(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 331 138**

(51) Int. Cl.:
G06K 9/00 (2006.01)
G06K 9/62 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05252045 .9**
(96) Fecha de presentación : **31.03.2005**
(97) Número de publicación de la solicitud: **1612717**
(97) Fecha de publicación de la solicitud: **04.01.2006**

(54) Título: **Sistema de autenticación biométrica y método de registro.**

(30) Prioridad: **28.06.2004 JP 2004-190437**
08.10.2004 JP 2004-296976

(45) Fecha de publicación de la mención BOPI:
22.12.2009

(45) Fecha de la publicación del folleto de la patente:
22.12.2009

(73) Titular/es: **FUJITSU LIMITED**
1-1, Kamikodanaka 4-chome
Nakahara-ku, Kawasaki-shi
Kanagawa 211-8588, JP
Fujitsu Frontech Limited

(72) Inventor/es: **Kamata, Hideo;**
Kishino, Takumi y
Eguchi, Shinichi

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Sistema de autenticación biométrica y método de registro.

Esta invención se refiere a un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos, que usan las características de una porción del cuerpo humano para realizar autenticación individual, y se refiere en particular a un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos, que detectan las características de la palma de una mano por medios sin contacto para adquirir información biométrica.

Hay numerosas porciones del cuerpo humano, tal como las huellas dactilares y las huellas de los dedos del pie, las retinas de los ojos, características faciales, y los vasos sanguíneos, que permiten la discriminación de individuos. Con los avances logrados en biometría en los últimos años, se han propuesto varios dispositivos para la autenticación de individuos identificando características biométricas de dichas porciones del cuerpo humano.

Por ejemplo, los vasos sanguíneos de la palma y dedos, y las huellas de las palmas y las huellas dactilares, proporcionan una cantidad comparativamente grande de datos individuales característicos, y así son adecuados para verificar fiablemente a un individuo (autenticación). En particular, 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 adecuadas para autenticación individual. Las figuras 18 a 21 explican técnicas convencionales de autenticación de la palma. Como se representa en la figura 18, al tiempo del registro o la autenticación, el usuario pone la palma de la mano 110 cerca de un dispositivo de captura de imagen 100. El dispositivo de captura de imagen 100 emite rayos infrarrojos cercanos, que son incidentes sobre la palma de la mano 110. El dispositivo de captura de imagen 100 usa un sensor para capturar rayos infrarrojos cercanos que rebotan de la palma de la mano 110.

Como se representa en la figura 19, la hemoglobina de los corpúsculos rojos que fluyen en las venas 112 ha perdido oxígeno. Esta hemoglobina (hemoglobina reducida) absorbe rayos infrarrojos cercanos a longitudes de onda cerca de 760 nanómetros. En consecuencia cuando los rayos infrarrojos cercanos se hacen incidentes en la palma de una mano, se reduce la reflexión solamente en las zonas en que hay venas, y la intensidad de los rayos infrarrojos cercanos reflejados puede ser usada para identificar las posiciones de las venas.

Para empezar, el usuario usa en primer lugar el dispositivo de captura de imagen 100 de la figura 18 para registrar datos de imagen de las venas de la palma de su propia mano en un servidor o en una tarjeta. Entonces, para identificarse (autenticarse) posteriormente, el usuario emplea el dispositivo de captura de imagen 100 de la figura 18 para leer los datos de imagen de las venas de su propia mano.

El usuario es autenticado comparando las configuraciones de las venas en la imagen de venas registrada recuperada usando la ID del usuario y en la imagen de verificación de venas así leída. Por ejemplo, al comparar las configuraciones de las venas en la imagen registrada y una imagen de verificación como en la figura 20, el usuario es autenticado como el individuo en cuestión. Por otra parte, después de la comparación de las configuraciones de las venas en una imagen registrada y en una imagen de verificación como en la figura 21, el individuo no es autenticado (véase por ejemplo la Publicación de Patente japonesa número 2004-062826).

En dicha detección sin contacto de información biométrica, la parte del cuerpo se puede mover libremente con respecto al dispositivo de captura de imagen 100, y en particular la mano se puede mover libremente. Por otra parte, con el fin de realizar una detección exacta, la parte del cuerpo para detección 110 se debe colocar dentro del rango de captura de imagen del dispositivo de captura de imagen 100. Para lograrlo, se han propuesto métodos en los que la posición y orientación de la mano son detectadas a partir de una imagen capturada, y cuando no es posible la captura de imagen exacta, se emplea una salida visual o de voz para comunicar la impropiedad de la posición u orientación de la mano (véase por ejemplo WO04/021884). En este método propuesto, una imagen de toda la mano es capturada y comparada con la forma media registrada de la mano para detectar la posición y orientación de la mano.

En el registro de dicha información biométrica, se han propuesto métodos en los que, al registrar datos de huellas dactilares, los datos de huellas dactilares son detectados varias veces y los datos de características comunes son extraídos de la pluralidad de conjuntos de datos de huellas dactilares, y estos datos de características comunes son registrados (véase por ejemplo la Publicación de Patente japonesa número 01-263775 y la Publicación de Patente japonesa número 11-232459). Mediante tales métodos se puede evitar el efecto que en los datos registrados produce el ruido de detección y los cambios de la forma de las huellas dactilares debido a diferencias en la presión de los dedos.

En tal detección sin contacto de información biométrica, la detección se lleva a cabo por medios sin contacto, y además, la parte del cuerpo, y en particular la mano, se puede mover libremente. Por otra parte, con el fin de realizar una autenticación biométrica rápida, es necesario que la captura de imagen se lleve a cabo frecuentemente, y que las imágenes apropiadas sean detectadas y enviadas al proceso de registro/autenticación. Por lo tanto, en los métodos que comparan las imágenes de toda la mano, se necesita tiempo para detectar la posición y orientación de la mano, y además se incrementa el tamaño del sensor en el dispositivo de captura de imagen, haciendo que tales métodos sean inadecuados cuando se demanda detección rápida o equipo de tamaño pequeño.

Además, en los métodos convencionales en los que se extraen y registran características comunes, se puede excluir el ruido debido al dispositivo de detección biométrica y las diferencias en los estados de detección al tiempo de la detección biométrica. Pero al registrar datos comunes, existe la posibilidad de que un conjunto de datos de características biométricas individuales del usuario obtenidos para verificación no concuerden exactamente con sus datos registrados, y que la cantidad de datos registrados difiera de (por ejemplo, sea menor que) la cantidad de datos de detección de características. Por lo tanto, al comparar los datos de verificación con datos registrados al tiempo de la autenticación, puede ser difícil realizar la verificación con alta exactitud.

Además, dado que los datos reales son datos biométricos, también hay que tomar en cuenta los cambios del estado físico. Y al registrar datos comunes, si hay diferencias en el estado físico al tiempo de la autenticación y al tiempo del registro, incluso cuando el individuo es el mismo, la autenticación como el mismo individuo puede no ser posible, de modo que pueden surgir problemas. Por ejemplo, en la autenticación usando configuraciones de las venas, hay numerosos factores que dan lugar a fluctuaciones, entre ellos la tasa de pulsos, el tiempo de captura de imagen, y la manera en que se presenta la mano.

Por lo tanto, hay impedimentos para la aplicación a equipo en general para uso en cualquier tiempo, en cualquier lugar, por cualquier persona. Pero si las tasas de verificación no son satisfactorias, y surgen problemas por razones biométricas, se impide la amplia adopción tanto por parte de los usuarios como de los fabricantes de equipos.

WO 2004/021884 describe un dispositivo de identificación individual para formación de imágenes de vasos sanguíneos, incluyendo el dispositivo medios de guía para ayudar al usuario a colocar la mano.

"Biometric Template Selection: A Case Study in Fingerprints", Jain y colaboradores, describe obtener datos conjuntos que tienen semejanza.

US 2002/0048014 describe un sistema para obtener una configuración de las venas de un dedo.

Por lo tanto, es deseable proporcionar un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos para extraer rápidamente datos de características incluso al usar captura de imagen sin contacto de una parte del cuerpo (por ejemplo la palma de la mano).

También es deseable proporcionar un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos, para obtener datos de características exactos, incluso cuando el dispositivo de captura de imagen sin contacto es de tamaño reducido.

También es deseable proporcionar un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos, para utilizar efectivamente una pluralidad de conjuntos de datos de características obtenidos por captura de imagen con un dispositivo de captura de imagen sin contacto, para mejorar la exactitud de la verificación.

También es deseable proporcionar un método de registro para un sistema de autenticación biométrica, un sistema de autenticación biométrica, y un programa para los mismos, para evitar las reducciones de la exactitud de la verificación, incluso cuando hay cambios en el dispositivo de captura de imagen, cambios en condición de la parte del cuerpo, y cambios en el estado de detección.

Un sistema de autenticación biométrica, un método y un programa según la invención se definen en las reivindicaciones anexas.

Además, se obtienen imágenes de la mano del mismo usuario varias veces de la unidad de captura de imagen, se determina el grado de semejanza mutua entre conjuntos de datos de características de una pluralidad de imágenes de la palma de la mano, y se registran múltiples conjuntos de datos de características con un alto grado de semejanza en una unidad de almacenamiento. Así, incluso cuando se usan datos de características detectados varias veces, se puede llevar a cabo una verificación que acomoda los cambios en el estado biométrico, sin disminuir la exactitud de la verificación, y además se puede evitar la incomodidad del usuario, contribuyendo a la adopción difundida del sistema de autenticación biométrica. Dado que la forma de la mano en imágenes se verifica usando los contornos (de la palma) de la mano en la imagen, es posible determinar rápidamente si una captura de imagen ha sido exitosa y extraer datos de características, e incluso usando dicho método, el procesado de registro se puede llevar a cabo en un período de tiempo corto.

Se hace referencia ahora, a modo de ejemplo solamente, a los dibujos acompañantes, donde:

La figura 1 representa la configuración de un sistema de autenticación biométrica de una realización de la invención.

La figura 2 es una vista exterior del dispositivo de captura de imagen de la palma de la figura 1.

La figura 3 es un diagrama de bloques funcionales del procesado de autenticación biométrica de la figura 1.

La figura 4 es un diagrama de bloques funcionales del procesado de registro de información biométrica de la figura 3.

La figura 5 explica el rango de captura de imagen del dispositivo de captura de imagen de la palma de la figura 2.

La figura 6 explica la imagen de vasos sanguíneos de la figura 4.

La figura 7 explica los datos de imagen de vasos sanguíneos de la figura 6.

La figura 8 explica datos registrados en la porción de almacenamiento en la figura 3.

La figura 9 representa el flujo del procesado de detección de distancia/contorno de la mano en la figura 3.

La figura 10 explica el procesado del contorno de la mano en la figura 9.

La figura 11 es un primer diagrama del flujo de procesado de registro en la figura 3.

La figura 12 es un segundo diagrama del flujo de procesado de registro en la figura 3.

La figura 13 explica la comparación de tres conjuntos de datos de imagen de vasos sanguíneos en la figura 11.

La figura 14 explica la comparación de cuatro conjuntos de datos de imagen de vasos sanguíneos en la figura 12.

La figura 15 es un diagrama de bloques funcionales de procesado de autenticación de prueba en otra realización de la invención.

La figura 16 representa el flujo del procesado de autenticación de prueba en la figura 15.

La figura 17 explica el procesado de verificación de la figura 15.

La figura 18 explica un dispositivo convencional de captura de imagen de la palma.

La figura 19 explica el principio de un dispositivo convencional de captura de imagen de la palma.

La figura 20 explica tecnología convencional de captura de imagen de la palma.

Y la figura 21 explica tecnología convencional de captura de imagen de la palma.

A continuación se explican realizaciones de la invención, en el orden de un sistema de autenticación biométrica, método de procesado de registro de datos biométricos, procesado de detección de distancia/contorno de la mano, método de procesado de registro de datos de características biométricas, procesado de autenticación de prueba y de autenticación, y otras realizaciones.

Sistema de autenticación biométrica

La figura 1 representa la configuración de un sistema de autenticación biométrica de una realización de la invención; la figura 2 es una vista exterior del dispositivo de captura de imagen de la palma de la figura 1; y la figura 3 explica el procesado de autenticación biométrica de la figura 1.

Como un sistema de autenticación biométrica, la figura 1 representa un ejemplo de un sistema de autenticación de venas de la palma en una institución financiera. Un dispositivo de captura de imagen de la palma 1 explicado en la figura 2, y un terminal de oficina sucursal (por ejemplo, un ordenador personal) 3 conectado al dispositivo de captura de imagen 1, están dispuestos en una zona de servicio 2 de la institución financiera. Un usuario que pide autenticación por configuración de las venas pone la mano sobre el dispositivo de captura de imagen de la palma (a continuación el "dispositivo de captura de imagen") 1. Como se representa en la figura 3, el dispositivo de captura de imagen 1 lee la palma, y el procesado de extracción de imagen de vasos sanguíneos 3a del terminal 3 extrae la configuración de las venas, y la registra como datos de venas en el terminal 3.

