(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 977**

(51) Int. CI.:

G07C 9/00 (2006.01)
G06F 21/83 (2013.01)
G06F 21/32 (2013.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.08.2007 E 07113935 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2013 EP 1901194**

(54) Título: **Método de autenticación biométrica, medio para autenticación individual, y dispositivo de autenticación biométrica**

(30) Prioridad:

12.09.2006 JP 2006246443

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2013

(73) Titular/es:

FUJITSU LIMITED (50.0%)
1-1, KAMIKODANAKA 4-CHOME, NAKAHARA-KU KAWASAKI-SHI, KANAGAWA 211-8588, JP y
FUJITSU FRONTECH LIMITED (50.0%)

(72) Inventor/es:

TAKAKU, KAZUO;
MITA, YASUHIKO;
SUZUKI, NAOKO;
IWASAKI, SHINYA y
YANO, MASAYUKI

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Método de autenticación biométrica, medio para autenticación individual, y dispositivo de autenticación biométrica

Esta solicitud se basa y reivindica el beneficio de prioridad de la solicitud de patente japonesa anterior número 2006-246443, presentada el 12 de Septiembre de 2006.

Esta invención se refiere a un método de autenticación biométrica, un medio usado en autenticación individual, y un dispositivo de autenticación biométrica, para autenticación de un individuo utilizando características biométricas que son una porción del cuerpo humano. En particular esta invención se refiere a un método de autenticación biométrica, un medio para autenticación individual, y un dispositivo de autenticación biométrica que son adecuados para uso en la autenticación de un individuo verificando conjuntos de datos biométricos registrados contra un conjunto de datos biométricos detectados.

Recientemente, como una técnica para identificar o autenticar individuos, ha concitado atención el uso de biometría. Hay numerosas porciones del cuerpo humano que pueden ser usadas para diferenciar el individuo, tal como las huellas dactilares y las huellas de los dedos de los pies, las retinas de los ojos, los rasgos faciales y los vasos sanguíneos; en tales métodos, las características biométricas de tales porciones del cuerpo humano son identificadas para realizar autenticación de individuos.

Por ejemplo, se obtienen cantidades comparativamente grandes de unos datos característicos de los individuos a partir de los vasos sanguíneos de los dedos, las palmas, y el reverso de las manos. Además, las configuraciones de los vasos sanguíneos (venas) no cambian durante toda la vida desde la infancia y se consideran completamente únicas, y por ello ésta es una biométrica adecuada para la autenticación de individuos.

En dicha autenticación biométrica, una porción de las características biométricas del usuario es detectada en primer lugar por un aparato de detección, y los datos biométricos detectados son registrados en una tarjeta o en un servidor. A continuación, con el fin de realizar autenticación de un individuo, una porción de las características biométricas del usuario es detectada por un aparato de detección, los datos biométricos detectados son verificados contra los datos biométricos registrados, y la autenticación del individuo se lleva a cabo en base al grado de semejanza.

Si tales datos biométricos son registrados y almacenados en una posición, si los datos se filtrasen a una parte exterior, existe la posibilidad de que la totalidad de los datos biométricos puedan ser copiados o de que pueda tener lugar alguna falsificación o análogos, dando lugar a un uso ilícito. Por lo tanto, se ha propuesto un método de almacenamiento distribuido, en el que los datos biométricos son divididos y las porciones divididas son almacenadas en medios diferentes.

Por ejemplo, se ha propuesto un método en el que se divide la información biométrica relativa a una persona registrada, almacenándose las respectivas porciones de información divididas en una tarjeta y en un dispositivo de autenticación, y al tiempo de la verificación los datos divididos son leídos y combinados para obtener los datos biométricos registrados (véase por ejemplo, la Publicación de Patente japonesa número 2001-067137 y la Publicación de Patente japonesa número 2002-351843). Se ha propuesto otro método en el que cada una de las porciones de información biométrica divididas relativas a una persona registrada es almacenada en un centro de gestión de autenticación y en un terminal de usuario respectivamente, y al tiempo de la verificación los datos divididos son leídos y combinados para obtener los datos biométricos registrados (véase por ejemplo, la Publicación de Patente japonesa número 2005-122478).

GB 2397419 describe un método de identificación que incluye los pasos de introducir elementos de información biométrica primero y segundo, comparar datos representativos del primer elemento de información biométrica con datos almacenados mantenidos en una primera memoria de datos, comparar datos representativos del segundo elemento de información biométrica con datos almacenados mantenidos en una segunda memoria de datos, y operar un dispositivo usando los resultados de las dos comparaciones.

WO 2005/098742 describe un método y aparato para autenticar una identificación de una persona, donde se obtiene información biométrica de la persona y una porción de la misma es extraída y almacenada en un soporte de datos adaptado para ser llevado por la persona. Una porción restante de la información biométrica es almacenada en un sistema de identificación. Para la autenticación, la persona presenta el soporte de datos y se obtiene nueva información biométrica de la persona. Se lleva a cabo una comparación entre la nueva información biométrica de la persona, la porción de la información biométrica almacenada en el soporte de datos y la porción restante de la información biométrica almacenada en el sistema de identificación.

Cuando los datos biométricos son distribuidos (divididos) de esta forma, se necesita una clave para relacionar los datos divididos. Es decir, se usa una clave para asociar y para combinar los datos divididos para reproducir los datos registrados al tiempo de la verificación. En las propuestas de la técnica anterior descrita anteriormente se usa como clave un número de identificación encriptado (por ejemplo, un número de ID, número de contraseña o análogos) de

la persona registrada.

Sin embargo, aunque el número de identificación en la tecnología de la técnica anterior esté encriptado, el número puede ser desencriptado. Si el número de identificación es desencriptado, incluso cuando los datos han sido divididos con el fin de evitar el uso ilícito de la totalidad de los datos biométricos, los datos divididos correspondientes pueden ser recuperados y combinados fácilmente para reproducir la totalidad de los datos biométricos.

Además, los datos biométricos son información privada, y por ello, naturalmente, se debe evitar el acceso ilícito y naturalmente dicha adquisición ilícita. Por esta razón hay preocupación porque la seguridad de los dispositivos de autenticación biométrica usados por individuos se pueda poner en peligro, impidiendo la difusión de tales dispositivos; y por ello se necesitan más medidas para permitir el uso efectivo de la autenticación biométrica.

Por lo tanto, es deseable proporcionar un método de autenticación biométrica, un medio para autenticación individual, y un dispositivo de autenticación biométrica para evitar la adquisición ilícita y la combinación de información biométrica dividida incluso cuando la información biométrica esté distribuida (dividida y almacenada) en medios diferentes.

También es deseable proporcionar un método de autenticación biométrica, un medio para autenticación individual, y un dispositivo de autenticación biométrica para evitar la falsificación de información biométrica incluso cuando la información biométrica esté distribuida en medios diferentes.

Además, es deseable proporcionar un método de autenticación biométrica, un medio para autenticación individual, y un dispositivo de autenticación biométrica para evitar la adquisición ilícita de información biométrica mediante el robo del medio incluso cuando la información biométrica esté distribuida en medios diferentes.

Según un primer aspecto de la presente invención, se facilita un dispositivo de autenticación biométrica, que detecta características de un cuerpo de un usuario y realiza autenticación individual, incluyendo: un dispositivo de detección, que detecta una porción de interés de un cuerpo, y envía datos biométricos que indican una característica biométrica; un archivo de base de datos, dispuesto para almacenar una primera porción de datos biométricos de una pluralidad de porciones de datos resultantes de la división de datos biométricos del usuario detectados por el dispositivo de detección, para almacenar porciones de datos de una pluralidad de usuarios; un medio individual para almacenar una segunda porción de datos biométricos de la pluralidad de porciones de datos; y una unidad de control que, al tiempo de la autenticación usando el medio individual, combina la segunda porción de datos biométricos del medio individual con una primera porción de datos biométricos recuperados del archivo de base de datos, caracterizado porque el medio individual guarda una clave de información biométrica generada a partir de los datos biométricos, la unidad de control crea una clave de información biométrica a partir de los datos biométricos combinados, compara la clave de información biométrica leída del medio individual con la clave de información biométrica creada para determinar si la primera porción de datos biométricos recuperada está asociada con la segunda porción de datos biométricos del medio individual donde, cuando el resultado de la comparación es una falta de concordancia, la unidad de control está dispuesta para recuperar otra porción de datos biométricos del archivo de base de datos perteneciente a un usuario diferente, combinar la segunda porción de datos biométricos en el medio individual y la otra porción de datos biométricos recuperada del archivo de base de datos, y crear una clave de información biométrica a partir de los datos biométricos combinados, y cuando el resultado de la comparación es una concordancia, la unidad de control está dispuesta para verificar los datos biométricos combinados contra los datos biométricos obtenidos del dispositivo de detección, y realiza autenticación individual.

Según otro aspecto de la presente invención, se facilita un método de autenticación biométrica que consiste en detectar una característica biométrica de un usuario y realizar autenticación individual, incluyendo: un paso de registrar los datos biométricos de una pluralidad de usuarios; y un paso de verificar los datos biométricos de un usuario, donde el paso de registro incluye: un paso de detección que consiste en detectar una porción de interés del cuerpo del usuario, y enviar datos biométricos que indican las características biométricas; un paso de dividir los datos biométricos del usuario, detectados en el paso de detección, en una pluralidad de porciones; un paso de almacenar una primera porción de los datos biométricos divididos en un archivo de base de datos, el método de autenticación se caracteriza porque el paso de registro también incluye: un paso de crear una clave de información biométrica a partir de los datos biométricos; y un paso de escribir la clave de información biométrica generada a partir de los datos biométricos y una segunda porción de datos biométricos dividida en el medio individual, y el paso de verificación incluye: un paso de combinar la segunda porción de datos biométricos en el medio individual con una primera porción de datos biométricos en el archivo de base de datos; un paso de crear una clave de información biométrica de los datos biométricos combinados; un paso de comparar la clave de información biométrica leída en el medio individual con la clave de información biométrica creada; un paso de recuperar, cuando el resultado de la comparación en el paso de comparación es una falta de concordancia, otra primera porción de datos biométricos perteneciente a un usuario diferente del archivo de base de datos; un paso de combinar la segunda porción de datos biométricos en el medio individual con la otra primera porción de datos biométricos recuperada del archivo de base de datos; un paso de crear una clave de información biométrica a partir de los datos biométricos combinados; y un paso de verificar, cuando el resultado de la comparación es una concordancia, los datos biométricos combinados contra datos biométricos obtenidos del dispositivo de detección, y realizar autenticación o identificación de un

individuo.

En esta invención, la unidad de control se puede disponer para dividir los datos biométricos de un usuario detectados por el dispositivo de detección al tiempo del registro de los datos biométricos, registrar una primera porción dividida de datos biométricos en el archivo de base de datos, y almacenar una segunda porción de datos biométricos y la clave de información biométrica en el medio individual.

En esta invención, la unidad de control se puede disponer para crear la clave de información biométrica a partir de una zona de datos que cubre una intersección de la pluralidad de porciones divididas de los datos biométricos.

En esta invención, la unidad de control puede crear la clave de información biométrica a partir de los datos biométricos y de un número de identificación introducido por el usuario.

La invención puede incluir además un dispositivo de lectura/escritura de medio que lee información de almacenamiento y escribe información de almacenamiento en el medio individual.

En esta invención, cuando el resultado de la comparación es una concordancia, la unidad de control puede operar el dispositivo de detección y obtiene los datos biométricos para el usuario.

En esta invención, la unidad de control puede tener un módulo de control de gestión de datos biométricos que combina la segunda porción de datos biométricos en el medio individual y la primera porción de datos biométricos en el archivo de base de datos, crea una clave de información biométrica a partir de los datos biométricos combinados, y compara la clave de información biométrica leída en el medio individual con la clave de información biométrica creada, y un módulo de control de verificación, que verifica los datos biométricos combinados contra datos biométricos obtenidos del dispositivo de detección y realiza autenticación individual.

