(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 993 502**

(51) Int. Cl.:

G06F 21/32 (2013.01)
G06F 21/74 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.02.2015 E 21207849 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.10.2024 EP 4009204**

(54) Título: **Procedimiento y aparato para procesar información biométrica en un dispositivo electrónico**

(30) Prioridad:

19.02.2014 KR 20140019226

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.01.2025

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.00%)
129, Samsung-roYeongtong-gu, Suwon-si
Gyeonggi-do, 443-742, KR

(72) Inventor/es:

AN, TEAIN;
KIM, TAEHO;
KIM, HYUNGJOON;
PARK, SEULHAN;
PARK, JONGHOON;
YOU, HEEJUN;
LEE, YANGSOO;
CHANG, MOONSU y
HYEON, JINHO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y aparato para procesar información biométrica en un dispositivo electrónico

Campo técnico

La presente divulgación se refiere a dispositivos electrónicos para procesar información biométrica.

Antecedente

Con el desarrollo de la tecnología de hardware y software, los dispositivos electrónicos, como los divulgados p. ej. en los documentos US 2009/0315675 A1, US 2012/0117381 A1 y WO 2012/167352 A1, son ahora capaces de controlar y soportar una variedad de funciones. Por ejemplo, un dispositivo electrónico puede estar equipado con una función biométrica que reconoce la biometría de un individuo para su uso en sistemas de seguridad o autenticación. En la implementación, se realiza una función biométrica para autenticar a un usuario comparando los datos de entrada del usuario con los datos almacenados en el sistema de autenticación, por ejemplo, utilizando una característica personal y/o inherente al cuerpo (por ejemplo, huella dactilar, cara, iris, voz, líneas de la palma de la mano, patrones de venas, etc.).

En los últimos años, se han incrementado los casos en los que la información personal de un usuario era frecuentemente divulgada a partir de sus dispositivos electrónicos por programas de piratería informática. Por lo tanto, los dispositivos electrónicos necesitan sistemas que puedan evitar que la información biométrica inherente y/o personal de un usuario sea divulgada por piratería informática con intenciones maliciosas, etc. En este sentido, se han realizado estudios sobre el rendimiento de la seguridad y la fiabilidad de los procedimientos biométricos de acuerdo con los sistemas de seguridad, los sistemas de autenticación o las aplicaciones.

La información anterior se presenta como información de antecedente sólo para ayudar a la comprensión de la presente divulgación. No se ha determinado, ni se ha hecho ninguna afirmación, si alguno de los anteriores podría ser aplicable como técnica anterior con respecto a la presente divulgación.

Sumario

Los aspectos de la presente divulgación abordarán al menos los problemas y/o desventajas mencionados anteriormente y proporcionarán al menos las ventajas descritas a continuación. En consecuencia, un aspecto de la presente divulgación es proporcionar un aparato para procesar y proteger la información biométrica cuando se realiza una función biométrica y la autenticación del usuario mediante el uso de su información biométrica.

Según un aspecto de la presente divulgación, que no es parte de la invención reivindicada, pero es útil para su comprensión, se proporciona un procedimiento para procesar información biométrica en un dispositivo electrónico que incluye un procesador que controla en modo normal o de seguridad. El procedimiento incluye detectar un evento de entrada biométrica de un módulo de sensor biométrico en el modo normal, en respuesta al evento de entrada biométrica, crear datos biométricos basándose en datos captados por el módulo de sensor biométrico en el modo de seguridad, llevar a cabo el registro biométrico o la autenticación biométrica basándose en los datos biométricos creados en el modo de seguridad, proporcionar información del resultado del registro biométrico o la autenticación biométrica en el modo normal.

La invención viene definida solo por el alcance de las reivindicaciones adjuntas.

Breve descripción de los dibujos

Los anteriores y otros aspectos, características, y ventajas de determinadas realizaciones de la presente divulgación serán más evidentes a partir de la siguiente descripción tomada en conjunto con los dibujos adjuntos, en los cuales:

la Figura 1 es un diagrama de bloques esquemático de un procesador de un dispositivo electrónico, de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 2 es un diagrama de bloques esquemático de un dispositivo electrónico, de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 3 es un diagrama de bloques esquemático de un módulo de procesamiento de información biométrica de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 4 es un diagrama de flujo que describe un procedimiento para registrar información biométrica en un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 5 es un diagrama de flujo que describe un procedimiento para autenticar información biométrica en un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 6 es un diagrama de flujo que describe un procedimiento para procesar información biométrica en un

dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 7 ilustra un entorno de red que incluye dispositivos electrónicos de acuerdo con diversas realizaciones de la presente divulgación;

la Figura 8 es un diagrama de bloques de un dispositivo electrónico, de acuerdo con diversas realizaciones de la presente divulgación.