Estos datos de venas son registrados en una porción de almacenamiento 4a de un servidor de base de datos 4 conectado al terminal 3, o en un dispositivo de almacenamiento personal (por ejemplo, una tarjeta CI) 5 que lleva el usuario. El servidor 4 está conectado a un terminal de zona de servicio 8 en una zona de servicio 7 de la institución financiera, y el terminal de zona de servicio 8 está conectado a un dispositivo de captura de imagen 1.

Con el fin de hacer una extracción o realizar alguna otra transacción financiera en la zona de servicio 7 de la institución financiera, el usuario pone la mano sobre el dispositivo de captura de imagen 1 dispuesto en la zona de servicio 7. Como se representa en la figura 3, el dispositivo de captura de imagen 1 lee la palma de la mano, y la configuración de sus venas es extraída mediante procesado de extracción de imagen de vasos sanguíneos 8a por el terminal de zona de servicio 8. Mediante procesado de verificación 8b, el terminal de zona de servicio 8 verifica la

configuración de las venas, como datos de venas, contra los datos de venas registrados en el servidor de base de datos 4 para identificar (autenticar) al individuo.

El servidor 4 está conectado a un CA (cajero automático) 6 de la institución financiera, y el CA 6 puede ser usado para realizar transacciones mediante autenticación por configuración de las venas. Para utilizar el CA 6 para efectuar una extracción o realizar alguna otra transacción financiera, el usuario pone la mano sobre un dispositivo de captura de imagen 1-1 dispuesto en el CA 6. El dispositivo de captura de imagen 1-1 lee la palma. Al igual que el terminal de zona de servicio 8, el CA 6 extrae la configuración de las venas (imagen de vasos sanguíneos), y verifica esta configuración, como datos de venas, contra los datos de venas registrados en una tarjeta CI 5 que lleva el usuario o en el servidor de base de datos 4, para autenticar al individuo.

Como se representa en la figura 2, el dispositivo de captura de imagen de la palma 1 de la figura 1 está equipado con una unidad sensora 18 sustancialmente en el centro de una unidad principal 10. En una porción delantera (en el lado del usuario) de la unidad sensora 18 se ha dispuesto una guía delantera 14. La guía delantera 14 incluye una hoja de resina sintética, transparente o sustancialmente transparente.

La guía delantera 14 cumple la finalidad de guiar la mano del usuario sobre la unidad 18 y de soportar la muñeca. Por lo tanto, la guía delantera 14 proporciona guía al usuario con el fin de guiar la muñeca sobre la unidad sensora 18 y soporta la muñeca. Como resultado, se puede colocar 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 (rebaje) 14-2 de forma continua en el centro de la porción horizontal 14-1, para facilitar la colocación de la muñeca.

Como se indica a continuación en la figura 4, la unidad sensora 18 está provista de un sensor de infrarrojos (sensor CMOS) 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 12 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. Por lo tanto, la posición y la altura de la guía delantera 14 se establecen de tal manera que la muñeca soportada se coloque en la región legible V.

Procesado de registro de datos biométricos

La figura 4 es un diagrama de bloques del procesado de registro de información biométrica de una realización de la invención, la figura 5 explica la relación entre el rango de captura de imagen del dispositivo de captura de imagen y la palma de la mano, la figura 6 explica la imagen de vasos sanguíneos detectada en la figura 4, la figura 7 explica los datos de características biométricas de la figura 4, y la figura 8 explica los datos registrados.

Como se representa en la figura 4, el dispositivo de captura de imagen de la palma 1 de la figura 2 está equipado con una unidad sensora 18 sustancialmente en el centro de la unidad principal 10. Una guía delantera 14 está dispuesta en la porción delantera (hacia el usuario) de la unidad principal 10. La guía delantera 14 incluye una hoja de resina sintética, transparente o sustancialmente transparente.

La guía delantera 14 cumple la finalidad de guiar la mano del usuario en la parte delantera y de soportar la muñeca. Por lo tanto, la guía delantera 14 proporciona guía al usuario con el fin de guiar la muñeca sobre la unidad sensora 18 y soporta la muñeca. 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.

Además, la unidad sensora 18 está provista de un sensor de infrarrojos (sensor CMOS) y una 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 12 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 configuración del sensor, la lente de enfoque, y la región de emisión de luz infrarroja cercana. Por lo tanto, la posición y la altura de la guía delantera 14 se establecen de tal manera que la muñeca soportada se coloque en la región legible V.

Como se representa en la figura 5, cuando la mano 50 se extiende con la palma plana, la palma tiene una zona máxima, y además es plana, de modo que cuando la palma se somete a captura de imagen en la región de captura de imagen V de la unidad sensora 18, se obtiene una configuración exacta de las venas que puede ser usada en el registro y la verificación. Como se representa en la figura 6, cuando la distancia de la unidad sensora 18 a la palma está dentro de un rango preestablecido, el sensor 16 de la unidad sensora 18 obtiene una imagen nítida enfocada de los vasos sanguíneos.

Por lo tanto, como se representa en la figura 4, haciendo que la guía delantera 14 soporte la muñeca 52 encima de la unidad sensora 18, la posición, la inclinación y la altura de la palma encima de la unidad sensora 18 son exactas con respecto al rango de captura de imagen de la unidad sensora 18, y la mano del usuario puede ser guiada y soportada.

Volviendo a la figura 4, el terminal 3 conectado al dispositivo de captura de imagen 1 ejecuta una serie de procesado de registro 30 a 42. La porción de control del terminal 3 tiene, por ejemplo, una CPU, varios tipos de memoria, circuitería de interface, y otros circuitos necesarios para procesado de datos. La CPU ejecuta la serie de procesado de registro 30 a 42.

El procesado de detección de distancia/contorno de la mano 30 recibe la distancia del dispositivo de captura de imagen 1 medida por el sensor de distancia 15, determina si la palma u otro objeto está a una distancia dentro de un rango preestablecido de la unidad sensora 18. Y además el procesado de detección de contorno 30 detecta el contorno de la mano de la imagen capturada por la unidad sensora 18, y en base al contorno, determina si la imagen puede ser usada en procesado de registro y verificación. Por ejemplo, se determina si aparece una zona suficiente de la palma en la imagen. Este procesado se describe más adelante utilizando la figura 9.

Como se explica en la figura 9 siguiente, el procesado de salida de mensaje de guía 32 envía a la pantalla del terminal 3 un mensaje que guía la palma a la izquierda o la derecha, hacia delante o hacia atrás, hacia arriba o hacia abajo, cuando la distancia medida por el sensor de distancia 15 indica que la mano está fuera del rango de captura de imagen, y cuando la imagen no puede ser usada en el procesado de registro y verificación. Mediante esto, la mano del usuario es guiada a posición sobre el dispositivo de captura de imagen 1.

El procesado de extracción de imagen de vasos sanguíneos 34 extrae una imagen de las 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, como se explica con la figura 18 y la figura 20, se obtiene datos en escala de grises de la imagen de la palma, como los de la figura 7, mediante diferencias de reflectividad. La imagen de configuración de las venas es una imagen análoga a la representada en la figura 6; los datos son datos en escala de grises como los de la figura 7.

El procesado de mantenimiento temporal de imagen de vasos sanguíneos 36 mantiene temporalmente los datos de imagen de vasos sanguíneos extraídos. El procesado de determinación de registrabilidad 38 determina el grado de semejanza de una pluralidad de conjuntos de datos de imagen de vasos sanguíneos, con el fin de registrar una pluralidad de conjuntos óptimos de datos de imagen de vasos sanguíneos de entre la pluralidad de conjuntos de datos de imagen de vasos sanguíneos mantenidos por el procesado de mantenimiento temporal de imagen de vasos sanguíneos 36, para registrar los datos o no. El procesado de registro 42 registra datos de imagen de vasos sanguíneos que se determina que se han de registrar en una porción de almacenamiento 4a. El procesado de salida de progreso de registro 40 envía el estado de progreso de procesado de registro 42 a la pantalla del dispositivo terminal 3.

Así, para cada imagen capturada, no se obtienen necesariamente exactamente los mismos datos de características biométricas, y hay diferencias según el dispositivo de captura de imagen, el estado físico de la palma, la manera de extender la mano, y otros factores. Por lo tanto, la captura de imagen se lleva a cabo varias veces, y solamente se registra información óptima adecuada para el registro. Sin embargo, si la persona que llevase a cabo el registro (el usuario) tuviese que realizar docenas de operaciones de registro, la carga impuesta al usuario sería severa. En consecuencia, el número de operaciones se limita al número que probablemente será aceptable por parte de los usuarios, y la información de registro óptima se obtiene de esta información y se registra en la porción de almacenamiento 4a. Por ejemplo, como se representa en la figura 8, para cada ID individual se registran tres conjuntos de datos de características biométricas (datos de imagen de vasos sanguíneos de la palma de la mano).

Procesado de detección de distancia/contorno de la mano

La figura 9 representa el flujo de procesado de detección de distancia/contorno de la mano en la figura 4, y la figura 10 explica el procesado para determinar la idoneidad de las imágenes capturadas mediante el contorno de la mano.

(S10) El valor del contador de imágenes capturadas “n” se inicializa a “1”.

(S12) Se hace que el sensor de distancia 15 mida la distancia a la palma de la mano, y se detecta la salida.

(S14) Se comparan la distancia detectada y la longitud focal determinada por el sensor y la lente 16 de la unidad sensora 18, y se determina si la distancia a la palma está dentro del rango apropiado. El rango apropiado puede emplear, por ejemplo, un margen estrecho durante el registro, poniéndose la distancia de la unidad sensora 18 a entre 50 y 60 mm, mientras que durante la verificación, descrita más adelante, el margen puede ser mayor, siendo la distancia del sensor entre 40 y 70 mm. Mediante esto, se puede mejorar la velocidad de procesado de verificación manteniendo al mismo tiempo la exactitud de los datos de registro.

(S16) Si la distancia es apropiada, el dispositivo de captura de imagen 1 emite luz infrarroja cercana, y la luz reflejada es recibida por el sensor 16, para obtener una imagen de la palma de la mano.

(S18) El contorno de la palma de la mano es detectado a partir de la imagen capturada por el dispositivo de captura de imagen 1. Como se representa en la figura 5, con el fin de obtener una imagen de vasos sanguíneos de la palma, el rango de captura de imagen para la mano 50 se limita a V. El rango de captura de imagen V se pone al rango en que se capture una imagen de la palma de la mano, una porción de la muñeca, y las bases de los cinco dedos. Mediante esto, la unidad sensora 18 se puede hacer más pequeña. Cuando se captura una imagen con la mano abierta y en la posición correcta como en la figura 5, hay seis contornos dentro del rango de captura de imagen V, que son C1 (el borde izquierdo de la mano); C2 (entre los dedos); C3 (entre los dedos); C4 (entre los dedos); C5 (entre los dedos); y C6 (el borde derecho de la mano, que llega a la muñeca), como se representa en la figura 10.

(S20) A continuación, para determinar si la imagen es utilizable en el procesado de verificación basado en los contornos, en primer lugar se cuenta el número de contornos dentro del rango de captura de imagen (marco) V. Entonces se determina si el número de contornos contado es apropiado. Como se ha explicado anteriormente, cuando los dedos están extendidos y la muñeca está presente, el número de contornos detectado es "6", y la determinación es apropiada. Por otra parte, si el número de contornos detectado es "5" o menos, o los dedos no están extendidos o la posición de la palma está desplazada, o no se pueden detectar los dedos de la mano. Esta imagen se considera inapropiada, y el procesado pasa al paso S28.

(S22) Si el número de contornos es apropiado, entonces se calculan las distancias entre los contornos y el marco de imagen V, y a partir de las distancias se determina si hay desplazamiento hacia la derecha-izquierda o hacia delante-hacia atrás. Como se representa en la figura 10, se calcula la distancia L1 entre el borde izquierdo VL del marco y la posición izquierda del contorno C1, y se determina si la distancia calculada está dentro de un rango de distancia preestablecido, y si hay desplazamiento a la izquierda-derecha; si hay desplazamiento, el procesado pasa al paso S28.

(S24) A continuación, como se representa en la figura 10, se calcula la distancia L3 del borde inferior VU del marco y la posición inferior del contorno C6, y se determina si la distancia calculada está dentro de un rango de distancia preestablecido, y si hay desplazamiento hacia delante-hacia atrás; si hay desplazamiento, el procesado pasa al paso S28.

(S26) Si no hay desplazamiento hacia delante, porque los dedos están extendidos, la muñeca está presente, y no hay desplazamiento de posiciones en la imagen capturada, se determina que la captura de imagen es exitosa, y se obtiene la imagen para procesado de registro 34-38. Entonces tiene lugar retorno del procesado. En el procesado de registro, se toma la imagen dentro del marco de la línea de trazos R en la figura 10, y se lleva a cabo la detección de la imagen de vasos sanguíneos explicada en la figura 4.

(S28) Por otra parte, si en el paso S14 la distancia no es apropiada, o en los pasos S20 a S24 los dedos no están extendidos o se detecta un desplazamiento de posición, se determina si el valor del contador de imágenes capturadas "n" ha alcanzado un número predeterminado "m" (por ejemplo, 10 veces).