En esta invención, el módulo de control de gestión de datos biométricos se puede disponer para dividir los datos biométricos detectados por el dispositivo de detección, registrar la primera porción de los datos biométricos divididos en el archivo de base de datos, y almacenar la segunda porción de los datos biométricos divididos y la clave de información biométrica en el medio individual, y la unidad de control puede incluir además un módulo de control de registro dispuesto para operar el dispositivo de detección, adquirir los datos biométricos, y pasar los datos al módulo de control de gestión de datos biométricos.

En esta invención, el dispositivo de detección puede ser un dispositivo que detecta imágenes de vasos sanguíneos en el cuerpo.

En esta invención, el dispositivo de detección puede incluir una unidad de captura de imagen que capture imágenes de vasos sanguíneos en una mano del cuerpo.

Por medio de esta invención, se crea una clave de información biométrica a partir de datos biométricos, los datos biométricos son separados en una pluralidad de porciones, cada porción es almacenada en medios diferentes, y las porciones son enlazada por la clave de información biométrica. Por lo tanto, incluso aunque los datos biométricos son separados y almacenados de manera distribuida, se mejora la confidencialidad de la asociación de las porciones de datos separadas, contribuyendo a la prevención de uso ilícito como resultado de la filtración o el robo de datos biométricos.

Ahora se describirá realizaciones de la presente invención con referencia a los dibujos acompañantes, en los que:

La figura 1 es un diagrama de la configuración del dispositivo de autenticación biométrica de una realización de la invención.

La figura 2 es un diagrama de la configuración del dispositivo de autenticación biométrica de la figura 1 al tiempo de registro.

La figura 3 es un diagrama que explica la operación al tiempo de registro en la figura 2.

La figura 4 es un diagrama del flujo de procesado durante el registro en la figura 2.

La figura 5 es un diagrama que explica el procesado de registro de la figura 4.

La figura 6 es un diagrama de la configuración del dispositivo de autenticación biométrica de la figura 1 al tiempo de la autenticación.

La figura 7 es un diagrama que explica la operación al tiempo de la autenticación en la figura 6.

La figura 8 es un diagrama del flujo de procesado durante la autenticación en la figura 6.

La figura 9 es un diagrama que explica el procesado de autenticación de la figura 8.

A continuación se explican realizaciones de la invención, siguiendo el orden de un dispositivo de autenticación biométrica, procesado de registro de datos biométricos, procesado de autenticación de datos biométricos, y otras realizaciones.

Dispositivo de autenticación biométrica

La figura 1 es una vista frontal del dispositivo de autenticación biométrica de una realización de la invención. La figura 1 representa un dispositivo de entrada/salida que emplea un mecanismo de autenticación de venas de la palma, como un dispositivo de autenticación biométrica. Como se representa en la figura 1, el dispositivo de autenticación biométrica 4 tiene una placa principal 3. En la placa principal 3 se ha dispuesto un dispositivo de lectura/escritura de tarjetas CI 2, un sensor de venas (dispositivo de detección biométrica) 1, una pantalla 14, una pantalla de resultado de autenticación 16, un zumbador 17, y un grupo de teclas de entrada 12.

El dispositivo de lectura/escritura de tarjetas CI 2 lee datos y escribe datos en un chip CI en una tarjeta CI (tarjeta individual) que lleva el usuario. Como se explica a continuación, esta tarjeta CI guarda datos biométricos separados β y una clave de información biométrica.

El sensor de venas 1 incluye un dispositivo de captura de imagen de la palma. El dispositivo de captura de imagen de la palma 1 lleva montada, sustancialmente en el centro de la unidad principal, una unidad sensora 1-1. Encima y debajo de la unidad sensora 1-1 se ha dispuesto un par de guías 1-2 y 1-3. La guía 1-2 sirve para soportar la muñeca, y la guía 1-3 sirve para soportar los dedos.

Por lo tanto la guía 1-2 guía al usuario con el fin de guiar y soportar la muñeca, y la guía 1-3 proporciona guía al usuario con el fin de guiar y soportar los dedos. En consecuencia, la posición de la palma encima de la unidad sensora 1-1, es decir, la posición, la inclinación y el tamaño pueden ser controlados.

La unidad sensora 1-1 está provista de un sensor de infrarrojos (sensor CMOS), lente de enfoque y un sensor de distancia en el centro; en su periferia se ha dispuesto una pluralidad de elementos emisores de luz infrarroja cercana (LEDs). Por ejemplo, los elementos emisores de luz infrarroja cercana están dispuestos en ocho lugares en la periferia, para emitir rayos infrarrojos cercanos hacia arriba. El sensor CMOS recibe la luz emitida que ha sido reflejada. Se extrae una configuración de las venas de la imagen capturada así recibida. La unidad de visualización 14 presenta varios estados, tales como, por ejemplo, mensajes de guía y similares. La unidad de visualización de resultado de autenticación 16 usa una lámpara para presentar el resultado de autenticación (OK, NB). El zumbador 17 usa sonidos para la notificación de varios estados. El grupo de teclas 12 tiene un teclado numérico 121 para la entrada de IDs y similares, una tecla de fin 122 para indicar el final de la operación, y una tecla de menú 123 para la selección de elementos de menú.

Como se explica a continuación, en este sistema de entrada/salida, el usuario introduce su propia tarjeta CI en el dispositivo de lectura/escritura de tarjetas CI 2 al tiempo de registro, y también mantiene su palma sobre el dispositivo de captura de imagen de la palma (a continuación simplemente “dispositivo de captura de imagen”) 1, para hacer que se lea una imagen de los vasos sanguíneos. La placa principal 3 crea datos de imagen de vasos sanguíneos (datos biométricos) a partir de la imagen leída de los vasos sanguíneos, y separa estos datos de imagen de vasos sanguíneos, y luego registra una porción de los datos de imagen de vasos sanguíneos α en la placa principal 3, y otra porción de los datos de imagen de vasos sanguíneos β en la tarjeta CI. Simultáneamente, la placa principal 3 crea una clave de información biométrica a partir de los datos de imagen de vasos sanguíneos y registra la clave de información biométrica en la tarjeta CI.

Después de la entrada, un usuario introduce su propia tarjeta CI en el dispositivo de lectura/escritura de tarjetas CI 2, y el dispositivo de lectura/escritura de tarjetas CI 2 lee los datos de imagen de vasos sanguíneos β y la clave de información biométrica de la tarjeta CI. El usuario también mantiene su palma sobre el dispositivo de captura de imagen 1, haciendo que se lea una imagen de los vasos sanguíneos. La placa principal 3 combina los datos de imagen de vasos sanguíneos β así leídos con una porción de datos de imagen de vasos sanguíneos α dentro de la placa principal 3, crea una clave de información biométrica a partir de los datos de imagen de vasos sanguíneos combinados, y verifica la clave contra la clave de información biométrica registrada leída de la tarjeta CI.

Si el resultado de la verificación es una concordancia, se determina que los datos de imagen de vasos sanguíneos α están asociados con los datos de imagen de vasos sanguíneos β en la tarjeta CI, se combinan los datos de imagen de vasos sanguíneos α y los datos de imagen de vasos sanguíneos β de la tarjeta CI, y se crean los datos de imagen de vasos sanguíneos registrados (datos biométricos). Entonces, los datos de imagen de vasos sanguíneos obtenidos de la imagen de vasos sanguíneos leída por el dispositivo de captura de imagen 1 son verificados contra estos datos de imagen de vasos sanguíneos creados. Si el resultado de la verificación es satisfactorio, se abre la puerta bajo el control realizado por la placa principal 3, y es posible la entrada.

Si el resultado de la verificación no es satisfactorio, la placa principal 3 recupera otros datos de imagen de vasos sanguíneos α de dentro de la placa principal 3, combina los datos de imagen de vasos sanguíneos leídos β con los datos de imagen de vasos sanguíneos recuperados α, crea una clave de información biométrica a partir de los datos de imagen de vasos sanguíneos combinados, y verifica la clave contra la clave de información biométrica registrada leída de la tarjeta CI.

Si el resultado de la verificación es una concordancia, se crean datos de imagen de vasos sanguíneos registrados, y los datos de imagen de vasos sanguíneos obtenidos del dispositivo de captura de imagen 1 son verificados contra estos datos de imagen de vasos sanguíneos registrados creados. Si el resultado de la verificación es una falta de concordancia, se puede recuperar igualmente otros datos de imagen de vasos sanguíneos α de dentro de la placa principal 3. Y los datos de imagen de vasos sanguíneos leídos β son combinados con los datos de imagen de vasos sanguíneos recuperados α, se crea una clave de información biométrica a partir de los datos de imagen de vasos sanguíneos combinados, y esta clave puede ser verificada contra la clave de información biométrica registrada leída de la tarjeta CI.

Así, al tiempo de registro, se crea una clave de información biométrica a partir de los datos de imagen de vasos sanguíneos registrados, y se asocian los datos de imagen de vasos sanguíneos α y los datos de imagen de vasos sanguíneos β que se habían separado de los datos de imagen de vasos sanguíneos registrados. Por lo tanto, incluso cuando las porciones separadas de datos de imagen de vasos sanguíneos se almacenan en medios diferentes, y los datos de imagen de vasos sanguíneos y la clave de información salen de uno de los medios, o aunque se produzca robo, si no se obtienen los otros datos de imagen de vasos sanguíneos, no se puede obtener la clave de información. Por lo tanto, la eficacia al evitar el uso ilícito a través de la gestión de datos biométricos distribuidos se puede mejorar más.

Procesado de registro de datos biométricos

La figura 2 explica el registro de datos biométricos en el dispositivo de la figura 1, y la figura 3 explica los datos creados. En la figura 2, las porciones idénticas a las de la figura 1 se indican con los mismos símbolos. Como se representa en la figura 2, la placa principal 3 tiene una CPU 3-1 con memoria, memoria de arranque 3-2, memoria de registro 3-3, y memoria de almacenamiento de datos (SRAM) 7. La memoria de arranque 3-2 guarda el OS (sistema operativo), un programa de aplicación 30, y una librería de autenticación (programa de autenticación) 34.

La memoria de registro 3-3 se usa para registros de información individual. La memoria de almacenamiento de datos 7 tiene una tabla biométrica 70, que guarda datos de venas separados α; una tabla de datos individuales 74, que guarda información individual; y una tabla de gestión de información individual 72, que guarda información individual para gestionar la tabla de datos individuales 74.

La CPU 3-1 ejecuta el programa de aplicación de tarea 30 y la librería de autenticación 34 bajo control por el OS, leído de la memoria de arranque 3-2. Como se representa en la figura 2, este programa de aplicación 30 tiene un programa de control de registro 32, un programa de control de gestión de datos de venas 36, y un programa de control de verificación 38, explicados en la figura 6.

La placa principal 3 está conectada a una clave de gestor 10 y a una placa de control de cerradura eléctrica 18 que acciona la apertura y el cierre de la puerta eléctrica 19. En unión con el programa de aplicación 30 se facilita un controlador 40 de un teclado numérico 12, un controlador 42 para la pantalla 14, un controlador 44 para el sensor de venas 1, un controlador 46 para la pantalla de resultado de autenticación (lámpara de LED) 16, un controlador 48 para el zumbador 17 y un controlador 50 para el dispositivo de lectura/escritura de tarjetas CI 2.

La operación al tiempo de registro se explica con referencia a la figura 3. En primer lugar, con el fin de realizar el registro, se introduce la clave de gestor 10 en la placa principal 3, para permitir el registro. El programa de aplicación 30 detecta la clave de gestor 10 y empieza el programa de control de registro 32, y se presenta un menú de registro en la pantalla 14.

Mientras ve el menú de registro, el usuario puede operar el teclado numérico del grupo de teclas 12 para introducir su propio número de registro (nombre, ID, departamento) y una ID de registro. Al recibir el número de registro y la ID de registro, el programa de control de registro 32 presenta un mensaje de inicio de registro en la pantalla 14, y emite una instrucción de captura de imagen al programa de autenticación de venas 34. En respuesta, el usuario pone la mano sobre el sensor de venas 1. El programa de autenticación de venas 34 arranca el sensor de venas 1, y el sensor de venas 1 captura una imagen de la palma de la mano, y envía la imagen capturada a la librería de autenticación de venas 34.