A lo largo de los dibujos, cabe señalar que se utilizan números de referencia similares para representar elementos, características, y estructuras iguales o similares.

Descripción detallada

La siguiente descripción, con referencia a los dibujos adjuntos, se proporciona para ayudar a una comprensión completa de diversas realizaciones de la presente divulgación, tal como se define en las reivindicaciones. Incluye varios detalles específicos para ayudar a esa comprensión, pero deben considerarse simplemente ejemplares. En consecuencia, los expertos en la técnica reconocerán que se pueden realizar diversos cambios y modificaciones de las diversas realizaciones descritas en la presente memoria sin apartarse del ámbito de la presente divulgación. Además, las descripciones de funciones y construcciones bien conocidas pueden omitirse por propósitos de claridad y concisión.

Los términos y palabras utilizados en la siguiente descripción y en las reivindicaciones no se limitan a los significados bibliográficos, ya que son simplemente utilizados por el inventor para permitir una comprensión clara y coherente de la presente divulgación. En consecuencia, debería ser evidente para los expertos en la técnica que la siguiente descripción de diversas realizaciones de la presente divulgación se proporciona con fines ilustrativos solamente y no con el propósito de limitar la presente divulgación como se define en las reivindicaciones adjuntas.

Debe entenderse que las formas singulares “un”, “una” y “el/la” incluyen referentes plurales a menos que el contexto dicte claramente lo contrario. Por lo tanto, por ejemplo, la referencia a “una superficie de componente” incluye la referencia a una o más de tales superficies.

Se entenderá que las expresiones “comprende” y “puede comprender” se utilizan para especificar la presencia de una función, operación, componente, etc. divulgados, pero no excluyen la presencia de una o más funciones, operaciones, componentes, etc. Se entenderá además que los términos “comprende” y/o “tiene”, cuando se utilizan en la presente memoria descriptiva, especifican la presencia de una característica declarada, número, etapa, operación, componente, elemento, o una combinación de estos, pero no excluyen la presencia o adición de una o más características, números, etapas, operaciones, componentes, elementos, o combinaciones de estos.

En la presente divulgación, la expresión “y/o” se toma como una divulgación específica de cada una y cualquier combinación de cosas enumeradas. Por ejemplo, A y/o B deben tomarse como una divulgación específica de cada uno de A, B, y A y B.

Tal y como se utiliza en la presente memoria, términos tales como “primero”, “segundo”, etc. se utilizan para describir varios componentes, pero no restringen los componentes correspondientes. Sin embargo, es evidente que los componentes no deben definirse con estos términos. Los términos se utilizan únicamente para distinguir un componente de otro. Por ejemplo, un primer componente puede ser referido como un segundo componente y, del mismo modo, un segundo componente también puede ser referido como un primer componente, sin apartarse de la enseñanza del concepto inventivo.

Se entenderá que cuando se hace referencia a un elemento o capa como “sobre”, “conectado a” o “acoplado a” otro elemento o capa, puede estar directamente sobre, conectado o acoplado al otro elemento o capa o pueden estar presentes elementos o capas intermedias. En cambio, cuando se hace referencia a que un elemento está “directamente sobre”, “directamente conectado a” o “directamente acoplado a” otro elemento o capa, no hay presentes elementos o capas intermedias.

La terminología utilizada en la presente memoria tiene por propósito describir únicamente realizaciones particulares y no pretende limitar la divulgación. Tal y como se utiliza en la presente memoria, las formas singulares tienen la intención de incluir las formas plurales también, a menos que el contexto indique claramente lo contrario.

A menos que se defina de otro modo, todos los términos utilizados en la presente memoria tienen el mismo significado que se entiende comúnmente por un experto en la técnica a la cual pertenece la presente divulgación, y no debe interpretarse que tienen un significado excesivamente amplio ni que tenga un significado excesivamente contraído. Los términos generales utilizados en la presente memoria deben interpretarse de acuerdo con las definiciones del diccionario o en el contexto y no deben interpretarse como un significado excesivamente contraído.