(S30) Si el valor del contador de imágenes capturadas "n" no ha alcanzado el número predeterminado "m"(por ejemplo, 10 veces), la causa de NB (fallo) de captura de imagen (dedos insuficientemente extendidos, desplazamiento a la izquierda-derecha/hacia delante-hacia atrás, desplazamiento de distancia) se (acumula) y guarda. El valor del contador de imágenes capturadas "n" se cambia entonces a "n+1", y el procesado vuelve al paso S12.

(S32) Por otra parte, si el valor del contador de imágenes capturadas "n" ha alcanzado el número predeterminado "m" (por ejemplo, 10 veces), se determina que la relación entre la palma y el sensor debe ser modificada. Por lo tanto, se analiza el número predeterminado m (por ejemplo, 10) de causas NB de captura de imagen. Por ejemplo, las causas se clasifican en insuficiente extensión de los dedos, posición desplazada (a la izquierda-derecha/hacia delante-hacia atrás), y distancia desplazada, y se cuenta cada una.

(S34) Los valores contados se usan para detectar la causa más frecuente de NB de captura de imagen. Cuando la insuficiente extensión de los dedos y la posición desplazada son las causas más frecuentes, se selecciona una pantalla de guía con texto para la extensión de los dedos y el desplazamiento de posición, y el procesado vuelve. Cuando los desplazamientos de distancia son las causas más frecuentes, se selecciona una pantalla de guía con texto para desplazamientos de distancia, y el procesado vuelve.

De esta forma, se limita el rango de captura de imagen, se extraen contornos en una imagen capturada, y los contornos se usan para determinar si la forma de la mano en la imagen capturada es apropiada, de modo que, en comparación con los métodos convencionales en los que se captura una imagen de toda la mano y se compara con una configuración básica de registro, se pueden obtener imágenes apropiadas de la palma mucho más rápidamente. Además, se puede reducir el tamaño de la unidad sensora.

Cuando la captura de imagen (incluyendo la medición de la distancia) se lleva a cabo varias veces a intervalos cortos, y NB de captura de imagen tiene lugar frecuentemente, se guardan para uso futuro, y si después de un número preestablecido de NB de capturas de imagen, el NB de captura de imagen no se ha resuelto, se determina que la posición relativa de la palma y el sensor debe ser corregida. Entonces se analiza el número predeterminado m (por ejemplo, 10) de causas de NB de captura de imagen guardadas, y se facilita una guía en pantalla acerca de la forma de extender la mano según los resultados del análisis.

Por lo tanto, la pantalla de guía no cambia frecuentemente, y así el usuario puede entender bien la causa del problema y puede cambiar la manera de extender la mano. Como resultado, se evita la confusión del usuario, la mano se puede mover rápidamente a una posición y distancia apropiadas, y se puede aumentar la velocidad de autenticación.

Además, se selecciona NB de captura de imagen más frecuencia, y se le indica al usuario la causa en una pantalla, de modo que se puedan evitar las causas NB (no buena) ocasionales de captura de imagen debidas al usuario, y la guía del usuario se puede llevar a cabo más fiablemente.

Método de procesado de registro de datos de características biométricas

La figura 11 y la figura 12 explican el flujo del procesado de registro de datos de características biométricas, y la figura 13 y la figura 14 explican este procesado. El flujo de procesado en la figura 11 y la figura 12 se explica con más detalle, con referencia a la figura 13 y la figura 14.

(S40) Como se ha explicado anteriormente, el dispositivo de captura de imagen 1 emite luz infrarroja cercana, para obtener una imagen de la palma de la mano (también llamada información biométrica).

(S42) Como se ha explicado anteriormente, por medio del procesado de detección del contorno de la mano 30 explicado en la figura 9, el contorno de la mano es detectado a partir de una imagen capturada por el dispositivo de captura de imagen 1, y a partir del contorno se determina si la imagen puede ser usada en el procesado de registro y verificación. Cuando la palma de la mano no aparece adecuadamente en la imagen o en casos similares, se lleva a cabo una determinación NB, el procesado de salida de mensaje de guía 32 descrito anteriormente envía a la pantalla del dispositivo terminal 3 un mensaje para dirigir la palma de la mano a la izquierda o derecha, o hacia delante o hacia atrás, y el procesado vuelve al paso S40.

(S44) Cuando el procesado de detección del contorno de la mano 30 determina que la captura de imagen tiene lugar con la mano extendida correctamente, el procesado de extracción de imagen de vasos sanguíneos 34 extrae de la imagen de la mano una imagen de las venas.

(S46) Se determina si la extracción es la primera extracción. Si es la primera extracción, la primera imagen de vasos sanguíneos se conserva temporalmente.

(S48) A continuación, se envía a la pantalla del dispositivo terminal 3 un mensaje de guía pidiendo la repetición de la operación, y el procesado vuelve al paso S40.

(S50) Por otra parte, si en el paso S46 la extracción no es la primera extracción, sino que se determina que es la segunda extracción o una posterior, se determina si la extracción es la segunda extracción.

(S52) Si la extracción es la segunda extracción, se compara el primer conjunto de datos de imagen de vasos sanguíneos con el segundo conjunto de datos de imagen de vasos sanguíneos, y se calcula el grado de semejanza. El grado de semejanza es una cantidad que indica el grado de coincidencia de las dos configuraciones de imagen de vasos sanguíneos; se puede aplicar varias técnicas de concordancia de configuración. Por ejemplo, en las dos matrices de píxeles de representación en escala de grises para las configuraciones de imagen de vasos sanguíneos en la figura 7, se obtienen y comparan los valores de píxel (valores de escala de grises) para un píxel de interés en las dos configuraciones. Si los dos coinciden, se incrementa en “1” un contador de grado de semejanza. El píxel de interés se cambia, y los valores de píxel se comparan igualmente para determinar la coincidencia del píxel nuevamente seleccionado. Si los dos coinciden, el contador de grado de semejanza se incrementa en “1”. Esto se lleva a cabo con respecto a todos los píxeles en las matrices de píxeles, y se considera que el valor del contador de grado de semejanza es el grado de semejanza. Si el grado de semejanza es igual o mayor que un umbral determinado con anterioridad, se determina que los dos son similares (OK), se determina que se registre el segundo conjunto de datos de imagen de vasos sanguíneos, se conserva temporalmente la segunda imagen de vasos sanguíneos en el paso S46, y el procesado pasa al paso S48. Por otra parte, si el grado de semejanza no excede del umbral, se determina que los dos no son similares (NB). El procesado pasa entonces al envío del mensaje de guía de repetición de operación del paso S48.

(S54) Por otra parte, si en el paso S50 la extracción no es la segunda, sino que es la extracción tercera o posterior, se determina si la extracción es la tercera extracción. Si no es la tercera extracción, el procesado pasa al paso S60 de la figura 12.

(S56) Por otra parte, si la extracción es la tercera extracción, entonces se calculan igualmente los grados de semejanza entre los datos de imagen de vasos sanguíneos extraídos hasta entonces (aquí, los conjuntos primero y segundo) y el tercer conjunto de datos de imagen de vasos sanguíneos. Es decir, como se representa en la figura 13, en el paso S42 se calcula el grado de semejanza #1 entre el segundo conjunto de datos de imagen de vasos sanguíneos y el primer conjunto de datos de imagen de vasos sanguíneos. En el paso S56 se calcula el grado de semejanza #3 entre el tercer conjunto de datos de imagen de vasos sanguíneos y el primer conjunto de datos de imagen de vasos sanguíneos, y el grado de semejanza #2 entre el tercer conjunto de datos de imagen de vasos sanguíneos y el segundo conjunto de datos de imagen de vasos sanguíneos, y se hacen las determinaciones. Si, como resultado de estas comparaciones, todos los grados de semejanza #1, #2 y #3 son iguales o mayores que el umbral, entonces se determina que los tres son imágenes de vasos sanguíneos similares. El procesado pasa entonces al paso S58 en la figura 12. Por otra parte, si

las comparaciones de la figura 13 indican que alguno de los grados de semejanza #1, #2, #3 no excede del umbral, el procesado vuelve al paso S48.

(S58) Se determina que se registre el tercer conjunto de datos de imagen de vasos sanguíneos. El procesado pasa entonces al paso S68.

(S60) Si, en el paso S54, la extracción no es la tercera extracción, entonces se determina si la extracción es la enésima extracción limitante (lectura final). Si lo es, entonces al operador se le muestra en la pantalla un mensaje de operación finalizada, y el procesado termina.

(S62) Si no es la enésima extracción limitante, entonces se llevan a cabo comparaciones con los n conjuntos de datos de imagen de vasos sanguíneos obtenidos hasta entonces. Por ejemplo, si la extracción es la cuarta extracción, entonces como se representa en la figura 14, se calculan el grado de semejanza #6 entre el cuarto conjunto de datos de imagen de vasos sanguíneos y el primer conjunto de datos de imagen de vasos sanguíneos, el grado de semejanza #5 entre el cuarto conjunto de datos de imagen de vasos sanguíneos y el segundo conjunto de datos de imagen de vasos sanguíneos, y el grado de semejanza #4 entre el cuarto conjunto de datos de imagen de vasos sanguíneos y el tercer conjunto de datos de imagen de vasos sanguíneos, y se llevan a cabo las determinaciones.

(S64) Si todos los grados de semejanza #4, #5, #6 son iguales o mayores que el umbral, se determina que las tres imágenes de vasos sanguíneos con grados de semejanza más altos entre los conjuntos primero, cuarto, segundo y tercero son similares, y el procesado pasa al paso S66. Por otra parte, si, en las comparaciones de la figura 14, se determina que alguno de los grados de semejanza #4, #5, #6 no excede del umbral, el procesado vuelve al paso S48 en la figura 11, y se capturan imágenes quinta y posteriores, se lleva a cabo extracción de imágenes de vasos sanguíneos, y se realizan igualmente los cálculos y determinaciones de grado de semejanza.

(S66) Se determina si el enésimo conjunto de datos de imagen de vasos sanguíneos está registrado.

(S68) Entonces se determina si se han obtenido tres conjuntos de datos de imagen de vasos sanguíneos que son similares y pueden ser registrados. Si no se obtuvieron, el procesado vuelve al paso S48. Si se obtuvieron, los tres conjuntos de datos de imagen de vasos sanguíneos son registrados en la porción de almacenamiento 4a, conjuntamente con una ID de usuario (número de cuenta o similar). Es decir, como se representa en la figura 8, en la porción de almacenamiento 4a se registran una ID individual y tres conjuntos de datos de imagen de vasos sanguíneos (aquí, la serie de valores de datos binarios blanco y negro) como los datos registrados de imagen de vasos sanguíneos de la porción de almacenamiento 4a.

Como se ha indicado en el paso S60, cuando tiene lugar de forma continua algún fenómeno incompatible con el registro, se incrementa la carga impuesta al usuario, y así se puede poner libremente un número N, y cuando se alcanza este número, se envía un mensaje indicando al usuario que repita las operaciones desde el inicio, o que consulte con el personal (por ejemplo, el cajero del banco).

De esta forma, los datos de imagen de vasos sanguíneos son detectados varias veces, y se registra una pluralidad (aquí, tres) de conjuntos de datos de imagen de vasos sanguíneos con alto grado de semejanza como los datos óptimos de imagen de vasos sanguíneos. En consecuencia, aunque haya diferencias en los datos biométricos debidas al dispositivo de captura de imagen, a cambios físicos de la palma, o a la manera de extender la mano u otros aspectos del estado de captura de imagen, dado que la captura de imagen se lleva a cabo varias veces y solamente se registra información biométrica óptima con un alto grado de semejanza adecuado para registro, se puede registrar una pluralidad de conjuntos de información biométrica que reflejen las diferencias, sin disminuir la exactitud de la verificación. Si la persona que realiza el registro (el usuario) estuviese obligado a realizar docenas de operaciones de registro, la carga impuesta al usuario sería excesiva, y por ello el número de operaciones se limita al número probablemente aceptable por parte de los usuarios, y a partir de esta información se obtiene la información de registro óptima y se registra en la porción de almacenamiento.

Aquí, los datos iniciales de imagen de vasos sanguíneos se usan como referencia al realizar el registro. De las configuraciones segunda y posteriores de imagen de vasos sanguíneos se registran dos conjuntos de datos de imagen de vasos sanguíneos con un alto grado de semejanza. Dado que los datos iniciales se usan como referencia, se puede evitar la continuación indefinida de los cálculos y determinaciones del grado de semejanza.

Procesado de autenticación de prueba y de autenticación

A continuación se explica la autenticación de prueba. Como se ha indicado anteriormente, cuando finaliza el registro de n (en la explicación anterior, 3) conjuntos de datos, la operación para realizar el proceso de verificación se lleva a cabo inmediatamente. Así, el usuario extiende la mano sobre el dispositivo para verificación, y los datos detectados y registrados son comparados para confirmar que es posible una autenticación fiable usando la palma del usuario. Como resultado, se incrementa la sensación de seguridad y fiabilidad del sistema por parte del usuario. La autenticación de prueba se realiza usando el mismo procedimiento que el de la autenticación real. Por lo tanto, la autenticación de prueba es también el procesado de autenticación real. El procesado se explica a continuación usando las figuras 15 a 17.