La librería de autenticación de venas 34 ejecuta una serie de procesado de registro y verificación. Es decir, la librería de autenticación de venas 34 ejecuta procesado de detección de distancia/contorno de mano, procesado de extracción de imagen de vasos sanguíneos, y procesado de registro y verificación. En el procesado de detección de distancia/contorno de mano, la distancia medida por el sensor de distancia es recibida del dispositivo de captura de imagen 1, se determina que la palma u otro objeto está a una distancia dentro de un rango preestablecido de la

unidad sensora 1-1, y el contorno de la palma es detectado a partir de la imagen capturada por la unidad sensora 1-1, y en base al contorno se determina si la imagen es una imagen que puede ser usada en el procesado de registro y verificación. Por ejemplo, la palma puede no aparecer adecuadamente en la imagen.

En el procesado de extracción de imagen de vasos sanguíneos, cuando se determina en el procesado de detección del contorno de la mano que una imagen ha sido capturada con la mano colocada correctamente, se extrae una imagen de vasos sanguíneos de la imagen de la mano. Es decir, se extraen datos en escala de grises de la imagen de la palma usando diferencias en la reflectividad, y a partir de estos datos de imagen de vasos sanguíneos (escala de grises), se extraen características de la imagen de vasos sanguíneos (las direcciones y los números de los troncos y bifurcaciones de vasos sanguíneos, y similares), determinadas con anterioridad.

El procesado de verificación recupera datos de imagen de vasos sanguíneos, compara los datos de imagen de vasos sanguíneos detectados en el procesado de detección de imagen de vasos sanguíneos con los datos de imagen de vasos sanguíneos registrados recuperados, realiza el procesado de verificación, y envía un resultado de la verificación. El procesado de registro registra los datos característicos de imagen de vasos sanguíneos.

La librería de autenticación de venas 34 extrae una imagen de vasos sanguíneos de la imagen capturada por el sensor de venas 1, y extrae los datos característicos de la imagen de vasos sanguíneos. La librería de autenticación de venas 34 realiza control de captura de imagen y extracción de imágenes de vasos sanguíneos y datos característicos de imagen de vasos sanguíneos una pluralidad de veces (por ejemplo, tres veces). Y la librería de autenticación de venas 34 realiza la verificación de los datos característicos de una pluralidad de imágenes de vasos sanguíneos, y si los resultados de la verificación son satisfactorios, notifica al programa de control de registro 32 el resultado de autenticación OK de los datos como datos característicos de imagen de vasos sanguíneos adecuados para registro.

A la obtención del OK de autenticación, el programa de control de registro 32 usa la lámpara de LED 16 y el zumbador 17, mediante los controladores 46 y 48, para notificar el OK de autenticación. El programa de control de registro 32 envía entonces los datos de registro (datos individuales y datos característicos de imagen de vasos sanguíneos) al programa de control de gestión de datos de venas 36.

Como se representa en la figura 3, el programa de control de gestión de datos de venas 36 recibe como información de registro los datos individuales (información de registro, ID de registro) 64 y los datos característicos de imagen de vasos sanguíneos 68, y a partir de los datos característicos 68 crea una clave de información biométrica 66. Los detalles del método de creación se explican más adelante. El programa de control de gestión de datos de venas 36 separa los datos característicos 68 y crea datos de venas separados α (60) y datos de venas separados β (61).

Además, el programa de control de gestión de datos de venas 36 usa la clave de información biométrica 66 para crear una tabla de gestión de información individual 72 y una tabla de datos individuales 74. Por ejemplo, los datos individuales 64 se guardan en la tabla de datos individuales 74, y la clave de información biométrica 66 y su posición de almacenamiento se guardan en la tabla de gestión de información individual 72. El programa de control de gestión de datos de venas 36 guarda los datos de venas separados antes descritos α (60) en el archivo 70 para datos de venas separados α en la memoria 7.

Además, el programa de control de gestión de datos de venas 36 escribe la clave de información biométrica 66 antes descrita y los datos de venas separados (61) antes descritos en la tarjeta CI 20 mediante el controlador 50 y el dispositivo de lectura/escritura de tarjetas CI 2.

De esta forma, se crea una clave de información biométrica a partir de datos de imagen de vasos sanguíneos, los datos de imagen de vasos sanguíneos se separan en dos porciones, y las porciones se guardan en medios diferentes (la tarjeta CI 20 y la memoria 7 de la placa principal 3) y se enlazan mediante la clave de información biométrica.

A continuación se explica el procesado de registro por el programa de control de gestión de datos de venas 36, con referencia al flujo de procesado de la figura 4 y el procesado explicado en la figura 5.

(S10) En primer lugar, el programa de control de gestión de datos de venas (a continuación se denomina el “programa de control”) 36 adquiere datos característicos registrados G2 y una ID de registro de entrada.

(S12) A continuación, el programa de control 36 corta una zona específica G5 de los datos característicos G2. Aquí, los datos son separados en dos porciones, y así se corta una zona G5 perteneciente a ambas porciones separadas.

(S14) El programa de control 36 crea una clave de información biométrica 66 a partir de los datos característicos cortados G5 y la ID de registro adquirida, por medio de encriptado preestablecido. Por ejemplo, los datos de mapa de bits de la zona G5 de datos característicos y la ID de registro se someten a un algoritmo de encriptado preestablecido para crear la clave de información biométrica 66.

(S16) A continuación, el programa de control 36 divide los datos característicos registrados G2. Aquí, los datos característicos registrados G2 se dividen en porciones alta y baja para crear datos de venas α (G3) a almacenar en un medio A (memoria 7), y datos de venas β (G4) a almacenar en un medio B (la tarjeta CI 20).

(S18) El programa de control 36 guarda la clave de información biométrica 66, la ID de registro, y los datos de venas β (G4) 61 en el medio B (tarjeta CI 20). El programa de control 36 también guarda los datos de venas separados α (G3) 60 en el medio A (archivo de datos de venas 70 en la memoria 7 en la placa principal 3).

De esta forma, los datos biométricos (aquí, la imagen de vasos sanguíneos) son divididos, distribuidos y guardados, y se usa una porción de los datos biométricos para crear una clave de información biométrica asociada. Por lo tanto, la asociación de los datos biométricos divididos y guardados depende de los datos biométricos del usuario, y por ello es sumamente difícil de conocer aunque haya filtración de datos.

Además, se añade una ID de registro para crear la clave de información biométrica, de modo que el desencriptado resulte aún más difícil. La clave de información biométrica se guarda en la tarjeta CI, contribuyendo a evitar la manipulación y la filtración de la clave de información biométrica.

Procesado de verificación de datos biométricos

La figura 6 explica la verificación de datos biométricos en el dispositivo de la figura 1, y la figura 7 explica el procesado de verificación. En la figura 6, a las porciones idénticas a las de la figura 1 y la figura 2 se les asignan los mismos símbolos. Como se representa en la figura 2, la CPU 3-1 en la placa principal 3 ejecuta el programa de aplicación de tarea 30 y la librería de autenticación 34 bajo el control del OS leído de la memoria de arranque 3-2. La CPU 3-1 ejecuta el programa de control de verificación 38 y el programa de control de gestión de datos de venas 36.

La operación al tiempo de la verificación se explica con referencia a la figura 6. En primer lugar, el usuario introduce una tarjeta CI 20 en el dispositivo de lectura/escritura CI 2. El dispositivo de lectura/escritura de tarjetas CI 2 lee los datos de venas separados guardados β (61), la clave de información biométrica 66, y la ID de registro, y los envía al programa de control de verificación 38. A continuación, el programa de control de gestión de datos de venas 36 lee datos de venas separados α (60) del archivo de datos de venas separados 70.

Como se representa en la figura 7, el programa de control de gestión de datos de venas 36 combina los datos de venas separados β (61) leídos de la tarjeta CI 20 y los datos de venas separados α (60) leídos del archivo 70, y crea datos característicos 68. Entonces, el programa de control de gestión de datos de venas 36 crea una clave de información biométrica 66-1 a partir de la ID de registro y los datos característicos 68 antes descritos, por medio del procesado de encriptado antes descrito.

El programa de control de gestión de datos de venas 36 determina si la clave de información biométrica 66-1 así creada concuerda con la clave de información biométrica 66 leída de la tarjeta CI 20. Si no hay concordancia, el programa de control de gestión de datos de venas 36 lee los datos de venas separados α (60) guardados en la posición siguiente del archivo de datos de venas separados 70, combina igualmente los datos de venas separados β (61) leídos de la tarjeta CI 20 con los datos de venas separados α (60) del archivo 70, y crea datos característicos 68. Entonces, el programa de control de gestión de datos de venas 36 usa el procesado de encriptado antes descrito para crear una clave de información biométrica 66-1 a partir de LA ID de registro y los datos característicos 68 antes descritos. El programa de control de gestión de datos de venas 36 determina si la clave de información biométrica 66-1 así creada concuerda con la clave de información biométrica 66 leída de la tarjeta CI 20.

Por otra parte, al determinar que la clave de información biométrica 66-1 así creada concuerda con la clave de información biométrica 66 leída de la tarjeta CI 20, el programa de control de gestión de datos de venas 36 usa la clave de información biométrica 66 para consultar la tabla de gestión de información individual 62, recupera los datos individuales (número de registro) 64 correspondientes al archivo de datos individuales 74, lo prepara conjuntamente con los datos característicos 68 previamente creados como información de registro, y notifica al programa de control de verificación 38 la terminación de la preparación.

El programa de control de verificación 38 presenta en la pantalla 14 un mensaje de inicio de autenticación, y emite una instrucción de captura de imagen al programa de autenticación de venas 34. En respuesta, el usuario pone la mano sobre el sensor de venas 1. El programa de autenticación de venas 34 arranca el sensor de venas 1, y el sensor de venas 1 captura una imagen de la palma de la mano, y envía la imagen capturada a la librería de autenticación de venas 34.

La librería de autenticación de venas 34 extrae una imagen de vasos sanguíneos de la imagen capturada por el sensor de venas 1, y extrae datos característicos de la imagen de vasos sanguíneos. La librería de autenticación de venas 34 notifica al programa de control de gestión de datos biométricos 36 la terminación de la extracción. El programa de control de gestión de datos biométricos 36 envía los datos característicos combinados antes descritos 68 a la librería de autenticación de venas 34.

Como se ha explicado anteriormente, la librería de autenticación de venas 34 realiza la verificación de los datos característicos de imagen de vasos sanguíneos obtenidos mediante captura de imagen contra los datos característicos combinados, y si el resultado de la verificación es satisfactorio, notifica al programa de control de registro 32 el resultado de la autenticación OK.

Al obtener un resultado de autenticación OK, el programa de control de registro 32 notifica el Resultado de autenticación OK usando la lámpara de LED 16 y el zumbador 17, mediante los controladores 46 y 48. El programa de control de registro 32 controla entonces la placa de control de cerradura eléctrica 18 mediante el controlador 52, permitiendo la apertura de la puerta eléctrica 19. Los datos individuales son registrados en la memoria de registro 3-3.

De esta forma se combinan los datos de imagen de vasos sanguíneos que han sido distribuidos y almacenados, se crea una clave de información biométrica, y la clave de nueva creación es comparada con la clave de información biométrica registrada, de modo que incluso cuando los datos biométricos sean distribuidos y guardados, se pueda mantener el secreto de la relación de enlace.

A continuación se explica el procesado de verificación por el programa de control de gestión de datos de venas 36, con referencia al diagrama de flujo de procesado de la figura 8 y el diagrama que explica el procesado en la figura 9.

(S20) En primer lugar, el programa de control de gestión de datos de venas 36 adquiere los datos de venas separados β (61), la clave de información biométrica 66, y la ID de registro guardados en la tarjeta CI 20, del programa de control de verificación 38.