En la siguiente descripción, un “dispositivo electrónico” puede ser un dispositivo que tenga una función de comunicación. Por ejemplo, un dispositivo electrónico puede incluir al menos uno de un teléfono inteligente, un ordenador personal (PC) tipo tableta, un teléfono móvil, un teléfono de vídeo, un lector de libros electrónicos (ebook),

un PC de escritorio, un PC portátil, un PC ultra portátil, un Asistente Personal Digital (PDA), un Reproductor Multimedia Portátil (PMP), un Reproductor MP3, un aparato médico móvil, una cámara, o un dispositivo portátil (por ejemplo, un dispositivo montado en la cabeza (HMD) tal como gafas electrónicas), ropa electrónica, una pulsera electrónica, un collar electrónico, un accesorio, un tatuaje electrónico, y un reloj inteligente).

De acuerdo con diversas realizaciones, los ejemplos del dispositivo electrónico pueden ser un electrodoméstico inteligente que tenga una función de comunicación. Los ejemplos de electrodomésticos inteligentes pueden incluir al menos uno de un televisor, un Reproductor de Discos de vídeo Digital (DVD), un Reproductor de Audio, un refrigerador, un aparato de aire acondicionado, un limpiador, un horno, un horno microondas, una máquina de lavado, un limpiador de aire, un decodificador, un aparato de televisión (por ejemplo, Samsung HomeSyncTM, Apple TVTM, y Google TVTM), una consola de juegos, un diccionario electrónico, una tecla electrónica, una videocámara, y un marco de fotos electrónico.

De acuerdo con diversas realizaciones, los ejemplos del dispositivo electrónico pueden incluir al menos uno de un aparato médico (por ejemplo, una Angiografía por Resonancia Magnética (ARM), una Imagen por Resonancia Magnética (IRM), una Tomografía Computarizada (TC), una cámara, y un dispositivo ultrasónico), un dispositivo de navegación, un Receptor del Sistema de Posicionamiento Global (GPS), un Registrador de Datos de Eventos (EDR), un Registrador de Datos de Vuelo (FDR), un dispositivo de infoentretenimiento para automóviles, un equipo electrónico para un barco (por ejemplo, un dispositivo de navegación marina y un girocompás), un dispositivo de aviónica, un dispositivo de seguridad, una Visualización Cabeza Arriba (HUD), un robot industrial o doméstico, un Cajero Automático (ATM) de una entidad financiera, y un Punto de Ventas (POS).

De acuerdo con diversas realizaciones, los ejemplos del dispositivo electrónico pueden incluir muebles o una parte de un edificio/construcción el cual tenga una función de comunicación, un tablero electrónico, un dispositivo de recepción de firmas electrónicas, un proyector, y un dispositivo de medición (por ejemplo, dispositivos de medición de agua, electricidad, y ondas eléctricas). De acuerdo con una realización, el dispositivo electrónico puede ser uno o cualquier combinación de los dispositivos enumerados anteriormente. De acuerdo con una realización, el dispositivo electrónico puede ser un dispositivo flexible. Sin embargo, es obvio para los expertos en la técnica que el dispositivo electrónico de la presente divulgación no se limita a los dispositivos anteriores.

Se hace una descripción de un dispositivo electrónico de acuerdo con diversas realizaciones con referencia a los dibujos que se acompañan a continuación. En la descripción de las diversas realizaciones, el término "usuario" puede denotar una el cual que utiliza el dispositivo electrónico.

La Figura 1 es un diagrama de bloques esquemático de un procesador de un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación

Con referencia a la Figura 1, el dispositivo 101 electrónico puede funcionar en un modo normal o en modo seguro. El dispositivo 101 electrónico puede incluir un procesador 120 que funciona dividiendo un núcleo en dos núcleos virtuales. Por ejemplo, el procesador 120 puede funcionar un SO (sistema operativo) normal utilizando un núcleo 111 virtual normal en un modo normal (por ejemplo, Entorno de Ejecución Enriquecido, mundo normal, etc.) y funcionar un SO virtual utilizando un núcleo 112 virtual seguro en un modo seguro (por ejemplo, Entorno de Ejecución de Confianza, mundo seguro, etc.).

