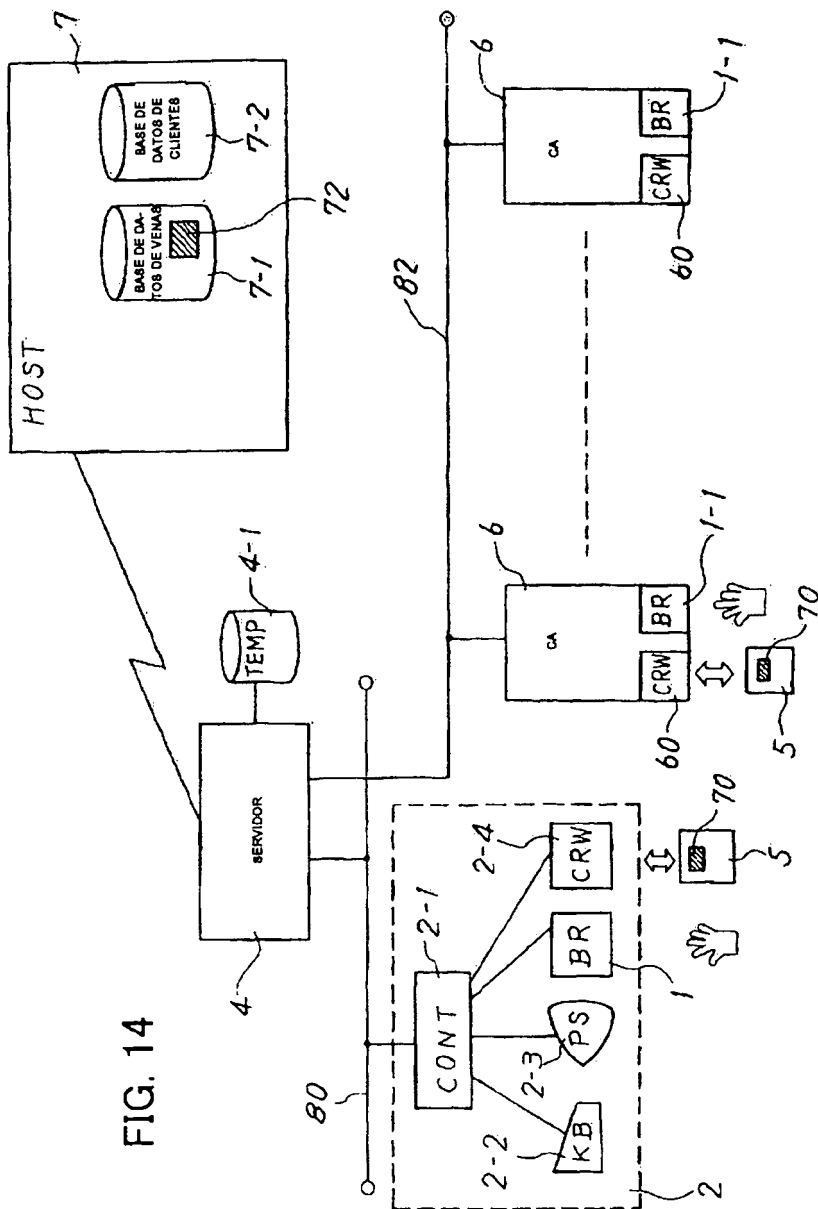


FIG. 14

FIG. 15