(S22) A continuación, el programa de control de gestión de datos de venas (a continuación se denomina el "programa de control") 36 adquiere los datos de venas separados α (60-1) de la memoria 70.

(S24) El programa de control 36 combina los datos de venas separados β (61) leídos de la tarjeta CI 20 y los datos de venas separados α (60-1) leídos del archivo 70, y crea datos característicos 68.

(S26) El programa de control 36 corta una zona específica G5 de los datos característicos G2. Aquí, los datos son separados en dos porciones, y así se corta una zona G5 perteneciente a ambas porciones separadas.

(S28) El programa de control 36 crea una clave de información biométrica 66 de los datos característicos cortados G5 y la ID de registro adquirida, por medio de encriptado preestablecido. Por ejemplo, los datos de mapa de bits de la zona G5 de datos característicos y la ID de registro se someten a un algoritmo de encriptado preestablecido para crear la clave de información biométrica 66-1.

(S30) A continuación, el programa de control 36 compara la clave de información biométrica creada nuevamente 61-1 y la clave de información biométrica 66 leída del medio B (tarjeta CI 20). Si el resultado de la comparación no es una concordancia, el procesado vuelve al paso S22, se adquieren los datos de venas α 60-2 en la posición siguiente, y se ejecuta el procesado de los pasos S24 a S30.

(S32) Por otra parte, si el resultado de la comparación es una concordancia, el programa de control 36 notifica la terminación de la preparación de información de registro, como se ha descrito anteriormente, realiza captura de imagen y verificación de los datos característicos G2 contra los datos característicos G2-1 obtenidos del resultado de captura de imagen, y realiza el procesado de autenticación.

De esta forma, los datos biométricos (aquí, datos de imagen de vasos sanguíneos) son divididos y distribuidos en medios diferentes para almacenamiento, y además se crea una clave de información biométrica asociada a partir de una porción de los datos biométricos. Por lo tanto, la asociación de los datos biométricos que han sido distribuidos y guardados depende de los datos biométricos del usuario, y así son sumamente difíciles de conocer aunque haya filtración de datos.

Además, se añade la ID de registro para crear la clave de información biométrica, de modo que el desencriptado todavía resulta más difícil. La clave de información biométrica se guarda en la tarjeta CI, contribuyendo a evitar la manipulación y la filtración de la clave de información biométrica.

Además, la separación y la fusión de los datos biométricos, la creación de la clave de información biométrica, y la comparación son ejecutadas por un programa de control de gestión de datos 36 que no participa en el procesado de registro o el procesado de verificación, de modo que el secreto se puede guardar mejor.

Otras realizaciones

En las realizaciones antes descritas se usaron datos de imagen de vasos sanguíneos de la palma de una mano como los datos biométricos en las explicaciones; sin embargo, también se puede usar la imagen de vasos sanguíneos del reverso de la mano o los dedos. Igualmente, también es posible la aplicación a huellas dactilares,

huellas de la mano, imágenes de la retina, rasgos faciales y otros datos biométricos.

Además, la división de datos biométricos se explicó con relación al caso de división en porciones alta y baja; pero la división puede ser en porciones izquierda y derecha, o en tres o más porciones. Al dividir en tres o más porciones, se puede crear una clave de información biométrica a partir de una zona quitada que incluya tres o más porciones separadas, o se puede crear una clave de información biométrica a partir de una zona quitada que incluya dos porciones separadas.

Igualmente, la clave de información biométrica puede ser creada a partir de la porción cortada sin usar la ID de registro, y el medio para almacenamiento distribuido no se limitan a una tarjeta CI (medio individual) y la memoria en el dispositivo de verificación, sino que pueden ser una combinación de dos unidades de medio individual, o pueden ser un medio individual y un dispositivo de gestión conjunto (por ejemplo, un servidor conectado al dispositivo de entrada/salida).

Además, se explicaron ejemplos en los que los datos de venas separados α guardados en el dispositivo no tenían índice; pero la ID de registro puede ser usada como un índice. En este caso, los datos de venas separados correspondientes α pueden ser recuperados rápidamente.

Además, los campos de aplicación no se limitan a dispositivos de entrada/salida, y es posible la aplicación al uso de hoteles y otras instalaciones, a sistemas de alquiler de vídeos, automóviles u otros artículos, a usos en lugar de tarjetas de crédito en zonas financieras y de distribución, a sistemas de verificación de reservas en trenes, aviones y otros sistemas de transporte, y análogos.

En lo que antecede se ha explicado la invención mediante realizaciones de la invención; pero se puede hacer varias modificaciones en la invención dentro del alcance de la invención, y estas modificaciones no quedan excluidas del alcance de la invención.

Se crea una clave de información biométrica a partir de datos biométricos, los datos biométricos son separados en una pluralidad de porciones que se guardan en medios diferentes, y las porciones son enlazadas por la clave de información biométrica, de modo que aunque los datos biométricos estén separados, distribuidos y guardados, se pueda mejorar la confidencialidad de la asociación de las porciones de datos separadas individuales, contribuyendo a evitar el uso ilícito debido a filtración o robo de datos biométricos.

REIVINDICACIONES

1. Un dispositivo de autenticación biométrica (4), que detecta características de un cuerpo de un usuario y realiza autenticación individual, incluyendo:

un dispositivo de detección (1), que detecta una porción de interés del cuerpo, y envía datos biométricos que indican características biométricas;

un archivo de base de datos (7), dispuesto para almacenar una primera porción de datos biométricos (60) de una pluralidad de porciones de datos resultantes de la división de los datos biométricos del usuario detectados por el dispositivo de detección, para almacenar porciones de datos de una pluralidad de usuarios;

un medio individual (20) para almacenar una segunda porción de datos biométricos (61) de la pluralidad de porciones de datos; y

una unidad de control (3-1) que, al tiempo de la autenticación, usando el medio individual, combina la segunda porción de datos biométricos (61) del medio individual (20) con una primera porción de datos biométricos (60) recuperada del archivo de base de datos (7), **caracterizado** porque el medio individual (20) guarda una clave de información biométrica (66) generada a partir de los datos biométricos,

la unidad de control (3-1) crea una clave de información biométrica (66-1) a partir de los datos biométricos combinados, compara la clave de información biométrica (66) leída del medio individual (20) con la clave de información biométrica creada (66-1) para determinar si la primera porción de datos biométricos recuperada (60) está asociada con la segunda porción de datos biométricos (61) del medio individual (20), donde,

cuando el resultado de la comparación es una falta de concordancia, la unidad de control (3-1) está dispuesta para recuperar otra primera porción de datos biométricos del archivo de base de datos (7) perteneciente a un usuario diferente, combinar la segunda porción de datos biométricos (61) en el medio individual (20) y la otra primera porción de datos biométricos recuperada del archivo de base de datos (7), y crear una clave de información biométrica (66-1) a partir de los datos biométricos combinados, y

cuando el resultado de la comparación es una concordancia, la unidad de control (3-1) está dispuesta para verificar los datos biométricos combinados contra los datos biométricos obtenidos del dispositivo de detección, y realizar autenticación individual.

2. El dispositivo de autenticación biométrica (4) según la reivindicación 1, donde, al tiempo del registro de datos biométricos, la unidad de control (3-1) está dispuesta para dividir los datos biométricos de un usuario detectados por el dispositivo de detección (1) en una pluralidad de porciones, registrar una primera porción de los datos biométricos divididos como la primera porción de datos biométricos (60) en el archivo de base de datos (7), y almacenar una segunda porción de los datos biométricos como la segunda porción de datos biométricos (61) y la clave de información biométrica (66) en el medio individual (20).

3. El dispositivo de autenticación biométrica (4) según la reivindicación 2, donde la unidad de control (3-1) está dispuesta para crear la clave de información biométrica (66) a partir de una zona de datos que cubre una intersección de la pluralidad de porciones de datos biométricos resultantes de la división de los datos biométricos.

4. El dispositivo de autenticación biométrica (4) según la reivindicación 2, donde la unidad de control (3-1) está dispuesta para crear la clave de información biométrica (66) a partir de los datos biométricos y a partir de un número de identificación introducido por el usuario.

5. El dispositivo de autenticación biométrica (4) según cualquier reivindicación precedente, incluyendo además:

un dispositivo de lectura/escritura de medio (2) configurado para leer información guardada y escribir información de almacenamiento en el medio individual.

6. El dispositivo de autenticación biométrica (4) según cualquier reivindicación precedente, donde, cuando el resultado de la comparación es una concordancia, la unidad de control (3-1) está dispuesta para operar el dispositivo de detección y obtiene los datos biométricos relativos al usuario.

7. El dispositivo de autenticación biométrica (4) según cualquier reivindicación precedente, donde la unidad de control (3-1) incluye:

un módulo de control de gestión de datos biométricos (36) dispuesto para combinar la segunda porción de datos biométricos (61) en el medio individual (20) y la primera porción de datos biométricos (60) en el archivo de base de datos (7), para crear una clave de información biométrica (66-1) a partir de los datos biométricos combinados, y para comparar la clave de información biométrica (66) leída del medio individual (20) con la clave de información

biométrica creada (66-1); y

un módulo de control de verificación (38) dispuesto para verificar los datos biométricos combinados contra datos biométricos obtenidos del dispositivo de detección (1) y para realizar autenticación individual.

8. El dispositivo de autenticación biométrica (4) según la reivindicación 7, donde el módulo de control de gestión de datos biométricos (36) también está dispuesto para dividir los datos biométricos detectados por el dispositivo de detección (1), registrar la primera porción de los datos biométricos divididos en el archivo de base de datos (7), y almacenar la segunda porción de los datos biométricos divididos y la clave de información biométrica en el medio individual (20); y

la unidad de control (3-1) incluye además un módulo de control de registro (32) dispuesto para operar el dispositivo de detección (1), para adquirir los datos biométricos, y para pasar los datos al módulo de control de gestión de datos biométricos (36).

9. El dispositivo de autenticación biométrica (4) según cualquier reivindicación precedente, donde el dispositivo de detección (1) es un dispositivo para detectar imágenes de vasos sanguíneos en el cuerpo.

10. El dispositivo de autenticación biométrica (4) según la reivindicación 9, donde el dispositivo de detección (1) incluye una unidad de captura de imagen para capturar imágenes de vasos sanguíneos en una mano del cuerpo.

11. Un método de autenticación biométrica que consiste en detectar una característica biométrica de un usuario y realizar autenticación individual, incluyendo:

un paso de registrar los datos biométricos de una pluralidad de usuarios; y

un paso de verificar los datos biométricos de un usuario,

donde el paso de registro incluye:

un paso de detección que consiste en detectar una porción de interés del cuerpo del usuario, y de enviar datos biométricos que indican las características biométricas;

un paso de dividir los datos biométricos del usuario, detectados en el paso de detección, en una pluralidad de porciones;

un paso de almacenar una primera porción de los datos biométricos divididos (60) en un archivo de base de datos (7), el método de autenticación **se caracteriza** porque el paso de registro incluye además:

un paso de crear una clave de información biométrica (66) a partir de los datos biométricos; y

un paso de escribir la clave de información biométrica (66) generada a partir de los datos biométricos y una segunda porción de datos biométricos divididos (61) en un medio individual (20), y

el paso de verificación incluye:

un paso de combinar la segunda porción de datos biométricos (61) en el medio individual (20) con una primera porción de datos biométricos (60) en el archivo de base de datos (7);

un paso de crear una clave de información biométrica (66-1) a partir de los datos biométricos combinados;

un paso de comparar la clave de información biométrica (66) leída del medio individual (20) con la clave de información biométrica creada (66-1);

un paso de recuperar, cuando el resultado de la comparación en el paso de comparación es una falta de concordancia, otra primera porción de datos biométricos perteneciente a un usuario diferente del archivo de base de datos (7);

un paso de combinar la segunda porción de datos biométricos (61) en el medio individual (20) con la otra primera porción de datos biométricos recuperada del archivo de base de datos (7);

un paso de crear una clave de información biométrica (66-1) a partir de los datos biométricos combinados; y

un paso de verificar, cuando el resultado de la comparación es una concordancia, los datos biométricos combinados contra datos biométricos obtenidos de un dispositivo de detección (1), y realizar autenticación individual.