El procesador 120 puede llamar al SO normal o al SO virtual a través de un controlador de kernel (no se muestra). El procesador 120 puede conmutar entre el modo normal que funciona en el SO normal y el modo seguro que funciona en el SO virtual.

El dispositivo 101 electrónico puede incluir una memoria 130 que tiene una zona 131 normal, una zona 132 segura, y una zona 133 compartida. La zona 131 normal puede almacenar datos e instrucciones de tareas relacionadas con el núcleo 111 virtual normal. La zona 131 normal puede incluir programas de software o módulos de programa (por ejemplo, una aplicación biométrica, un módulo de control de reconocimiento biométrico, etc.) que funcionan mediante el uso del núcleo 111 virtual normal. Por ejemplo, el procesador 120 que funciona mediante el uso del núcleo 111 virtual normal puede controlar los programas de software o los módulos de programa de la zona 131 normal sin limitación de acceso.

En la memoria 130 del dispositivo 101 electrónico, la zona 132 segura puede almacenar datos e instrucciones de tareas relacionadas con el núcleo 112 virtual seguro. La zona 132 segura puede incluir programas de software o módulos de programa (por ejemplo, un módulo de procesamiento biométrico, un módulo de control de canal, etc.) que funcionan mediante el uso del núcleo 112 virtual seguro. Por ejemplo, el procesador 120 que funciona mediante el uso del núcleo 112 virtual seguro puede controlar los programas de software o los módulos de programa de la zona 132 segura con limitación de acceso. Se puede acceder a la zona 132 segura mediante señales con acceso de seguridad, autorización, y/o fiabilidad.

La zona 131 normal y la zona 132 segura pueden formar parte de la memoria 130. La zona 133 compartida que almacena datos e instrucciones para permitir que el núcleo 111 virtual normal y el núcleo 112 virtual seguro se accedan mutuamente cuando el núcleo 111 virtual normal o el núcleo 112 virtual seguro funcionan. La zona 133 compartida puede gestionar el espacio de direcciones para un sistema operativo almacenado en la memoria 130 e incluir

información de gestión de memoria para la asignación de recursos. La zona 133 compartida puede almacenar información para llamar al SO normal o al SO seguro.

Un módulo 140 de sensor biométrico del dispositivo 101 electrónico puede detectar objetos para reconocimientos biométricos. Los objetos pueden ser el cuerpo de un usuario y/o al menos una parte del cuerpo. Los objetos pueden ser objetos inherentes y/o personales de un individuo que pueden clasificarse física o fisiológicamente, tal como una huella dactilar, un iris, un patrón de retina, un patrón de venas, una forma de oreja, un contorno facial, una voz, una forma de palma, la escritura de un usuario (por ejemplo, su firma), etc.

El módulo 140 de sensor biométrico puede incluir sensores que funcionan en varios tipos de modos de reconocimiento biométrico. Por ejemplo, el módulo 140 de sensor biométrico puede incluir un sensor de huellas dactilares, un sensor de retina, un sensor de iris, un sensor de patrón de venas, etc. El módulo 140 de sensor biométrico también puede incluir una cámara y un sensor óptico tal como un sensor de infrarrojos, etc. para reconocer una cara, un iris, etc., un sensor o un panel táctiles, etc. para detectar la escritura de un usuario, etc. En diversas realizaciones de la presente divulgación, el módulo 140 de sensor biométrico puede recibir datos detectados a partir del exterior del dispositivo 101 electrónico o de un sistema externo separado.

En la siguiente descripción, los componentes del dispositivo 101 electrónico de acuerdo con diversas realizaciones de la presente divulgación se describirán con más detalle refiriéndose a las Figuras 2 y 3.

La Figura 2 es un diagrama de bloques esquemático de un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 2, el dispositivo electrónico (por ejemplo, el dispositivo 101 electrónico de la Figura 1) puede que opere en el modo normal o en el modo seguro.

El dispositivo electrónico puede conmutar mutuamente entre el modo normal y el modo seguro. El dispositivo electrónico realiza tareas en el modo normal utilizando los recursos asignados al núcleo virtual normal. El dispositivo electrónico realiza tareas en el modo seguro utilizando los recursos asignados al núcleo virtual seguro.