La figura 15 es un diagrama de bloques funcionales del procesado de autenticación en un aspecto de la invención, la figura 16 representa el flujo de procesado de autenticación en la figura 15, y la figura 17 explica la operación.

En la figura 15, las porciones que son las mismas que las de las figuras 2 y 4 se denotan con los mismos símbolos. Es decir, la CPU del dispositivo terminal 3 conectado al dispositivo de captura de imagen 1 ejecuta la serie de procesado de autenticación 30 a 46.

Como se ha explicado anteriormente usando la figura 9, el procesado de detección del contorno de la mano 30 detecta el contorno de la mano a partir de una imagen capturada por el dispositivo de captura de imagen 1, y a partir del contorno determina si la imagen puede ser usada en el procesado de registro y verificación. Por ejemplo, la palma de la mano puede aparecer adecuadamente o no en la imagen. El procesado de salida de mensaje de guía 32 envía a la pantalla del dispositivo terminal 3 un mensaje para guiar la palma de la mano hacia la izquierda, hacia la derecha, hacia delante o hacia atrás cuando la imagen no puede ser usada en el procesado de registro y verificación. Mediante esto, el usuario en el dispositivo terminal 3 es guiado al extender la mano del usuario sobre el dispositivo de captura de imagen 1.

Cuando el procesado de detección del contorno de la mano 30 determina que se ha capturado satisfactoriamente una imagen con la mano extendida correctamente, el procesado de extracción de imagen de la sangre 34 extrae una imagen de las venas de la imagen de la mano. Es decir, como se ha explicado usando la figura 18 y la figura 19, los datos en escala de grises de la imagen de la palma de la mano se obtienen de las diferencias de reflectividad, como en la figura 6.

Como se representa en la figura 8, el procesado de búsqueda de imagen de vasos sanguíneos registrada 46 busca en la porción de almacenamiento 4a tres conjuntos registrados de datos de imagen de vasos sanguíneos R1, R2, R3 correspondientes a la ID individual (número de cuenta). Como se representa en la figura 17, el procesado de verificación 44 compara los datos de imagen de vasos sanguíneos A detectados por el procesado de detección de imagen de vasos sanguíneos 34 con los tres conjuntos registrados de datos de imagen de vasos sanguíneos R1, R2, R3, realiza el procesado de verificación, y envía el resultado de la verificación.

Se ofrece una explicación más detallada utilizando la figura 16.

(S70) La ID (número de cuenta) presentada por el usuario se emplea para leer los tres conjuntos de datos de imagen de vasos sanguíneos R1, R2, R3 registrados correspondientes en la porción de almacenamiento 4a.

(S72) El dispositivo de captura de imagen 1 emite luz infrarroja cercana para obtener una imagen de la palma de la mano. Se lleva a cabo procesado de detección del contorno de la mano 30 para detectar el contorno de la mano de la imagen capturada por el dispositivo de captura de imagen 1, y el contorno se usa para determinar si la imagen puede ser usada en el procesado de verificación. Si la imagen de la palma no está colocada correctamente o surgen otros problemas, se devuelve una determinación NB, y se lleva a cabo el procesado de salida de mensaje de guía antes descrito 32 para enviar a la pantalla del dispositivo terminal 3 un mensaje que dirija la palma de la mano hacia la izquierda, hacia la derecha, hacia delante o hacia atrás. Cuando el procesado de detección del contorno de la mano 30 determina que se ha capturado una imagen con la mano extendida correctamente, el procesado de extracción de imagen de vasos sanguíneos 34 extrae una imagen de las venas de la imagen de la mano.

(S74) Se comparan el primer conjunto registrado de datos de imagen de vasos sanguíneos R1 y los datos de imagen de vasos sanguíneos extraídos A, y se calcula el grado de semejanza. El grado de semejanza es una cantidad que indica la extensión de coincidencia de las dos configuraciones de imagen de vasos sanguíneos; se puede aplicar varias técnicas de concordancia de configuración. Si el grado de semejanza es igual o mayor que un umbral determinado con anterioridad, se determina que los dos son similares (OK), la autenticación tiene éxito, y el procesado termina.

(S76) Por otra parte, si en el paso S74 el grado de semejanza no excede del umbral, se devuelve una determinación de no semejanza (NB). El segundo conjunto de datos de imagen de vasos sanguíneos registrado R2 se compara entonces con los datos de imagen de vasos sanguíneos extraídos A, y se calcula el grado de semejanza. Si el grado de semejanza es igual o mayor que un umbral determinado con anterioridad, se determina que los dos son similares (OK), la autenticación tiene éxito, y el procesado termina.

(S78) Por otra parte, si en el paso S76 el grado de semejanza no excede del umbral, se devuelve una determinación de no semejanza (NB). El tercer conjunto de datos de imagen de vasos sanguíneos registrado R3 se compara entonces con los datos de imagen de vasos sanguíneos extraídos A, y se calcula el grado de semejanza. Si el grado de semejanza es igual o mayor que un umbral determinado con anterioridad, se determina que los dos son similares (OK), la autenticación tiene éxito, y el procesado termina. Sin embargo, si el grado de semejanza no excede del umbral, se devuelve una determinación de no semejanza (NB), y el procesado termina con un error (es decir, el usuario no es autenticado).

En esta autenticación de prueba, como se representa en la figura 15, si el procesado de verificación no es satisfactorio, se puede ordenar al dispositivo de captura de imagen 1 que capture una nueva imagen. Por lo tanto, el usuario tiene más oportunidades de autenticación de prueba, y se puede acostumbrar al método de autenticación, contribuyendo a la amplia adopción del equipo de autenticación. Este procesado de autenticación es similar al procesado de autenticación real, y dado que una explicación sería redundante, se omiten detalles del procesado de autenticación

real. Naturalmente, se puede usar un criterio diferente del descrito anteriormente (mayor o igual a) para comparación del grado de semejanza con el umbral.

Otras realizaciones

En la realización anterior se explicó la autenticación biométrica para el caso de autenticación usando la configuración de las venas en la palma de la mano; pero es posible la aplicación a la autenticación biométrica empleando las huellas de las palmas u otras características de la mano, o de otras partes del cuerpo. Además, la explicación supuso operaciones financieras, pero es posible la aplicación a cualquier tarea que requiera verificación de la identidad de una persona.

Además, el cálculo de los grados de semejanza se explicó usando técnicas de comparación de configuraciones de mapas de bits; pero se pueden emplear métodos conocidos en los que se vectorizan datos, y las direcciones y longitudes de los vectores se usan también para calcular los grados de semejanza. Además, el número de registros no se limita a tres, sino que puede ser cualquier número superior a uno. El procesado de verificación (autenticación) se puede realizar con el mismo método que en las figuras 15 a 17, y puede ser ejecutado por el terminal de zona de servicio 8 o el CA 6 de la figura 1.

En lo que antecede, se han explicado realizaciones de la invención; pero la invención se puede modificar de varias formas dentro del alcance de las reivindicaciones, y estas modificaciones no quedan excluidas del alcance de la invención.

Dado que las imágenes de la palma de una mano del mismo cuerpo son capturadas varias veces por una unidad de captura de imagen, se calculan los grados de semejanza entre conjuntos de datos de características de la pluralidad de imágenes de la palma de la mano, y se registra una pluralidad de conjuntos de datos de características con un alto grado de semejanza en una unidad de almacenamiento, incluso al usar datos de características detectados varias veces, se puede realizar una verificación que tenga en cuenta los cambios en el estado biométrico leído sin disminuir la exactitud de la verificación, y así se puede mejorar la fiabilidad, dando seguridad al usuario y contribuyendo a la amplia adopción del sistema de autenticación biométrica. Además, dado que la forma de la mano en una imagen puede ser verificada usando contornos en la imagen de la palma de la mano, se puede determinar rápidamente si se ha capturado una imagen apropiada y se pueden extraer datos de características, de modo que el procesado de registro puede ser ejecutado en un período de tiempo corto.

REIVINDICACIONES

1. Un sistema de autenticación biométrica para uso al autenticar a un individuo detectando y registrando datos de características (R1, R2, R3) de una mano de un usuario, y posteriormente detectando datos de características (A) de la mano del usuario y verificando los datos de características detectados contra dichos datos de características registrados, incluyendo dicho sistema:

una unidad de captura de imagen (1) para capturar imágenes de la mano de dicho usuario; y

una unidad de almacenamiento (4a) para almacenar los datos de características registrados (R1, R2, R3) de la mano de dicho usuario; **caracterizado** por incluir además una unidad de procesado (3) para extraer segmentos de silueta (C1 ... C6) de una imagen de la mano capturada por dicha unidad de captura de imagen (1), obteniéndose los segmentos de silueta del contorno restringido de la palma de la mano en un rango de captura de imagen (V) de dicha unidad de captura de imagen (1), y para determinar a partir de dichos segmentos de silueta extraídos (C1 ... C6) si dicha imagen ha sido capturada satisfactoriamente, extraer dichos datos de características de la imagen si se determina que han sido capturados satisfactoriamente, y registrar dichos datos de características (R1, R2, R3) en dicha unidad de almacenamiento (4a),

donde dicha unidad de procesado (3) puede operar para obtener una pluralidad de imágenes de la mano de dicho usuario a partir de dicha unidad de captura de imagen (1), determinar el grado de semejanza entre datos de características entre cada una de dicha pluralidad de imágenes de la mano, y registrar en dicha unidad de almacenamiento (4a) una pluralidad de conjuntos de datos de características (R1, R2, R3) con un alto grado de semejanza de la pluralidad de imágenes;

donde dicha unidad de captura de imagen (1) puede operar para capturar una porción de una mano, en el rango de captura de imagen (V), incluyendo la palma de la mano de dicho usuario y una porción de los dedos, y donde dichos datos de características (R1, R2, R3) son datos de la palma de la mano; y

donde

dicha unidad de procesado (3) puede operar para determinar si dicha captura de imagen ha sido exitosa a partir del número de segmentos de silueta en una imagen de la palma de dicha mano dentro de dicho rango de captura de imagen (V).

2. El sistema de autenticación biométrica según la reivindicación 1, donde dicha unidad de procesado (3) puede operar para determinar el grado de semejanza de los conjuntos de datos de características segundo y posteriores (R2, R3) de la mano, con referencia al primer conjunto de datos de características (R1) de la mano.

3. El sistema de autenticación biométrica según la reivindicación 1 o 2, donde dicha unidad de procesado (3) puede operar para obtener imágenes de la mano de dicho mismo usuario a partir de dicha unidad de captura de imagen (1), hasta que se obtiene un número preestablecido de conjuntos de datos de características (R1, R2, R3) con un alto grado de semejanza.

4. El sistema de autenticación biométrica según cualquier reivindicación precedente, donde dicha unidad de procesado (3), después de registrar dicha pluralidad de conjuntos de datos de características (R1, R2, R3) con un alto grado de semejanza en dicha unidad de almacenamiento (4a), obtiene de dicha unidad de captura de imagen (1) una imagen de dicha mano, extrae dichos datos de características (A), verifica dichos datos de características (A) contra dicha pluralidad de conjuntos de datos de características (R1, R2, R3) registrados en dicha unidad de almacenamiento (4a), y así realiza una autenticación de prueba del usuario.

5. El sistema de autenticación biométrica según cualquier reivindicación precedente, donde dicha unidad de procesado (3) también realiza autenticación individual extrayendo segmentos de silueta (C1 ... C6) de una imagen de una mano de otro usuario capturada por dicha unidad de captura de imagen (1), determinando si dicha captura de imagen ha sido exitosa a partir de dichos segmentos de silueta extraídos, extrayendo datos de características (A) de la imagen si se determina que han sido capturados satisfactoriamente, verificando estos datos de características (A) contra dicha pluralidad de conjuntos de datos de características (R1, R2, R3) registrados en dicha unidad de almacenamiento (4a), y determinando si el otro usuario es el mismo que el usuario.

6. El sistema de autenticación biométrica según cualquier reivindicación precedente, donde dicha unidad de procesado (3) determina que el grado de semejanza es alto cuando dicho grado de semejanza es igual o mayor que un umbral preestablecido.

7. El sistema de autenticación biométrica según cualquier reivindicación precedente, donde dicha unidad de procesado (3) registra el primer conjunto de datos de características biométricas (R1), y para un enésimo conjunto de datos de características biométricas, calcula todos los grados de semejanza con los conjuntos de datos de características primero a (n-1)-ésimo, y cuando todos los grados de semejanza son iguales o mayores que un umbral, registra dicho enésimo conjunto de datos de características biométricas en dicha unidad de almacenamiento (4a).

8. El sistema de autenticación biométrica según la reivindicación 5, donde, al tiempo de la autenticación individual, dicha unidad de procesado (3) lee dicha pluralidad de conjuntos de datos de características biométricas (R1, R2, R3) de dicha unidad de almacenamiento (4a) según información de identificación para el usuario, y verifica dichos datos de características (A) obtenidos de la imagen de la mano obtenida de dicha unidad de captura de imagen (1) contra dicha pluralidad de conjuntos de datos de características.