12. El método de autenticación biométrica según la reivindicación 11, donde el paso de crear la clave de información biométrica (66) incluye un paso de crear la clave de información biométrica (66) a partir de una zona de datos que cubre una intersección de la pluralidad de porciones de datos biométricos resultantes de la división de los datos biométricos.

13. El método de autenticación biométrica según la reivindicación 11 o 12, donde el paso de crear la clave de información biométrica (66) incluye un paso de crear la clave de información biométrica (66) a partir de los datos biométricos y de un número de identificación introducido por el usuario.

14. El método de autenticación biométrica según cualquiera de las reivindicaciones 11 a 13, incluyendo además un paso de ejecutar la lectura y la escritura de la clave de información biométrica (66) y los segundos datos biométricos (61) de y en el medio individual (20), usando un dispositivo de lectura/escritura de medio (2) que lee información de almacenamiento y escribe información de almacenamiento en el medio individual (20).

15. El método de autenticación biométrica según cualquiera de las reivindicaciones 12 a 14, incluyendo además un paso de operar, cuando el resultado de la comparación es una concordancia, el dispositivo de detección (1) y obtener datos biométricos relativos al usuario.

16. El método de autenticación biométrica según cualquiera de las reivindicaciones 11 a 15, incluyendo además:

un paso de hacer que un módulo de control de gestión de datos biométricos (36) ejecute el paso de combinar la segunda porción de datos biométricos (61) en el medio individual (20) y la primera porción de datos biométricos (60) en el archivo de base de datos (7) y crear una clave de información biométrica (66-1) a partir de los datos biométricos combinados y que ejecute el paso de comparar la clave de información biométrica (66) leída del medio individual (20) con la clave de información biométrica creada (66-1); y

un paso de hacer que un módulo de control de verificación (38) ejecute el paso de verificar los datos biométricos combinados contra datos biométricos obtenidos del dispositivo de detección (1) y realizar autenticación individual.

17. El método de autenticación biométrica según la reivindicación 16, incluyendo además:

un paso de hacer que el módulo de control de gestión de datos biométricos (36) ejecute el paso de dividir los datos biométricos detectados por el dispositivo de detección (1), ejecute el paso de registrar la primera porción de datos biométricos (60) resultante de la división en el archivo de base de datos (7), y ejecute el paso de escribir la segunda porción de datos biométricos (61) resultante de la división y la clave de información biométrica (66) en el medio individual (20); y

un paso de hacer que un módulo de control de registro (32) ejecute el paso de operar el dispositivo de detección (1), adquirir los datos biométricos, y pasar los datos al módulo de control de gestión de datos biométricos (36).

18. El método de autenticación biométrica según cualquiera de las reivindicaciones 11 a 17, donde el paso de detección incluye un paso de detectar una imagen de vasos sanguíneos usando un dispositivo para detección de imágenes de vasos sanguíneos en el cuerpo.

19. El método de autenticación biométrica según la reivindicación 18, donde el paso de detección incluye un paso de detectar una imagen de vasos sanguíneos usando una unidad de captura de imagen para capturar imágenes de vasos sanguíneos en una mano del cuerpo.

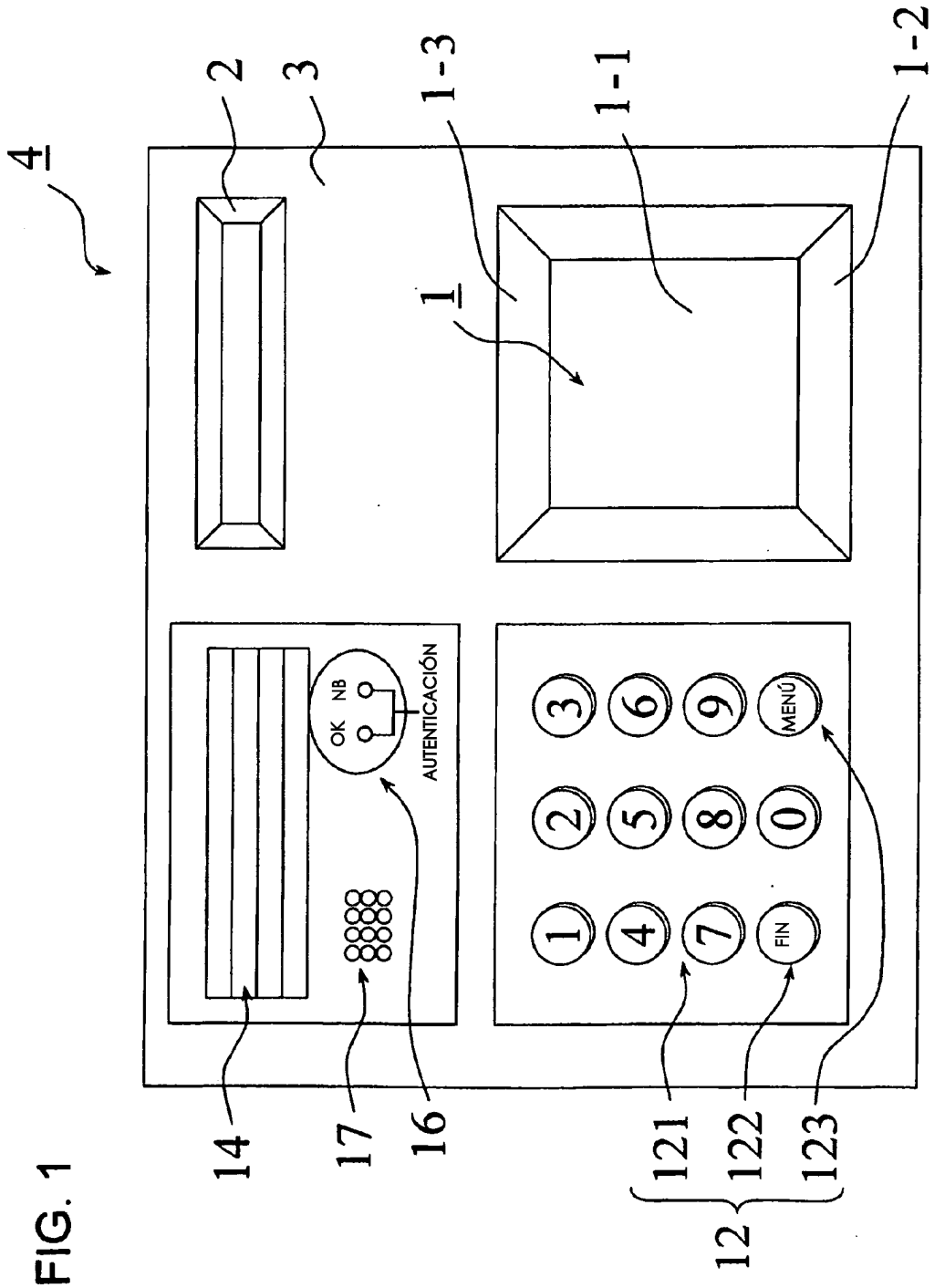
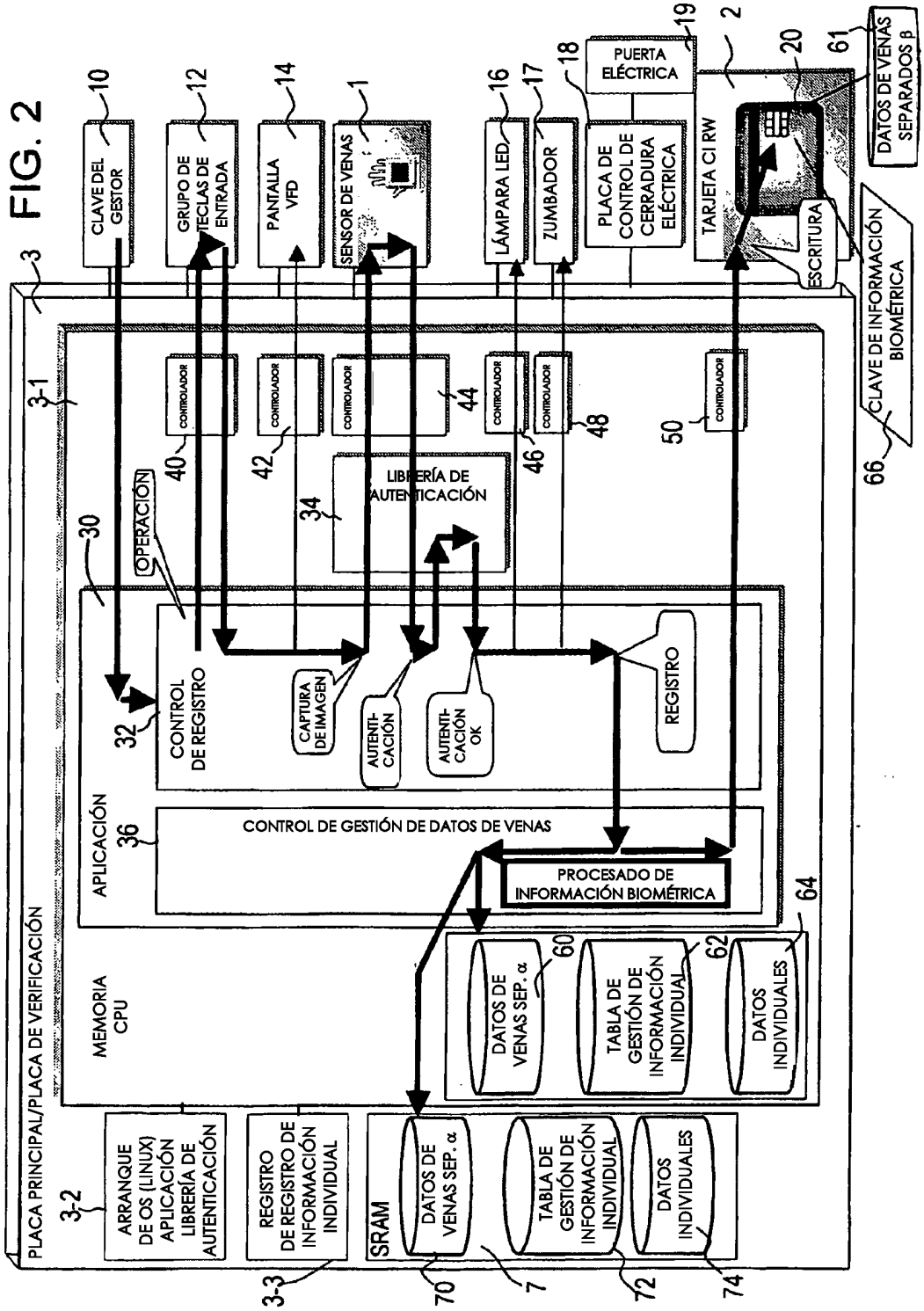

4
2
3
1-3
1-1
1-2
1
OK
NB
AUTENTICACIÓN
1
2
3
4
5
6
7
8
9
0
FIN
MENÚ
14
17
16
121
122
123
12

FIG. 1

FIG. 2


PLACA PRINCIPAL/PLACA DE VERIFICACIÓN
3
3-1
3-2
3-3
CLAVE DEL GESTOR
10
GRUPO DE TECLAS DE ENTRADA
12
PANTALLA VFD
14
SENSOR DE VENAS
1
LÁMPARA LED
16
ZUMBADOR
17
PUERTA ELÉCTRICA
18
19
PLACA DE CONTROL DE CERRADURA ELÉCTRICA
TARJETA CI RW
2
20
ESCRITURA
DATOS DE VENAS SEPARADOS β
61
CLAVE DE INFORMACIÓN BIOMÉTRICA
66
CONTROLADOR
40
42
44
46
48
50
LIBRERÍA DE AUTENTICACIÓN
34
OPERACIÓN
30
APLICACIÓN
36
CONTROL DE REGISTRO
32
CAPTURA DE IMAGEN
AUTENTI-CACIÓN
AUTENTI-CACIÓN OK
REGISTRO
CONTROL DE GESTIÓN DE DATOS DE VENAS
PROCESADO DE INFORMACIÓN BIOMÉTRICA
64
MEMORIA CPU
DATOS DE VENAS SEP. α
60
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
62
DATOS INDIVIDUALES
ARRANQUE DE OS (LINUX) APLICACIÓN LIBRERÍA DE AUTENTICACIÓN
REGISTRO DE REGISTRO DE INFORMACIÓN INDIVIDUAL
SRAM
DATOS DE VENAS SEP. α
70
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
7
DATOS INDIVIDUALES
72
74