En el modo normal, el dispositivo electrónico puede funcionar mediante el SO normal y realizar las siguientes operaciones. El dispositivo electrónico puede controlar las funciones de una interfaz 210 normal de entrada/salida, un módulo 211 de control de reconocimiento biométrico, y una aplicación 212 biométrica, y puede procesar datos. Por ejemplo, el dispositivo electrónico en el modo normal puede detectar si se produce un evento de entrada biométrica (señal) y solicitar (o notificar) para funcionar por el modo seguro en respuesta al evento de entrada biométrica. Por ejemplo, el dispositivo electrónico puede producir una señal de interrupción para el modo seguro y transferir una señal de interrupción a través de un controlador de kernel a partir del SO normal al SO seguro, y puede llamar a un núcleo virtual seguro. El dispositivo electrónico puede cambiar un modo actual al modo seguro. En el modo normal, el dispositivo electrónico puede realizar una operación para proporcionar información del resultado del procesamiento biométrico a una interfaz de usuario.

En el modo seguro, el dispositivo electrónico puede funcionar mediante el SO seguro y realizar las siguientes operaciones. El dispositivo electrónico puede controlar las funciones de una interfaz 220 segura de entrada/salida, un módulo 221 de procesamiento biométrico y un módulo 222 de control de canal, y puede procesar datos. Por ejemplo, en el modo seguro, el dispositivo electrónico puede obtener los datos detectados a partir del módulo 140 de sensor biométrico de acuerdo con una señal de interrupción. El dispositivo electrónico puede crear datos biométricos en base a los datos detectados, y registrar los datos biométricos, o puede comparar los datos biométricos creados con los datos biométricos previamente registrados para la autenticación biométrica. El dispositivo electrónico puede transferir el resultado del procesamiento biométrico utilizando un controlador de kernel (no se muestra), a partir del SO seguro al SO normal. Luego, el dispositivo electrónico puede llamar a un núcleo virtual normal y cambiar el modo seguro al modo normal. El resultado del procesamiento biométrico puede ser una información de tipo verdadero falso (señal). Sin embargo, debe entenderse que la presente divulgación no se limita al tipo de información (señal).

En diversas realizaciones de la presente divulgación, cuando el dispositivo electrónico se hace funcionar por el SO normal, el módulo 140 de sensor biométrico puede detectar objetos para ser reconocidos. Cuando el módulo 140 de sensor biométrico detecta objetos por reconocer, puede transferir una señal de interrupción para notificar la detección de objetos a la interfaz 210 normal de entrada/salida.

En el modo normal, el dispositivo electrónico puede conmutar a partir del SO normal al SO seguro en respuesta a la señal de interrupción. Por ejemplo, la señal de interrupción puede ser una señal de interrupción segura, tal como una señal con un acceso o autorización segura, etc.

En el modo seguro, el dispositivo electrónico puede obtener datos detectados a partir del módulo 140 de sensor biométrico a través de la interfaz 220 de entrada/salida segura. Los datos detectados pueden ser datos sin procesar adquiridos por el módulo 140 de sensor biométrico, sin ser sometidos a procesamiento.

En el modo seguro, el dispositivo electrónico puede transferir los datos detectados al módulo 221 de procesamiento biométrico a través de la interfaz 220 de entrada/salida segura. El módulo 221 de procesamiento biométrico para un

registro biométrico puede crear datos biométricos en base a los datos detectados, y registrar los datos biométricos como datos de registro. El módulo 221 de procesamiento biométrico para una autenticación biométrica también puede realizar una autenticación biométrica. Por ejemplo, el módulo 221 de procesamiento biométrico puede calcular las características de un objeto reconocido a partir de los datos detectados. El módulo 221 de procesamiento biométrico puede convertir las características en una forma de plantilla para crear datos biométricos y puede almacenar los datos biométricos creados. El módulo 221 de procesamiento biométrico puede comparar los datos de registro, almacenados en la memoria, con los datos biométricos, entrada que se utilizará para la autenticación, y determinar un resultado de autenticación. El módulo 221 de procesamiento biométrico puede transferir el resultado del resultado del registro biométrico o de la autenticación biométrica a la interfaz 220 de entrada/salida segura.

En diversas realizaciones de la presente divulgación, el módulo 221 de procesamiento biométrico puede crear una tecla única en base a un identificador de dispositivo único (por ejemplo, el identificador único del circuito integrado auxiliar, etc.), y puede cifrar o descifrar los datos biométricos utilizando la tecla única.