9. El sistema de autenticación biométrica según la reivindicación 8, donde dicha unidad de procesado (3) detecta el hecho de que dichos datos de características extraídos (A) son similares a uno de dicha pluralidad de conjuntos de datos de características registrados (R1, R2, R3), y así autentica al otro usuario como el usuario.

10. El sistema de autenticación biométrica según la reivindicación 1, donde dicha unidad de procesado (3) determina si dicha captura de imagen ha sido exitosa a partir de la relación posicional de los segmentos de silueta (C1 ... C6) de la imagen de la palma de dicha mano con el marco del rango de captura de imagen (V) de dicha unidad de captura de imagen (1) y a partir del número de dichos segmentos de silueta dentro de dicho rango de captura de imagen (V).

11. El sistema de autenticación biométrica según cualquier reivindicación precedente, donde dicha unidad de procesado (3), al determinar a partir de los segmentos de silueta (C1 ... C6) de una imagen de la mano que dicha captura de imagen no ha sido exitosa, hace que dicha unidad de captura de imagen (1) realice de nuevo captura de imagen de la mano, y obtiene una nueva imagen de la mano.

12. El sistema de autenticación biométrica según la reivindicación 5, o cualquiera de las reivindicaciones 6 a 11 en cuanto anexas a la reivindicación 5,

donde dicha unidad de captura de imagen (1) tiene un sensor de distancia (15) para medir la distancia entre dicha unidad de captura de imagen (1) y la mano,

y dicha unidad de procesado (3) obtiene la imagen de la mano de dicha unidad de captura de imagen (1) cuando la distancia medida por dicho sensor de distancia (15) está dentro de un rango preestablecido, y cambia dicho rango preestablecido dependiendo de si se están capturando imágenes para registro o para autenticación individual de un usuario.

13. Un método de registro para un sistema de autenticación biométrica para uso al autenticar a un individuo detectando y registrando datos de características (R1, R2, R3) de una mano de un usuario para uso futuro, y detectando posteriormente datos de características (A) de la mano del usuario y verificando los datos de características detectados contra dichos datos de características registrados, incluyendo el método el paso de:

obtener una imagen de la mano del usuario de una unidad de captura de imagen (1) que captura imágenes de la mano; **caracterizado** por incluir además

extraer segmentos de silueta (C1 ... C6) de la imagen de la mano, y determinar, a partir de dichos segmentos de silueta, si dicha captura de imagen ha sido exitosa, obteniéndose los segmentos de silueta del contorno restringido de la palma de la mano en un rango de captura de imagen (V) de dicha unidad de captura de imagen (1);

extraer los datos de características (R1, R2, R3) de una imagen de la mano cuya captura ha sido exitosa;

determinar el grado de semejanza entre una pluralidad de conjuntos de datos de características (R1, R2, R3) extraídos de una pluralidad de dichas imágenes capturadas; y

registrar una pluralidad de conjuntos de datos de características (R1, R2, R3) con un alto grado de semejanza en una unidad de almacenamiento (4a);

donde dicho paso de obtención de imagen incluye obtener, a partir del rango de captura de imagen (V) de dicha unidad de captura de imagen (1), una imagen capturada de una porción de la mano incluyendo la palma de la mano de dicho usuario y una porción de los dedos, y donde dichos datos de características (R1, R2, R3) son datos de la palma de la mano; y donde

dicho paso de determinar el éxito de dicha captura de imagen incluye determinar si dicha captura de imagen ha sido exitosa a partir del número de segmentos de silueta (C1 ... C6) en la imagen de la palma de dicha mano dentro de dicho rango de captura de imagen (V).

14. El método de registro para un sistema de autenticación biométrica según la reivindicación 13, donde dicho paso de determinar el grado de semejanza incluye determinar el grado de semejanza de los conjuntos de datos de características segundo y posteriores (R2, R3) de la mano con referencia al conjunto inicial de datos de características (R1) de la mano.

15. El método de registro para un sistema de autenticación biométrica según la reivindicación 13 o 14, incluyendo además un paso de obtener imágenes de la mano del mismo usuario de dicha unidad de captura de imagen (1), hasta

que se obtiene un número preestablecido de dichos conjuntos de datos de características (R1, R2, R3) con alto grado de semejanza.

16. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 15, incluyendo además los pasos de:

obtener una imagen de la mano de dicha unidad de captura de imagen (1), después de registrar una pluralidad de dichos conjuntos de datos de características (R1, R2, R3) con un alto grado de semejanza en dicha unidad de almacenamiento (4a);

extraer segmentos de silueta (C1 ... C6) de la imagen de la mano y determinar a partir de dichos segmentos de silueta si dicha captura de imagen ha sido exitosa;

extraer datos de características (A) de la imagen de la mano cuya captura ha sido exitosa; y

verificar dichos datos de características (A) contra la pluralidad de conjuntos de datos de características (R1, R2, R3) registrados en dicha unidad de almacenamiento (4a).

17. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 16, donde dicho paso de determinar el grado de semejanza incluye determinar que el grado de semejanza es alto cuando dicho grado de semejanza es igual a o mayor que un umbral preestablecido.

18. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 17, donde dicho paso de determinar el grado de semejanza incluye:

un paso de calcular, para un enésimo conjunto de datos de características biométricas, los grados de semejanza con todos los conjuntos de datos de características primero a (n-1)-ésimo; y

un paso de determinar que dicho enésimo conjunto de datos de características biométricas son datos de características adecuados para registro cuando todos los grados de semejanza son iguales o mayores que un umbral.

19. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 18, donde dicho paso de determinar el éxito de dicha captura de imagen incluye determinar si dicha captura de imagen ha sido exitosa a partir de la relación posicional entre los segmentos de silueta (C1 ... C6) de la imagen de la mano con el marco del rango de captura de imagen (V) de dicha unidad de captura de imagen (1), y a partir del número de dichos segmentos de silueta dentro de dicho rango de captura de imagen (V).

20. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 19, incluyendo además un paso de hacer que dicha unidad de captura de imagen (1) capture de nuevo una imagen de la mano, cuando dicho paso de determinación determina a partir de los segmentos de silueta (C1 ... C6) de la imagen de dicha mano que dicha captura de imagen no es exitosa.

21. El método de registro para un sistema de autenticación biométrica según cualquiera de las reivindicaciones 13 a 20, donde dicho paso de obtención de imagen incluye un paso de obtener una imagen de la mano de dicha unidad de captura de imagen (1) cuando la distancia medida por un sensor de distancia (15) que mide la distancia entre dicha unidad de captura de imagen y la mano está dentro de un rango preestablecido.

22. Un programa conteniendo código de programa que, cuando es ejecutado por un ordenador, hace que el ordenador ejecute el método según cualquiera de las reivindicaciones 13 a 21.