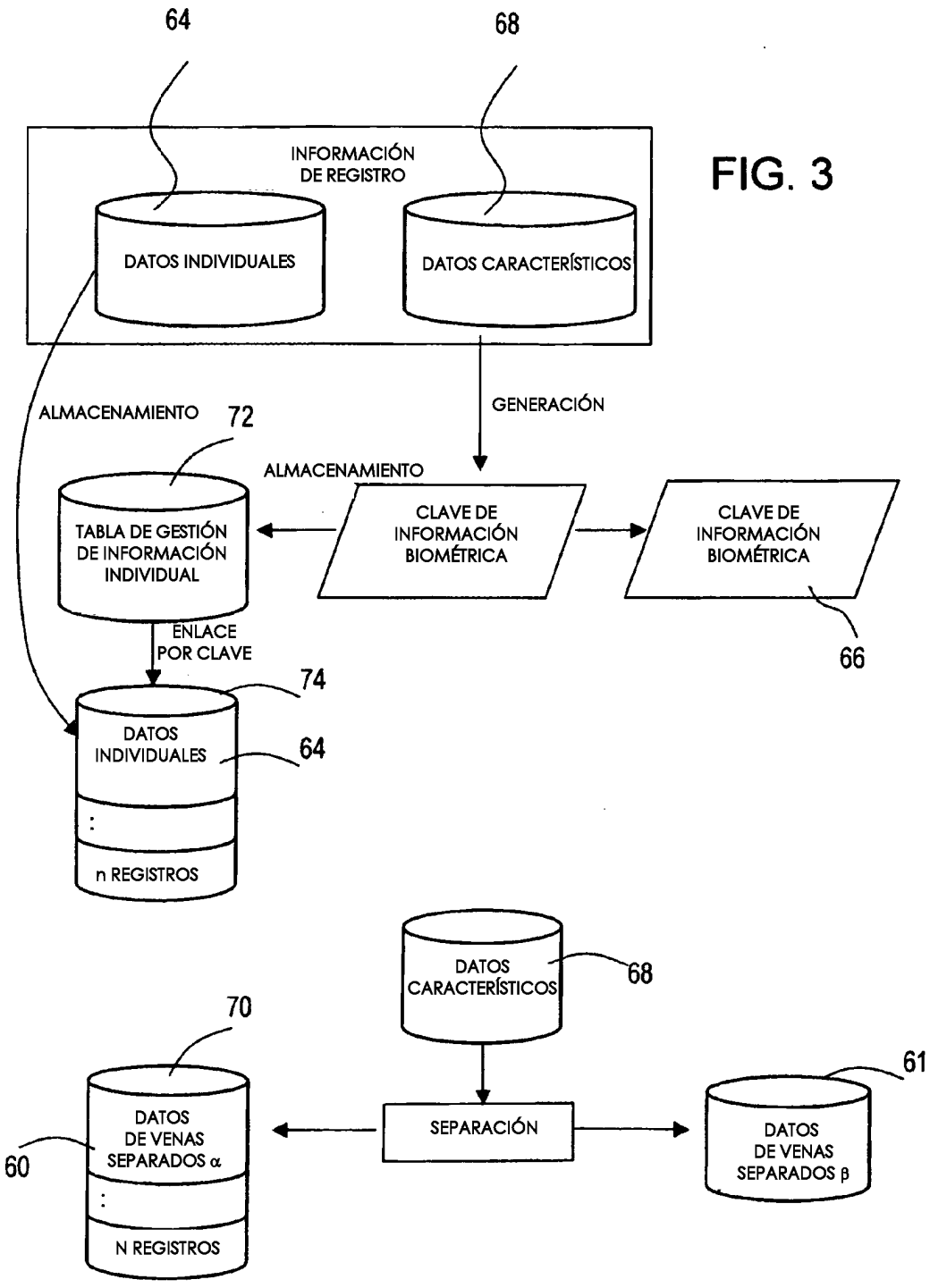

64
68
INFORMACIÓN DE REGISTRO
DATOS INDIVIDUALES
DATOS CARACTERÍSTICOS
ALMACENAMIENTO
72
GENERACIÓN
ALMACENAMIENTO
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
CLAVE DE INFORMACIÓN BIOMÉTRICA
CLAVE DE INFORMACIÓN BIOMÉTRICA
66
ENLACE POR CLAVE
74
DATOS INDIVIDUALES
64
:
n REGISTROS
DATOS CARACTERÍSTICOS
68
70
61
DATOS DE VENAS SEPARADOS α
60
SEPARACIÓN
DATOS DE VENAS SEPARADOS β
:
N REGISTROS

FIG. 3

FIG. 4

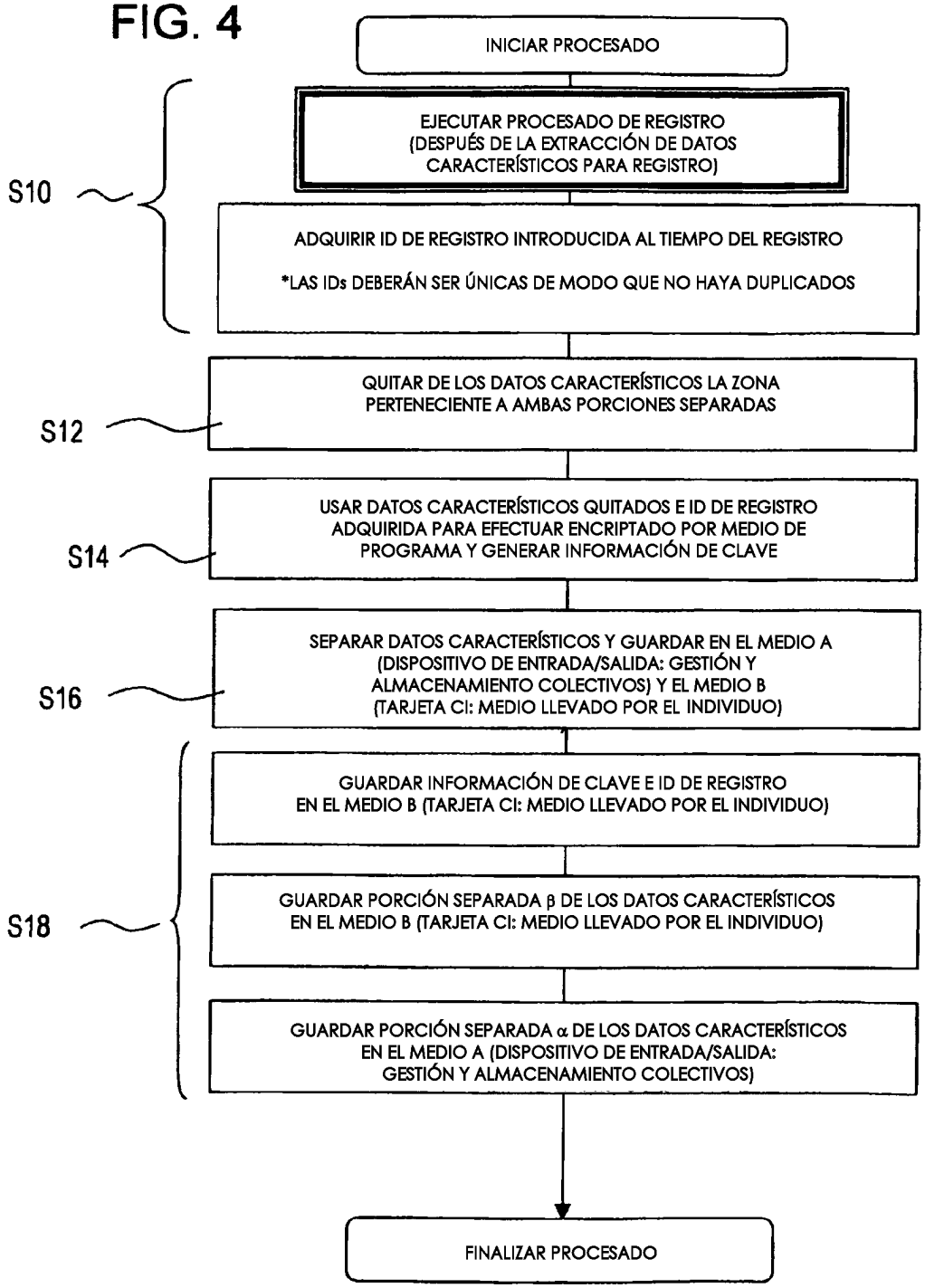

INICIAR PROCESADO
EJECUTAR PROCESADO DE REGISTRO (DESPUÉS DE LA EXTRACCIÓN DE DATOS CARACTERÍSTICOS PARA REGISTRO)
S10
ADQUIRIR ID DE REGISTRO INTRODUCIDA AL TIEMPO DEL REGISTRO
*LAS IDs DEBERÁN SER ÚNICAS DE MODO QUE NO HAYA DUPLICADOS
QUITAR DE LOS DATOS CARACTERÍSTICOS LA ZONA PERTENECIENTE A AMBAS PORCIONES SEPARADAS
S12
USAR DATOS CARACTERÍSTICOS QUITADOS E ID DE REGISTRO ADQUIRIDA PARA EFECTUAR ENCRIPTADO POR MEDIO DE PROGRAMA Y GENERAR INFORMACIÓN DE CLAVE
S14
SEPARAR DATOS CARACTERÍSTICOS Y GUARDAR EN EL MEDIO A (DISPOSITIVO DE ENTRADA/SALIDA: GESTIÓN Y ALMACENAMIENTO COLECTIVOS) Y EL MEDIO B (TARJETA CI: MEDIO LLEVADO POR EL INDIVIDUO)
S16
GUARDAR INFORMACIÓN DE CLAVE E ID DE REGISTRO EN EL MEDIO B (TARJETA CI: MEDIO LLEVADO POR EL INDIVIDUO)
GUARDAR PORCIÓN SEPARADA β DE LOS DATOS CARACTERÍSTICOS EN EL MEDIO B (TARJETA CI: MEDIO LLEVADO POR EL INDIVIDUO)
S18
GUARDAR PORCIÓN SEPARADA α DE LOS DATOS CARACTERÍSTICOS EN EL MEDIO A (DISPOSITIVO DE ENTRADA/SALIDA: GESTIÓN Y ALMACENAMIENTO COLECTIVOS)
FINALIZAR PROCESADO