En diversas realizaciones de la presente divulgación, el módulo 221 de procesamiento biométrico puede crear pseudodatos mediante el uso de una función unidireccional, un cambio de conjunto de datos, etc., y puede realizar la autenticación biométrica utilizando los pseudodatos. En ese caso, los datos biométricos en base a los datos detectados pueden cifrarse y almacenarse en la zona segura, y los pseudodatos pueden almacenarse en la zona normal.

En diversas realizaciones de la presente divulgación, el módulo 222 de control de canal puede realizar el control de la conexión para ser mutuamente compatible con el SO normal o el SO virtual, y también puede establecer canales seguros para otros dispositivos electrónicos (por ejemplo, servidores, etc.). El módulo 222 de control de canal puede realizar el control de la conexión para ser mutuamente compatible con varios entornos de ejecución seguros (por ejemplo, SO seguro) que funcionan en el modo seguro. El módulo 222 de control de canal puede configurar la información biométrica, extraída para diversos usos de la información biométrica, tal como el pago, el inicio de sesión, etc., en un único mensaje biométrico (por ejemplo, un mensaje de información), y puede establecer un canal seguro para transmitir el mensaje a otro dispositivo electrónico (por ejemplo, un servidor, etc.). El módulo 222 de control de canal puede establecer canales seguros con otro dispositivo electrónico, cifrados por una tecla creada en base al identificador de dispositivo único preestablecido.

En el modo seguro, el dispositivo electrónico puede transferir (o notificar) una información del resultado (por ejemplo, señal del resultado) del registro biométrico o de la autenticación biométrica a la interfaz 210 normal de entrada/salida a través de la interfaz 220 de entrada/salida segura. El dispositivo electrónico puede conmutar el modo actual al modo normal, en respuesta al resultado.

En el modo normal, el dispositivo electrónico puede recibir la información del resultado a través de la interfaz 210 normal de entrada/salida y puede transferirla al módulo 211 de control de reconocimiento biométrico.

El módulo 211 de control de reconocimiento biométrico puede proporcionar la información del resultado del registro biométrico o de la autenticación biométrica al usuario a través de la aplicación 212 biométrica. El módulo 211 de control de reconocimiento biométrico puede controlar la aplicación 212 biométrica para que realice las funciones de acuerdo con la información del resultado.

En diversas realizaciones de la presente divulgación, cuando el módulo 211 de control de reconocimiento biométrico determina que la autenticación biométrica es exitosa, puede hacer funcionar una aplicación preestablecida o realizar una función preestablecida, en respuesta al evento de éxito de la autenticación. Por ejemplo, cuando la autenticación biométrica es exitosa, el módulo 211 de control de reconocimiento biométrico puede desbloquear el estado de bloqueo de pantalla o puede permitir el acceso a una aplicación que requiera la autenticación del usuario.

La aplicación 212 biométrica puede acompañar a una autenticación biométrica. La autenticación biométrica puede ser programada de modo que la aplicación pueda realizar la autenticación biométrica. La autenticación biométrica puede ser soportada por aplicaciones separadas para soportar la autenticación biométrica, SOs, plataformas, o funciones para controlar/gestionar los dispositivos electrónicos.

La Figura 3 es un diagrama de bloques esquemático de un módulo de procesamiento biométrico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 3, el módulo 221 de procesamiento biométrico puede incluir una unidad 310 de creación de datos biométricos, una unidad 320 de coincidencia de datos, y una unidad 330 de procesamiento de seguridad.

La unidad 310 de creación de datos biométricos puede calcular una característica inherente sobre un objeto reconocido, en base a los datos detectados por un módulo de sensor biométrico (por ejemplo, el módulo 140 de sensor biométrico que se muestra en la Figura 2). La unidad 310 de creación de datos biométricos puede transformar la característica inherente calculada en una plantilla biométrica y crear los datos biométricos. La plantilla se crea codificando la información de la imagen biométrica detectada por el sensor. En una realización de la presente divulgación, la unidad 310 de creación de datos biométricos puede obtener una imagen biométrica (por ejemplo, una imagen de huella dactilar, una imagen de patrón de iris, una imagen facial, etc.) a partir de los datos detectados. Por ejemplo, la imagen biométrica puede obtenerse de manera óptica utilizando el principio de reflexión de la luz o de