FIG. 1

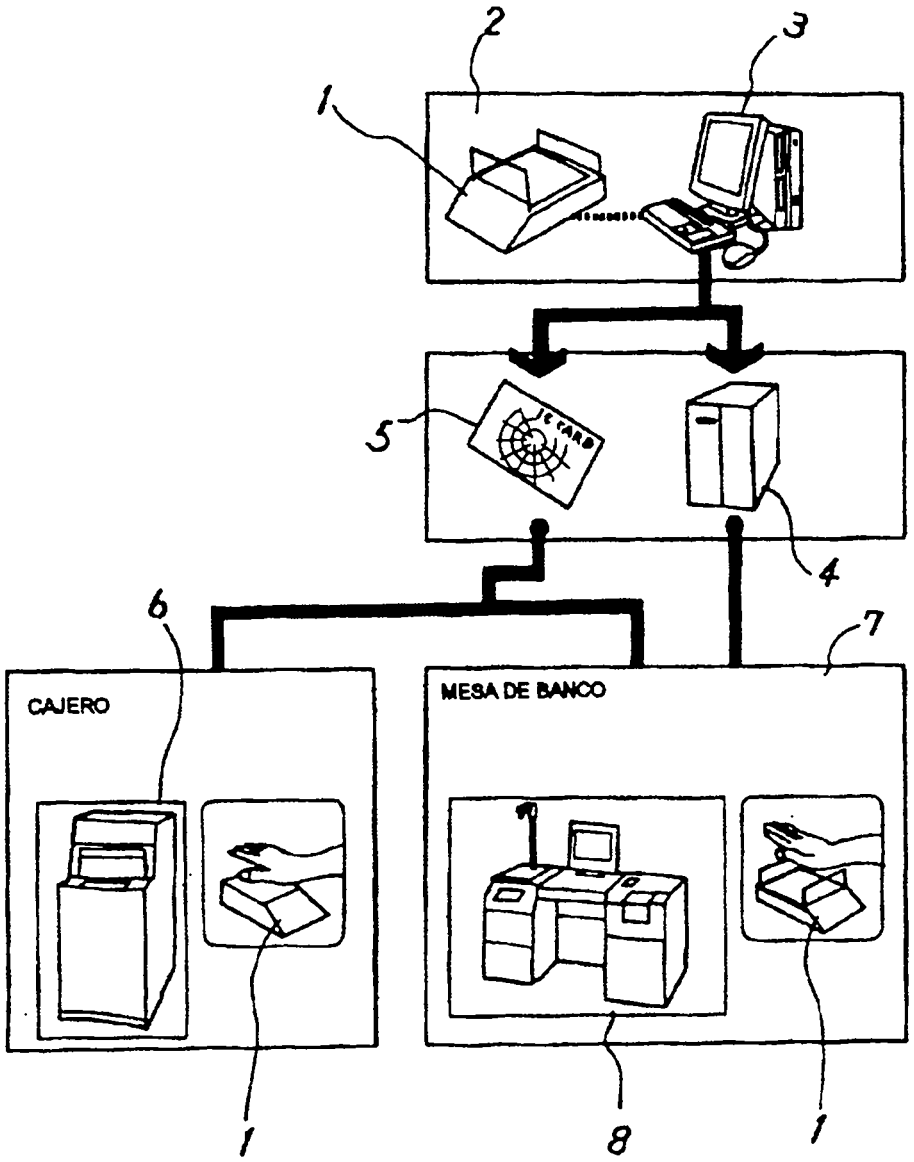


FIG. 2

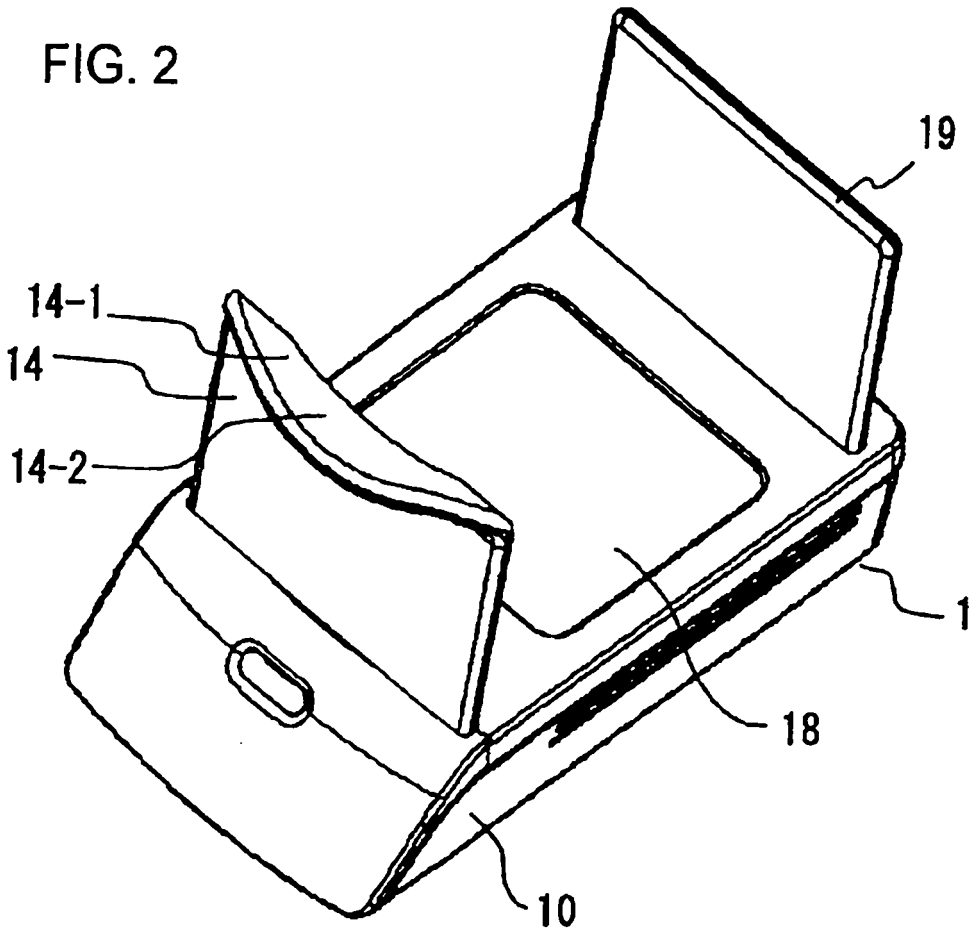


FIG.3

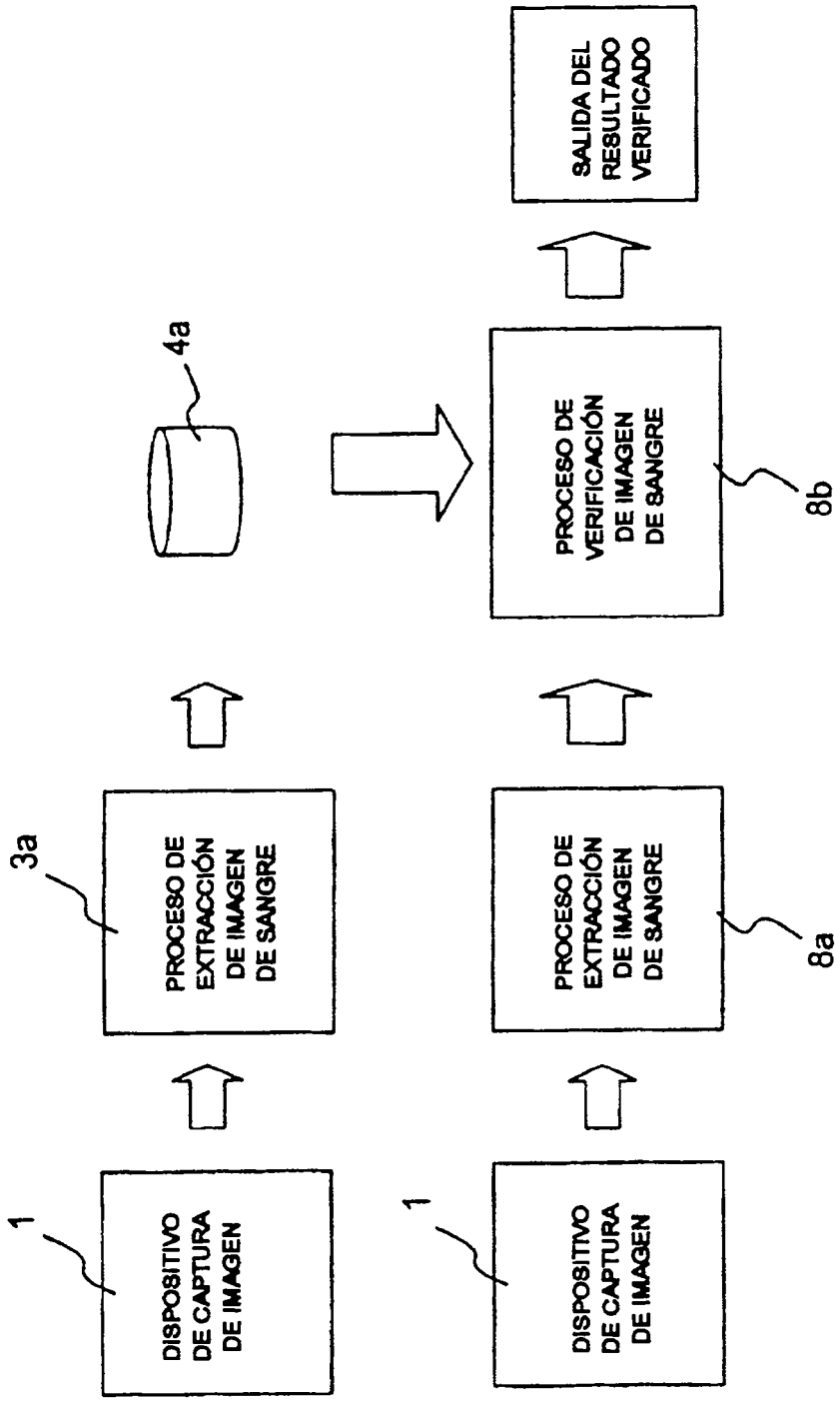

1
DISPOSITIVO DE CAPTURA DE IMAGEN
3a
PROCESO DE EXTRACCIÓN DE IMAGEN DE SANGRE
4a
1
DISPOSITIVO DE CAPTURA DE IMAGEN
PROCESO DE EXTRACCIÓN DE IMAGEN DE SANGRE
8a
PROCESO DE VERIFICACIÓN DE IMAGEN DE SANGRE
8b
SALIDA DEL RESULTADO VERIFICADO

FIG.4

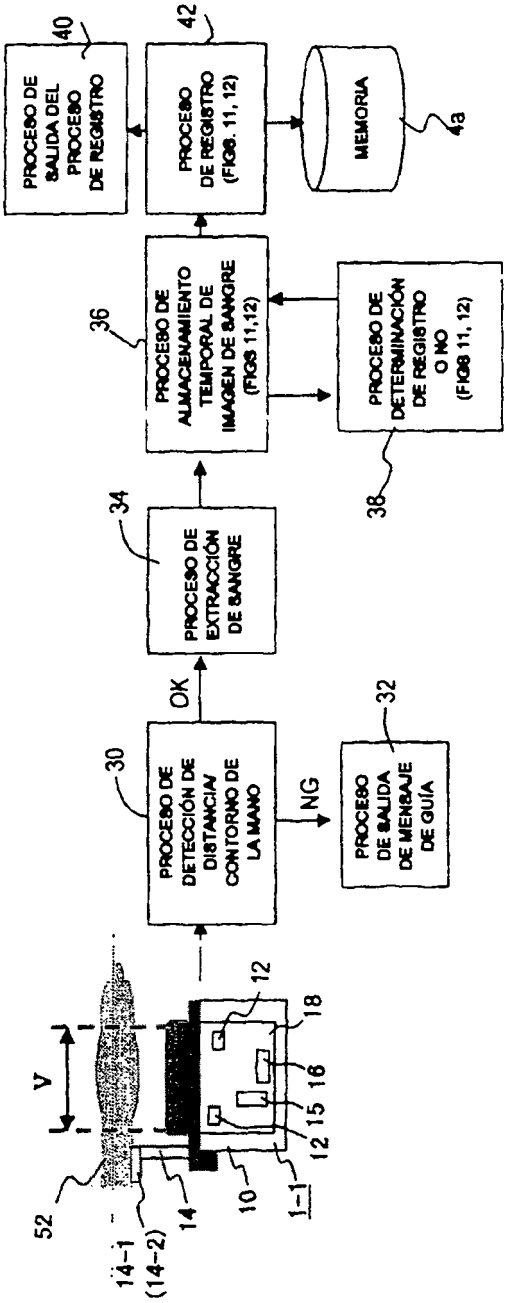

PROCESO DE SALIDA DEL PROCESO DE REGISTRO
40
PROCESO DE REGISTRO (FIGS. 11, 12)
42
MEMORIA
4a
PROCESO DE ALMACENAMIENTO TEMPORAL DE IMAGEN DE SANGRE (FIGS 11,12)
36
PROCESO DE DETERMINACIÓN DE REGISTRO O NO (FIGS 11, 12)
38
PROCESO DE EXTRACCIÓN DE SANGRE
34
OK
PROCESO DE DETECCIÓN DE DISTANCIA/ CONTORNO DE LA MANO
30
NG
PROCESO DE SALIDA DE MENSAJE DE GUÍA
32
V
12
18
16
15
12
1-1
10
14
52
14-i
(14-2)

FIG. 5

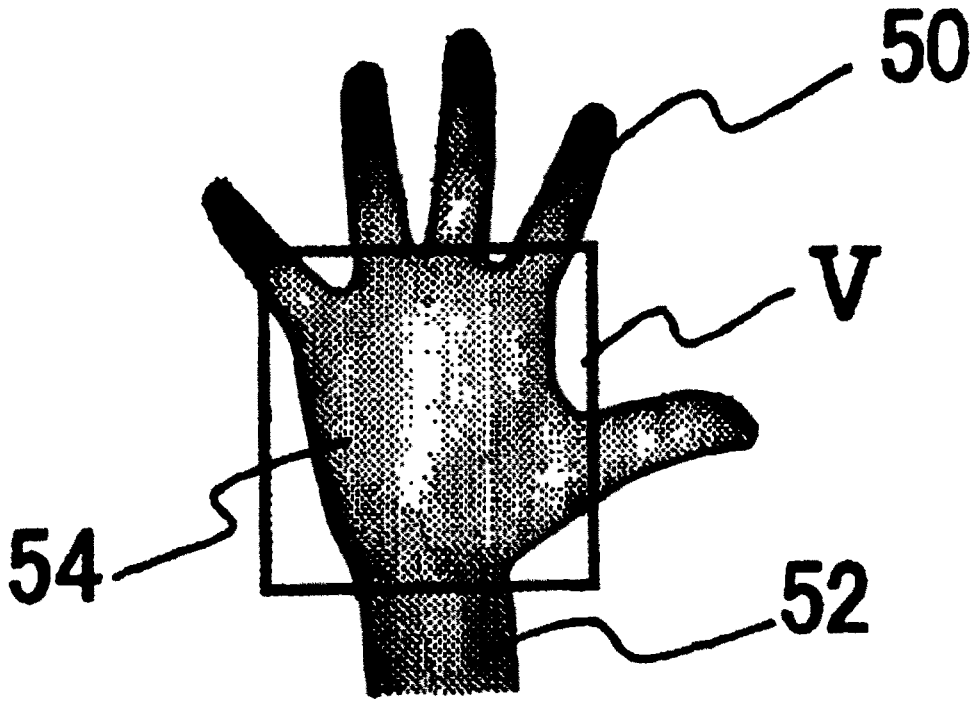


FIG. 6

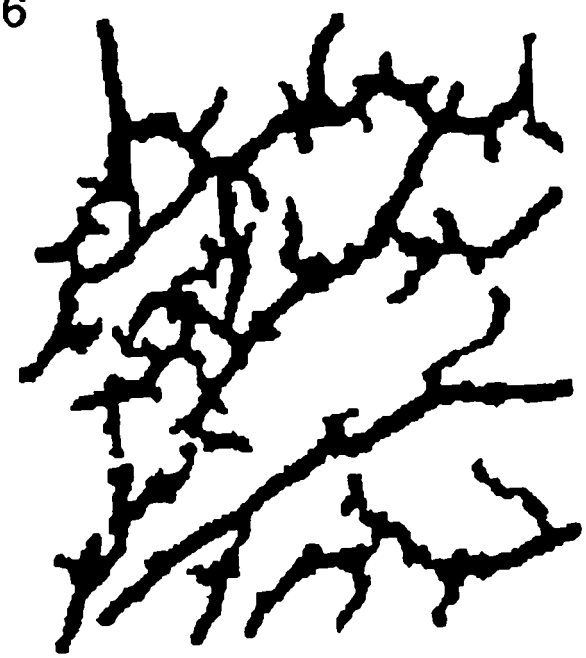


FIG. 7

IMAGEN DE VENA N1

	0	1	2	3	4
0	255	255	0	255	255
1	255	255	0	0	0
2	255	255	0	255	0
3	0	0	255	0	0
4	0	0	0	255	0

IMAGEN DE VENA N2

	0	1	2	3	4
0	255	255	0	0	255
1	255	255	255	0	0
2	255	255	0	255	255
3	0	0	255	255	0
4	0	0	0	255	255

FIG. 8

ID PERSONAL	DATOS DE CARACTERÍSTICAS BIOMÉTRICAS
0001	0, 0, 0, 1, 1, 1, 0, 0, 0,...
0001	0, 0, 0, 1, 1, 1, 1, 0, 0,...
0001	0, 0, 1, 1, 1, 1, 0, 0, 0,...
0002	0, 1, 1, 1, 1, 0, 0, 0, 0,...
0002	0, 1, 1, 1, 1, 1, 0, 0, 0,...,
0002	1, 1, 1, 1, 1, 0, 0, 0, 0,...
⋮	⋮
⋮	⋮
⋮	⋮