FIG. 5

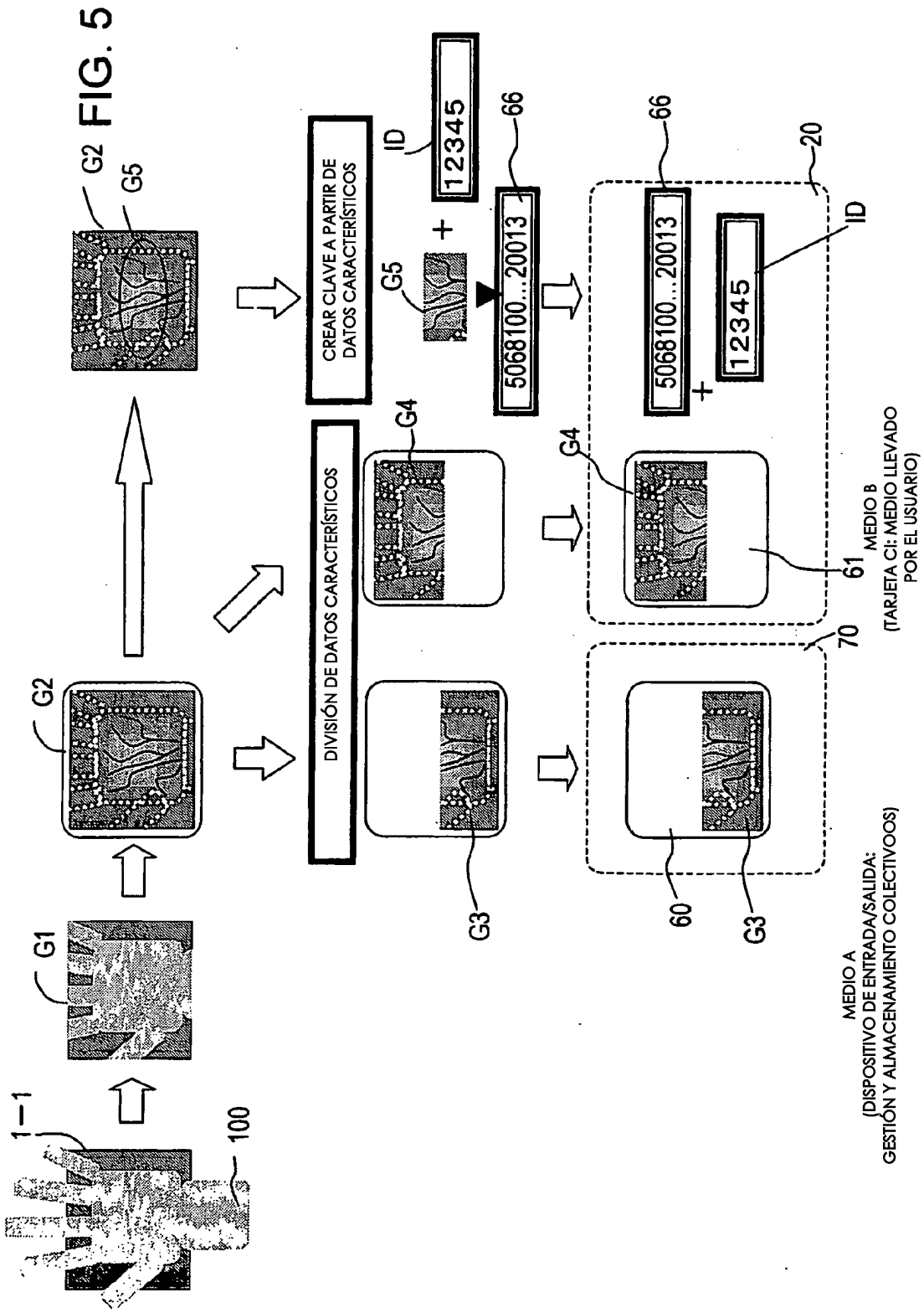

1-1
100
G1
G2
G5
CREAR CLAVE A PARTIR DE DATOS CARACTERÍSTICOS
ID
12345
66
5068100...20013
DIVISIÓN DE DATOS CARACTERÍSTICOS
G4
G3
60
61
70
20
MEDIO A
(DISPOSITIVO DE ENTRADA/SALIDA: GESTIÓN Y ALMACENAMIENTO COLECTIVOOS)
MEDIO B
(TARJETA CI: MEDIO LLEVADO POR EL USUARIO)

FIG. 6

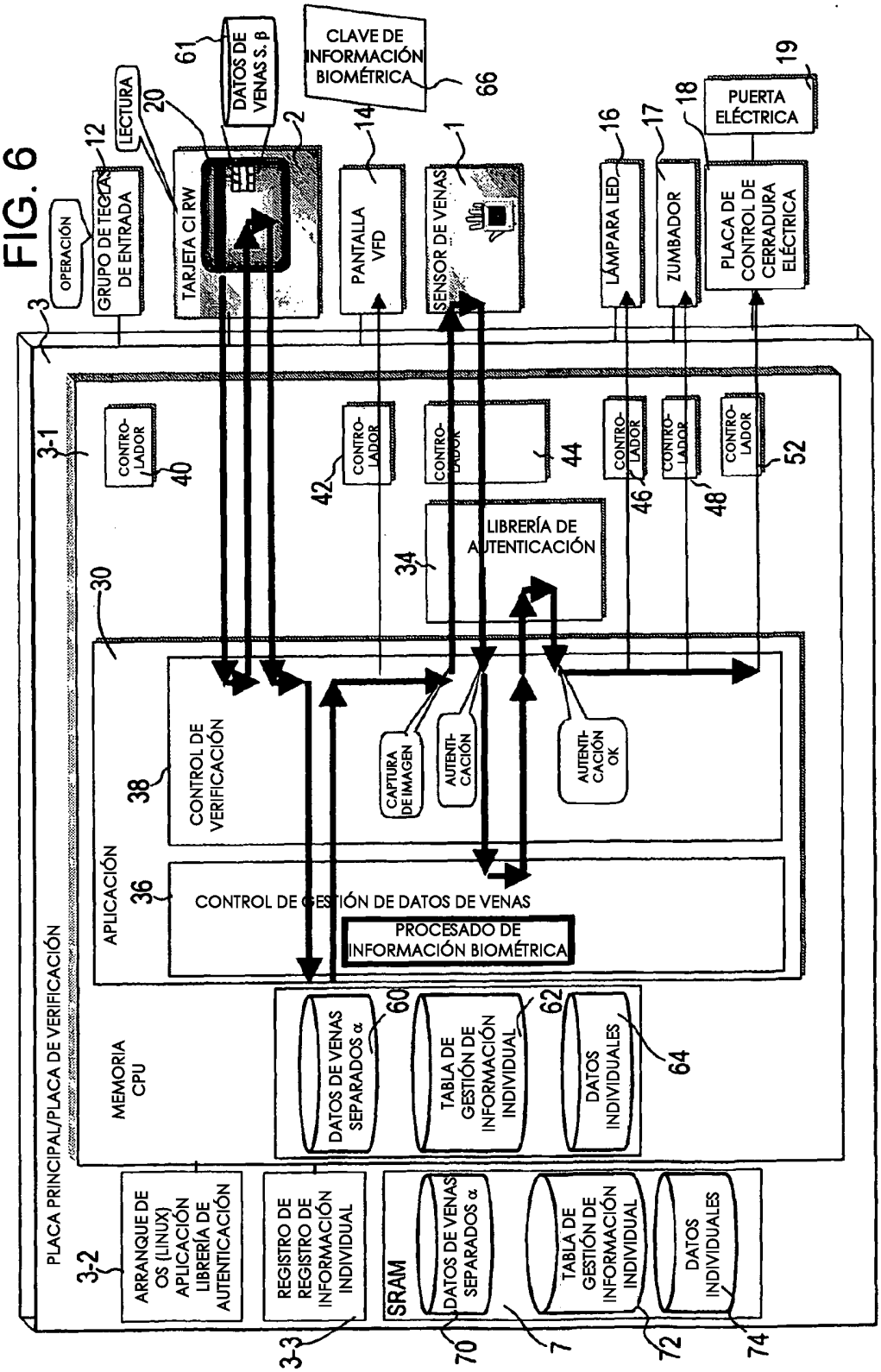

PLACA PRINCIPAL/PLACA DE VERIFICACIÓN
3
3-1
3-2
3-3
OPERACIÓN
GRUPO DE TECLAS DE ENTRADA
12
LECTURA
20
TARJETA CI RW
DATOS DE VENAS S. β
61
2
CLAVE DE INFORMACIÓN BIOMÉTRICA
66
14
PANTALLA VFD
1
SENSOR DE VENAS
16
LÁMPARA LED
17
ZUMBADOR
18
PUERTA ELÉCTRICA
19
PLACA DE CONTROL DE CERRADURA ELÉCTRICA
CONTRO-LADOR
40
42
44
46
48
52
LIBRERÍA DE AUTENTICACIÓN
34
30
APLICACIÓN
CONTROL DE VERIFICACIÓN
38
CAPTURA DE IMAGEN
AUTENTI-CACIÓN
AUTENTI-CACIÓN OK
36
CONTROL DE GESTIÓN DE DATOS DE VENAS
PROCESADO DE INFORMACIÓN BIOMÉTRICA
MEMORIA CPU
DATOS DE VENAS SEPARADOS α
60
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
62
DATOS INDIVIDUALES
64
ARRANQUE DE OS (LINUX) APLICACIÓN LIBRERÍA DE AUTENTICACIÓN
REGISTRO DE REGISTRO DE INFORMACIÓN INDIVIDUAL
SRAM
DATOS DE VENAS SEPARADOS α
70
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
7
72
DATOS INDIVIDUALES
74

FIG. 7

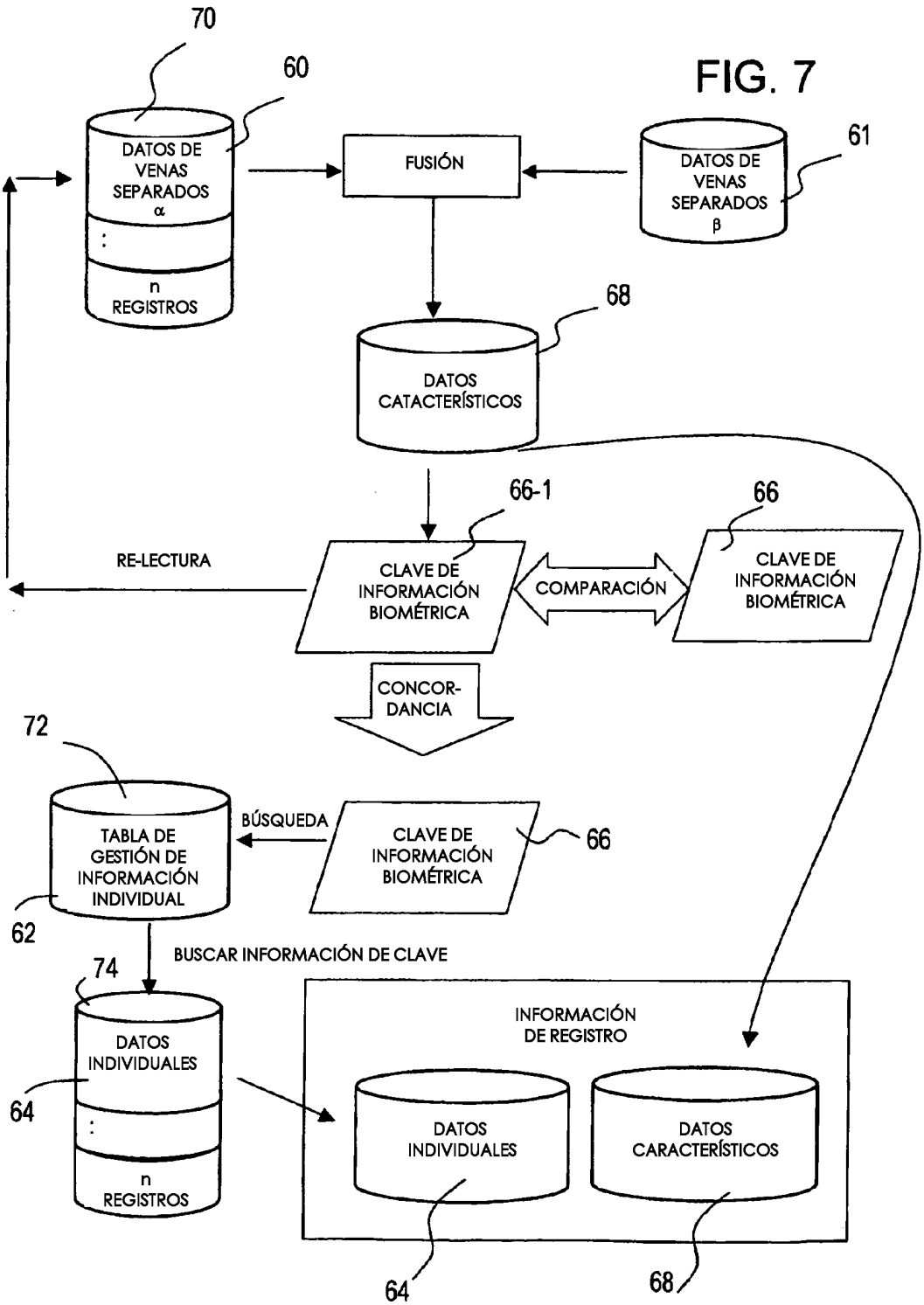

70
60
DATOS DE VENAS SEPARADOS α
:
n REGISTROS
FUSIÓN
61
DATOS DE VENAS SEPARADOS β
68
DATOS CATACTERÍSTICOS
66-1
66
RE-LECTURA
CLAVE DE INFORMACIÓN BIOMÉTRICA
COMPARACIÓN
CLAVE DE INFORMACIÓN BIOMÉTRICA
CONCOR-DANCIA
72
TABLA DE GESTIÓN DE INFORMACIÓN INDIVIDUAL
BÚSQUEDA
CLAVE DE INFORMACIÓN BIOMÉTRICA
66
62
BUSCAR INFORMACIÓN DE CLAVE
74
DATOS INDIVIDUALES
64
:
n REGISTROS
INFORMACIÓN DE REGISTRO
DATOS INDIVIDUALES
DATOS CARACTERÍSTICOS
64
68