manera no óptica utilizando presión, calor, una onda ultrasónica, etc. La unidad 310 de creación de datos biométricos puede extraer la característica inherente y/o personal de un individuo, en base a las imágenes biométricas. Por ejemplo, cuando se realiza la autenticación de una huella dactilar, las características para la autenticación de la huella dactilar pueden ser puntos característicos, tal como un extremo de cresta, un punto de bifurcación, un punto de núcleo un punto delta, etc. Con el fin de evaluar en qué medida los datos detectados coinciden con los datos de registro biométrico almacenados, la unidad 310 de creación de datos biométricos puede extraer las características en un formato (o trama) preestablecido. Por ejemplo, el formato preestablecido de las características puede ser una forma de una plantilla.

Al detectar una solicitud para el registro biométrico, la unidad 310 de creación de datos biométricos puede almacenar los datos biométricos creados como datos de registro en la memoria.

Al detectar una solicitud de autenticación biométrica, la unidad 320 de coincidencia de datos puede determinar si los datos biométricos creados de entrada a partir del módulo de sensor biométrico coinciden con los datos de registro almacenados.

En diversas realizaciones de la presente divulgación, la unidad 320 de coincidencia de datos puede comparar el valor característico calculado a partir de los datos biométricos, creados para la autenticación biométrica, con al menos uno de los valores de los datos de registro, y calcular los valores de coincidencia. Los valores de coincidencia pueden mostrar información sobre cuánto coinciden los datos biométricos con los datos de registro.

Por ejemplo, un valor de coincidencia puede ser el número de puntos característicos que coinciden entre los datos biométricos y los datos de registro durante el procedimiento de coincidencia. Un valor de coincidencia puede calcularse utilizando estadísticas o una función de probabilidad, considerando la distancia y la dirección entre los puntos característicos incluidos en los datos biométricos, la similitud en la disposición de los puntos característicos, y/o similares.

La unidad 320 de coincidencia de datos puede determinar si la autenticación biométrica es exitosa en base al valor de coincidencia de la información característica. Cuando la unidad 320 de coincidencia de datos confirma que el valor de coincidencia supera un umbral, concluye que la autenticación biométrica ha tenido éxito. Por el contrario, cuando la unidad 320 de coincidencia de datos confirma que el valor de coincidencia es menor que o igual a un umbral, concluye que la autenticación biométrica ha fallado.

La unidad 320 de coincidencia de datos puede transferir el resultado de la autenticación (por ejemplo, una señal de tipo verdadero falso) a un módulo de control de reconocimiento biométrico (por ejemplo, 211 en la Figura 2) que funciona en el modo normal.

La unidad 330 de procesamiento de seguridad puede cifrar o descifrar los datos biométricos. La unidad 330 de procesamiento de seguridad puede crear una tecla única en base a un identificador de dispositivo único. Por ejemplo, la tecla única puede ser un valor accesible en un modo seguro.

En una realización de la presente divulgación, al realizar el registro biométrico, la unidad 330 de procesamiento de seguridad puede cifrar los datos biométricos utilizando una tecla única y almacenar los datos biométricos cifrados como datos de registro en la zona segura de la memoria. Al realizar la autenticación biométrica, la unidad 330 de procesamiento de seguridad puede obtener los datos de registro cifrados a partir de la zona segura, y descifrarlos utilizando una tecla única. La unidad 330 de procesamiento de seguridad puede transferir los datos de registro descifrados a la unidad de coincidencia de datos. En ese caso, una función para crear una tecla única puede ser un valor creado cuando el procesador se hace funcionar como un SO seguro, y el acceso de la tecla única es limitado cuando el procedimiento se hace funcionar como un SO normal.

En una realización de la presente divulgación, la unidad 330 de procesamiento de seguridad puede cifrar los datos biométricos utilizando una tecla única, y puede transferir los datos biométricos cifrados al módulo de control de reconocimiento biométrico (por ejemplo, el módulo 211 que se muestra en la Figura 2) del modo normal. Al realizar la autenticación biométrica, la unidad 330 de procesamiento de seguridad puede recibir los datos biométricos cifrados a partir del módulo de control de reconocimiento biométrico del modo normal y puede descifrarlos utilizando la tecla única creada a través del SO seguro. La unidad 330 de procesamiento de seguridad puede transferir los datos biométricos descifrados a la unidad de coincidencia de datos.