FIG.9

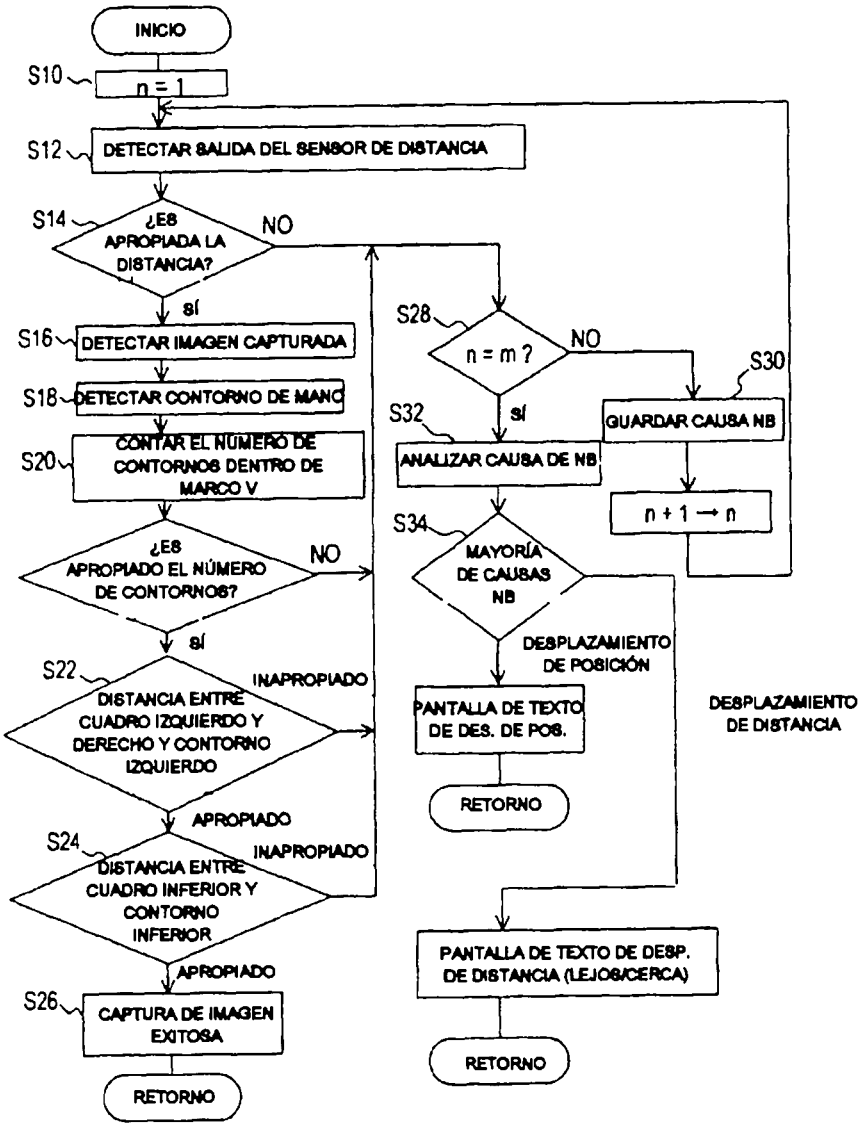
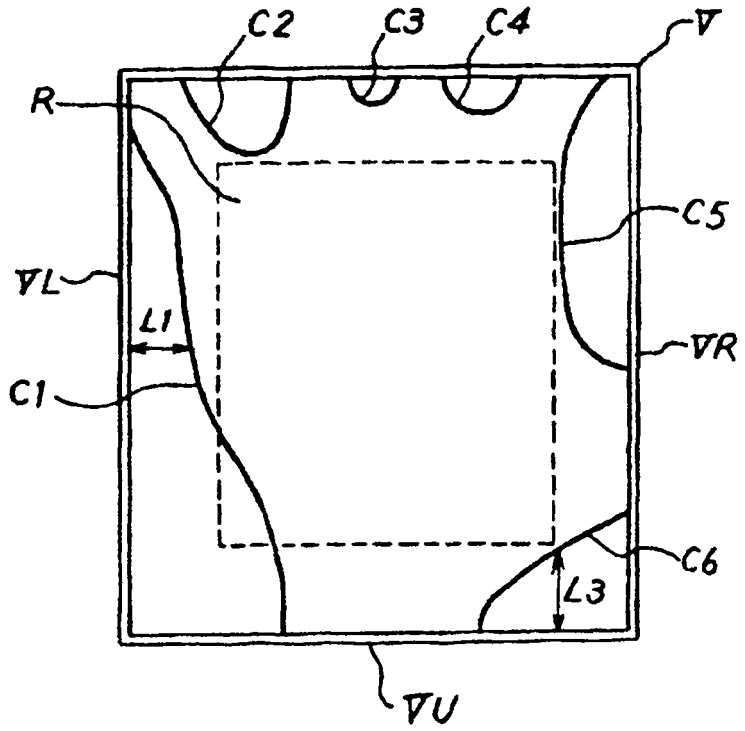

INICIO
S10
n = 1
S12
DETECTAR SALIDA DEL SENSOR DE DISTANCIA
S14
¿ES APROPIADA LA DISTANCIA?
NO
sí
S16
DETECTAR IMAGEN CAPTURADA
S18
DETECTAR CONTORNO DE MANO
S20
CONTAR EL NÚMERO DE CONTORNOS DENTRO DE MARCO V
¿ES APROPIADO EL NÚMERO DE CONTORNOS?
NO
sí
S22
DISTANCIA ENTRE CUADRO IZQUIERDO Y DERECHO Y CONTORNO IZQUIERDO
INAPROPIADO
APROPIADO
S24
DISTANCIA ENTRE CUADRO INFERIOR Y CONTORNO INFERIOR
INAPROPIADO
APROPIADO
S26
CAPTURA DE IMAGEN EXITOSA
RETORNO
S28
n = m ?
NO
sí
S30
GUARDAR CAUSA NB
n + 1 → n
S32
ANALIZAR CAUSA DE NB
S34
MAYORÍA DE CAUSAS NB
DESPLAZAMIENTO DE POSICIÓN
PANTALLA DE TEXTO DE DES. DE POS.
RETORNO
DESPLAZAMIENTO DE DISTANCIA
PANTALLA DE TEXTO DE DESP. DE DISTANCIA (LEJOS/CERCA)
RETORNO

FIG. 10



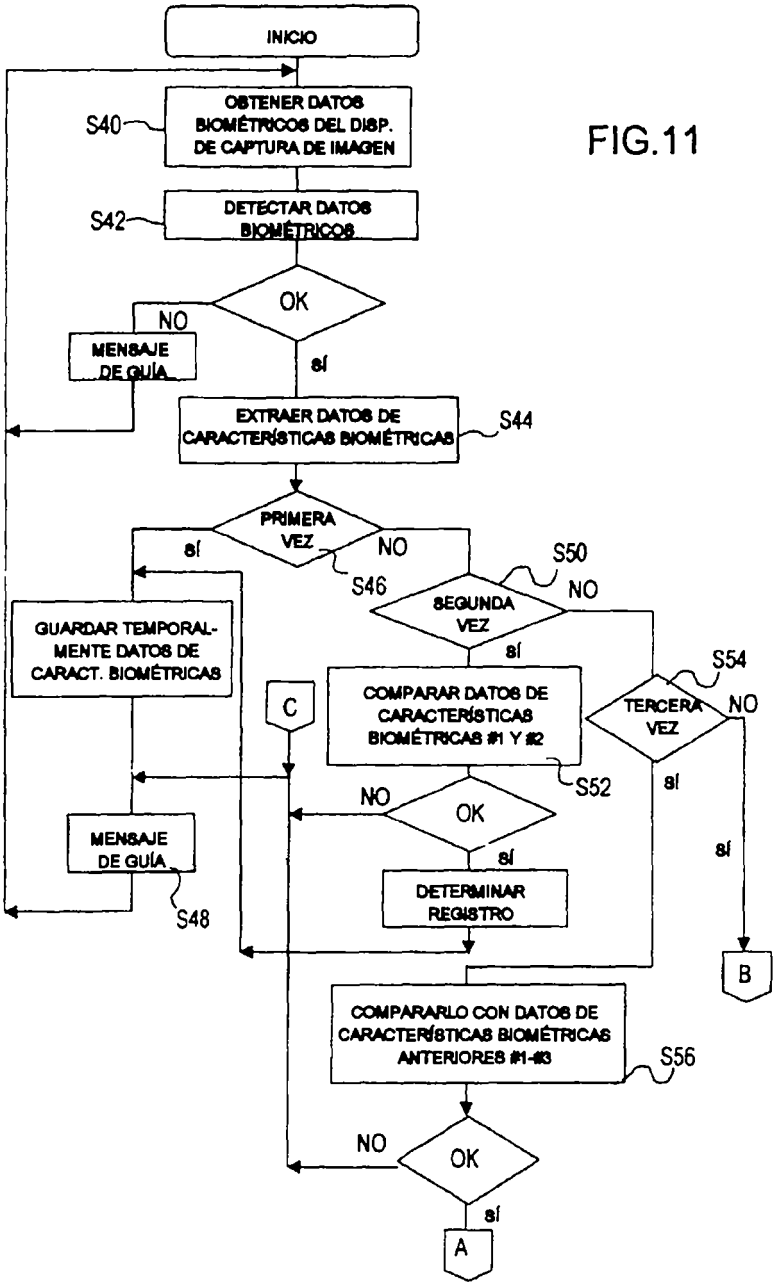

INICIO
OBTENER DATOS BIOMÉTRICOS DEL DISP. DE CAPTURA DE IMAGEN
S40
DETECTAR DATOS BIOMÉTRICOS
S42
OK
NO
MENSAJE DE GUÍA
sí
EXTRAER DATOS DE CARACTERÍSTICAS BIOMÉTRICAS
S44
PRIMERA VEZ
sí
NO
S46
S50
SEGUNDA VEZ
NO
sí
GUARDAR TEMPORAL-MENTE DATOS DE CARACT. BIOMÉTRICAS
C
COMPARAR DATOS DE CARACTERÍSTICAS BIOMÉTRICAS #1 Y #2
S52
S54
TERCERA VEZ
NO
sí
NO
OK
sí
MENSAJE DE GUÍA
S48
DETERMINAR REGISTRO
sí
B
COMPARARLO CON DATOS DE CARACTERÍSTICAS BIOMÉTRICAS ANTERIORES #1-#3
S56
NO
OK
sí
A

FIG.11

FIG.12

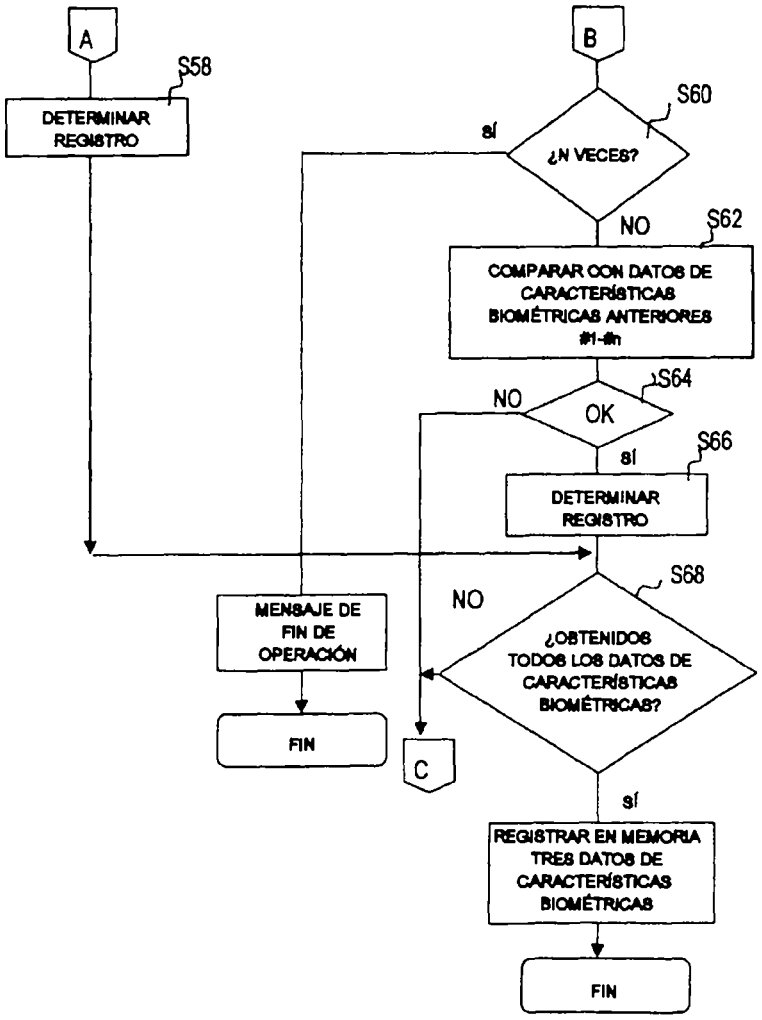

A
S58
DETERMINAR REGISTRO
B
S60
¿N VECES?
sí
NO
S62
COMPARAR CON DATOS DE CARACTERÍSTICAS BIOMÉTRICAS ANTERIORES #1-#n
S64
NO
OK
sí
S66
DETERMINAR REGISTRO
S68
NO
¿OBTENIDOS TODOS LOS DATOS DE CARACTERÍSTICAS BIOMÉTRICAS?
sí
MENSAJE DE FIN DE OPERACIÓN
FIN
C
REGISTRAR EN MEMORIA TRES DATOS DE CARACTERÍSTICAS BIOMÉTRICAS
FIN