FIG. 8

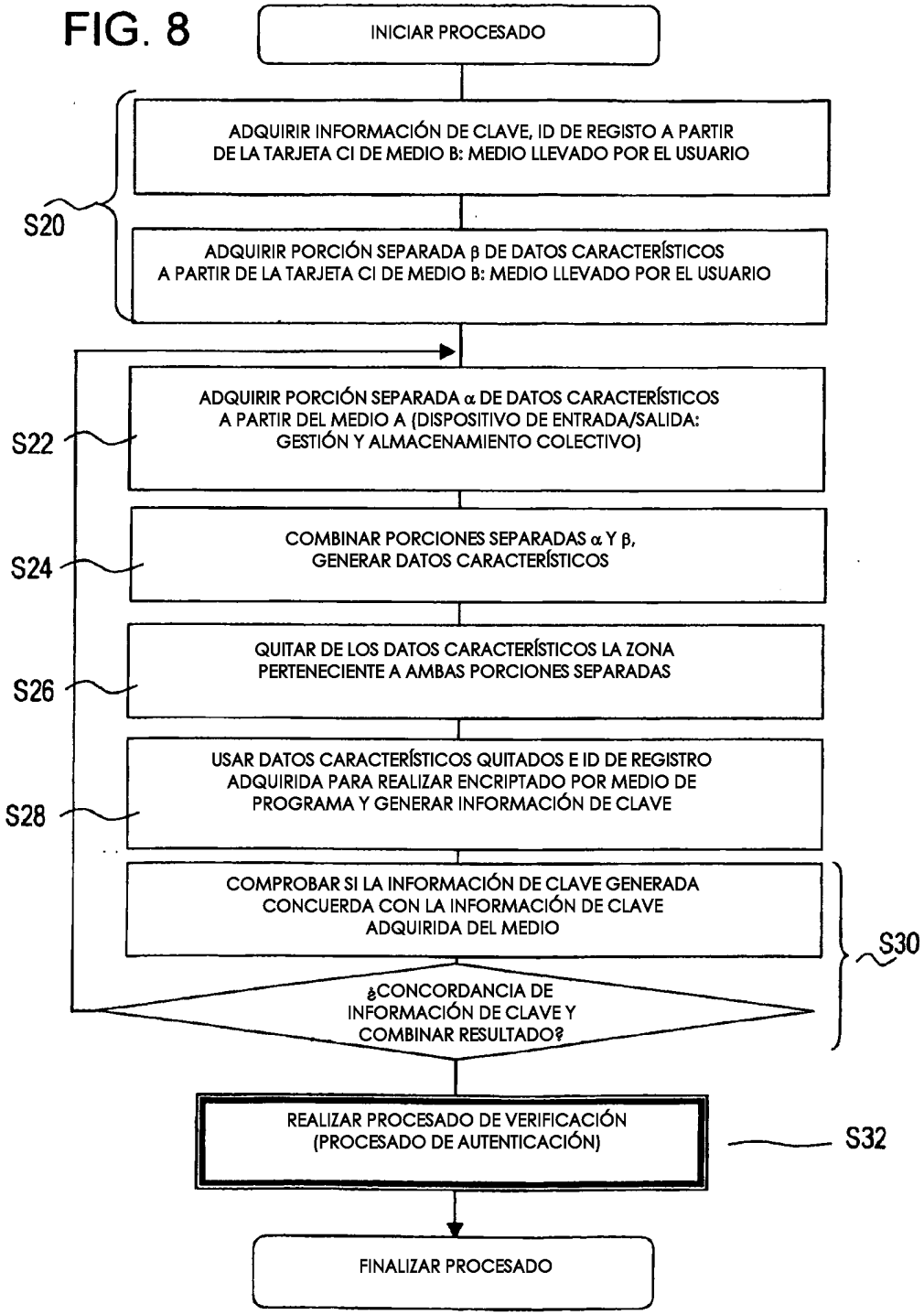
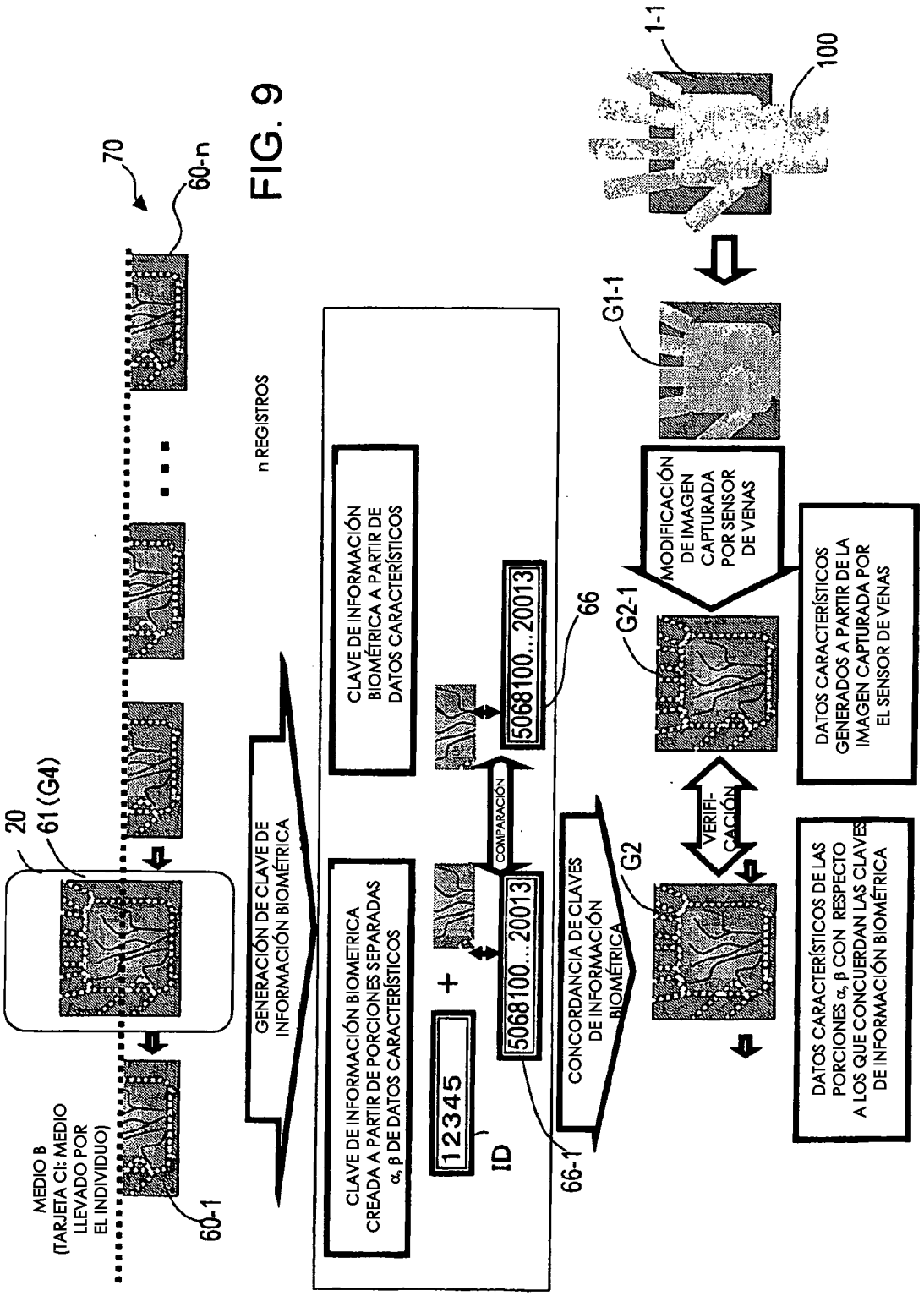

INICIAR PROCESADO
ADQUIRIR INFORMACIÓN DE CLAVE, ID DE REGISTO A PARTIR DE LA TARJETA CI DE MEDIO B: MEDIO LLEVADO POR EL USUARIO
S20
ADQUIRIR PORCIÓN SEPARADA β DE DATOS CARACTERÍSTICOS A PARTIR DE LA TARJETA CI DE MEDIO B: MEDIO LLEVADO POR EL USUARIO
ADQUIRIR PORCIÓN SEPARADA α DE DATOS CARACTERÍSTICOS A PARTIR DEL MEDIO A (DISPOSITIVO DE ENTRADA/SALIDA: GESTIÓN Y ALMACENAMIENTO COLECTIVO)
S22
COMBINAR PORCIONES SEPARADAS α Y β, GENERAR DATOS CARACTERÍSTICOS
S24
QUITAR DE LOS DATOS CARACTERÍSTICOS LA ZONA PERTENECIENTE A AMBAS PORCIONES SEPARADAS
S26
USAR DATOS CARACTERÍSTICOS QUITADOS E ID DE REGISTRO ADQUIRIDA PARA REALIZAR ENCRIPTADO POR MEDIO DE PROGRAMA Y GENERAR INFORMACIÓN DE CLAVE
S28
COMPROBAR SI LA INFORMACIÓN DE CLAVE GENERADA CONCUERDA CON LA INFORMACIÓN DE CLAVE ADQUIRIDA DEL MEDIO
S30
¿CONCORDANCIA DE INFORMACIÓN DE CLAVE Y COMBINAR RESULTADO?
REALIZAR PROCESADO DE VERIFICACIÓN (PROCESADO DE AUTENTICACIÓN)
S32
FINALIZAR PROCESADO

FIG. 9


70
60-n
n REGISTROS
20
61 (G4)
MEDIO B
(TARJETA CI: MEDIO
LLEVADO POR
EL INDIVIDUO)
60-1
GENERACIÓN DE CLAVE DE
INFORMACIÓN BIOMÉTRICA
CLAVE DE INFORMACIÓN BIOMETRICA
CREADA A PARTIR DE PORCIONES SEPARADAS
α, β DE DATOS CARACTERÍSTICOS
CLAVE DE INFORMACIÓN
BIOMÉTRICA A PARTIR DE
DATOS CARACTERÍSTICOS
12345
ID
+
COMPARACIÓN
5068100...20013
5068100...20013
66
66-1
CONCORDANCIA DE CLAVES
DE INFORMACIÓN
BIOMÉTRICA
G2
VERIFI-
CACIÓN
G2-1
MODIFICACIÓN
DE IMAGEN
CAPTURADA
POR SENSOR
DE VENAS
G1-1
1-1
100
DATOS CARACTERÍSTICOS
GENERADOS A PARTIR DE LA
IMAGEN CAPTURADA POR
EL SENSOR DE VENAS
DATOS CARACTERÍSTICOS DE LAS
PORCIONES α, β CON RESPECTO
A LOS QUE CONCUERDAN LAS CLAVES
DE INFORMACIÓN BIOMÉTRICA