FIG.13

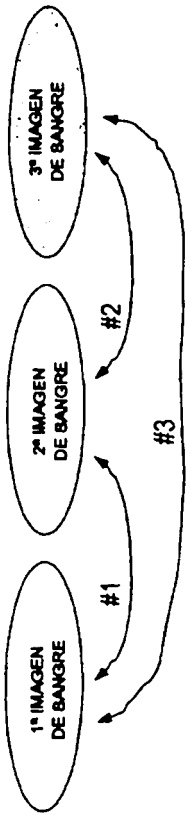

1ª IMAGEN DE SANGRE
2ª IMAGEN DE SANGRE
3ª IMAGEN DE SANGRE
#1
#2
#3

FIG.14

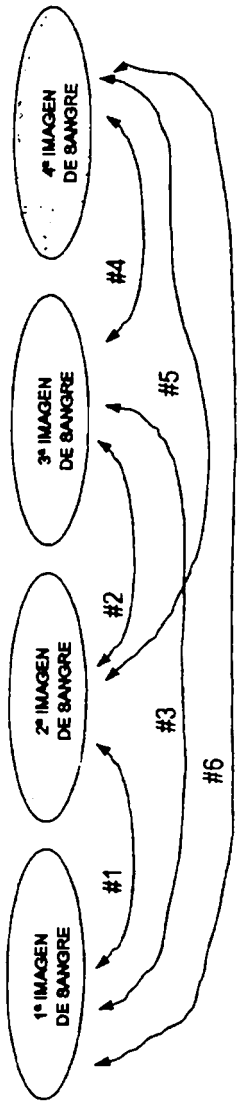
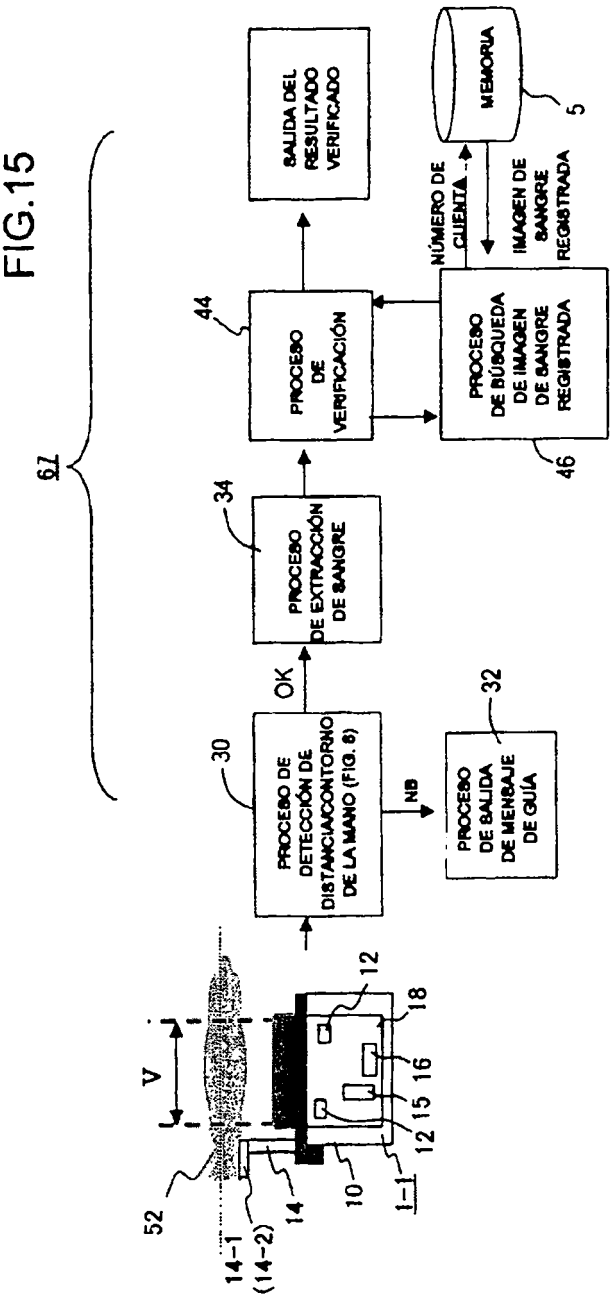

1ª IMAGEN DE SANGRE
2ª IMAGEN DE SANGRE
3ª IMAGEN DE SANGRE
4ª IMAGEN DE SANGRE
#1
#2
#3
#4
#5
#6

FIG.15


61
PROCESO DE DETECCIÓN DE DISTANCIA/CONTORNO DE LA MANO (FIG. 8)
30
OK
NB
PROCESO DE EXTRACCIÓN DE SANGRE
34
PROCESO DE VERIFICACIÓN
44
PROCESO DE BÚSQUEDA DE IMAGEN DE SANGRE REGISTRADA
46
PROCESO DE SALIDA DE MENSAJE DE GUÍA
32
SALIDA DEL RESULTADO VERIFICADO
MEMORIA
5
NÚMERO DE CUENTA
IMAGEN DE SANGRE REGISTRADA
V
52
14-1
(14-2)
14
10
1-1
12
15
16
18

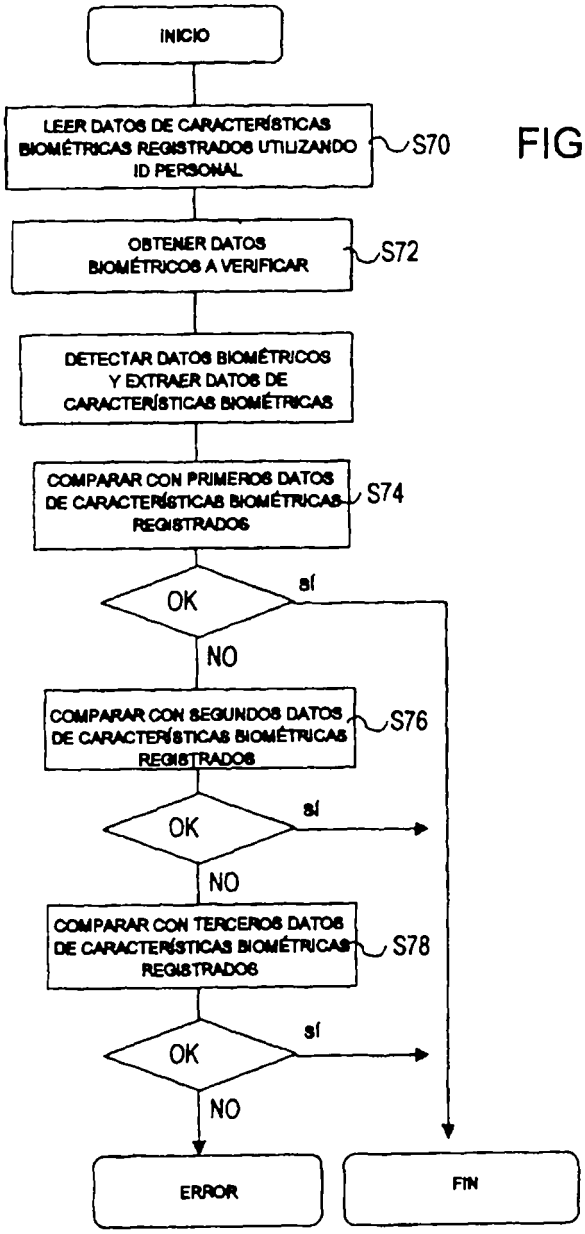

INICIO
LEER DATOS DE CARACTERÍSTICAS BIOMÉTRICAS REGISTRADOS UTILIZANDO ID PERSONAL
S70
OBTENER DATOS BIOMÉTRICOS A VERIFICAR
S72
DETECTAR DATOS BIOMÉTRICOS Y EXTRAER DATOS DE CARACTERÍSTICAS BIOMÉTRICAS
COMPARAR CON PRIMEROS DATOS DE CARACTERÍSTICAS BIOMÉTRICAS REGISTRADOS
S74
OK
sí
NO
COMPARAR CON SEGUNDOS DATOS DE CARACTERÍSTICAS BIOMÉTRICAS REGISTRADOS
S76
OK
sí
NO
COMPARAR CON TERCEROS DATOS DE CARACTERÍSTICAS BIOMÉTRICAS REGISTRADOS
S78
OK
sí
NO
ERROR
FIN

FIG.16

FIG. 17

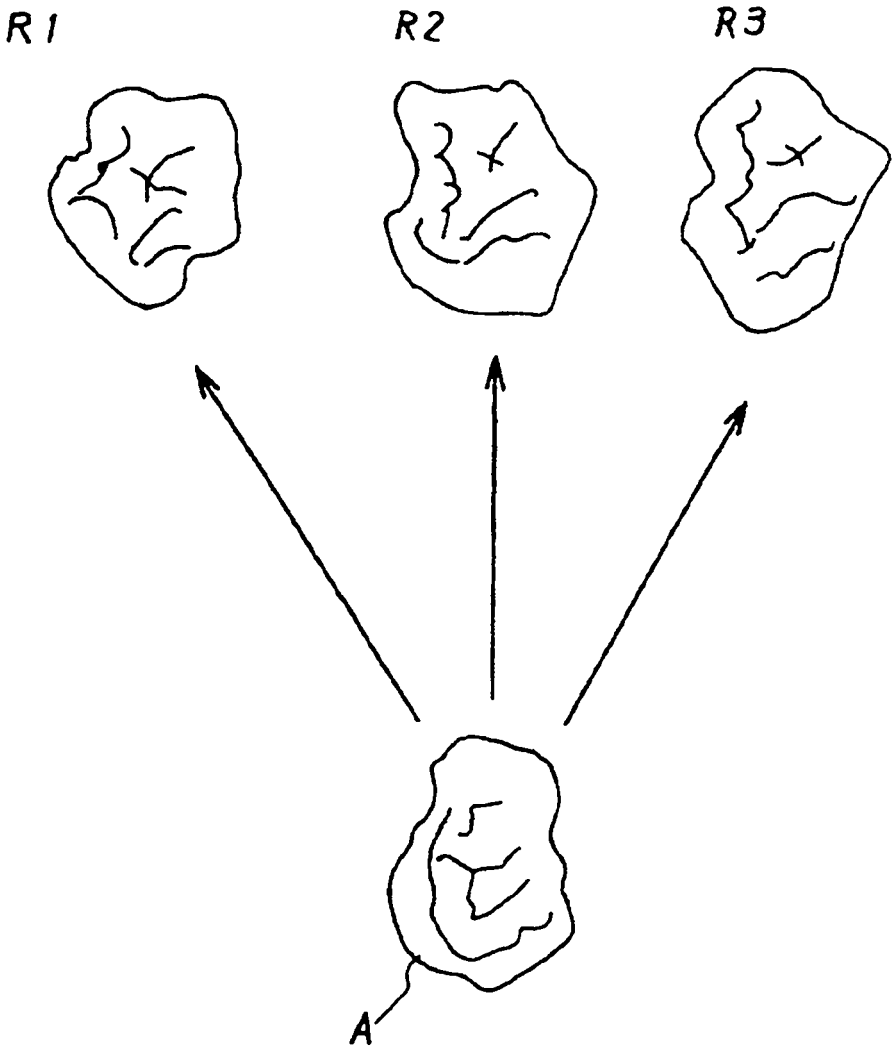


FIG. 18

TÉCNICA ANTERIOR

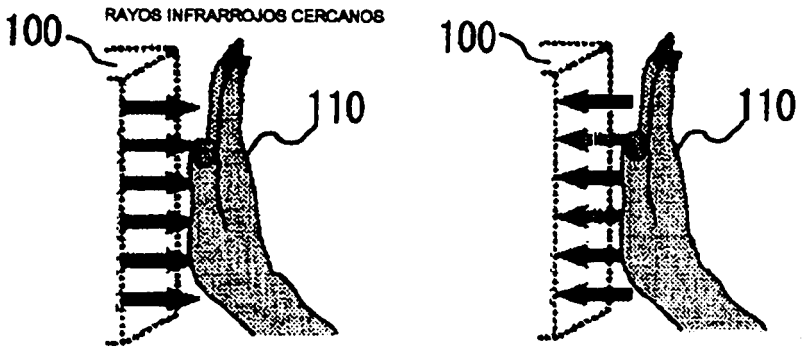
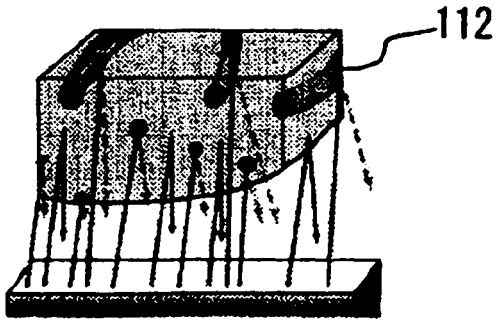


FIG. 19 TÉCNICA ANTERIOR



TÉCNICA ANTERIOR

FIG. 20

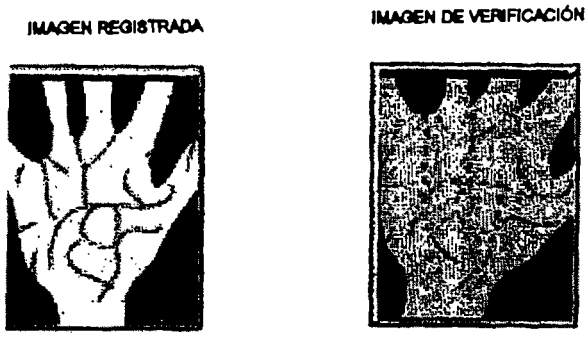


FIG. 21

TÉCNICA ANTERIOR