En una realización de la presente divulgación, la unidad 330 de procesamiento de seguridad puede transformar los datos biométricos en pseudodatos utilizando una función de transformación. La función de transformación puede incluir una función unidireccional, una función de conjunto de datos, etc. La función de transformación puede utilizar una función que utiliza un valor obtenible a partir de un dispositivo de hardware seguro separado o cuando funciona en un modo seguro. La función de transformación puede almacenar los datos biométricos como metadatos.

La unidad 330 de procesamiento de seguridad puede transferir los pseudodatos creados a la unidad 320 de coincidencia de datos y a la unidad 310 de creación de datos biométricos. Por ejemplo, la unidad 330 de procesamiento de seguridad puede almacenar los pseudodatos como datos de registro. La unidad 310 de creación de datos biométricos puede determinar si la autenticación biométrica es exitosa comparando los pseudodatos registrados con los pseudodatos recién creados.

La unidad 330 de procesamiento de seguridad puede gestionar de manera variable una función de transformación para crear pseudodatos. Por ejemplo, cuando los datos biométricos se divulgan involuntariamente, la unidad 330 de procesamiento de seguridad puede cambiar la función de transformación y crear pseudodatos mediante la función de transformación cambiada. Cuando se divulgan los datos biométricos, dado que los metadatos de los datos biométricos se actualizan, la unidad 330 de procesamiento de seguridad puede actualizar o descartar los datos biométricos existentes.

La Figura 4 es un diagrama de flujo que describe un procedimiento para registrar información biométrica en un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 4, un dispositivo electrónico puede detectar un evento de entrada de información biométrica en base a una señal de interrupción transferida a partir de un módulo de sensor biométrico en el modo normal, con el fin de realizar el registro biométrico (por ejemplo, el modo de registro) en la operación 410. Cuando se realiza una solicitud de registro biométrico en el modo normal, el dispositivo electrónico activa el módulo de sensor biométrico para detectar un objeto que debe ser reconocido. Por ejemplo, el dispositivo electrónico puede reconocer el dedo de un usuario en contacto con un sensor de huellas dactilares. El dispositivo electrónico puede reconocer el ojo de un usuario acercándose a un sensor de iris. El dispositivo electrónico puede reconocer la mano de un usuario acercándose a un sensor de venas. El dispositivo electrónico puede reconocer la entrada de voz de un usuario a un sensor de voz. El dispositivo electrónico puede reconocer la cara de un usuario acercándose a un sensor facial.

Después de detectar el evento de entrada biométrica en la operación 410, el dispositivo electrónico puede transferir una señal de evento a un SO seguro para llamar a un núcleo virtual seguro en la operación 420. La señal de evento puede ser una señal de interrupción segura. El dispositivo electrónico puede conmutar a partir del modo normal al modo seguro.

En el modo seguro, el dispositivo electrónico puede obtener datos detectados a través del módulo de sensor biométrico en la operación 430. Los datos detectados pueden ser datos sin procesar de la información biométrica. Por ejemplo, los datos detectados pueden incluir al menos una de las huellas dactilares, las líneas de la palma de la mano, un patrón de retina, un patrón de iris, un patrón de venas, una forma de oreja, un contorno facial, una voz, los escritos de un usuario (por ejemplo, la firma), etc.

En el modo seguro, el dispositivo electrónico puede extraer una característica única de un objeto reconocido en base a los datos detectados en la operación 440. Por ejemplo, el dispositivo electrónico puede extraer una imagen detectada a partir de los datos detectados y puede calcular una característica a partir de la imagen detectada.

En el modo seguro, el dispositivo electrónico puede transformar las características en una forma de plantilla y puede crear datos biométricos en la operación 450.

En el modo seguro, el dispositivo electrónico puede cifrar los datos biométricos en la operación 460. Por ejemplo, el dispositivo electrónico puede crear una tecla única en base a un identificador de dispositivo único en el modo seguro. La tecla única puede ser un valor accesible en modo seguro. Por ejemplo, en el modo seguro, el dispositivo electrónico puede almacenar información de función para crear una tecla única en una zona segura en una memoria, y puede crear una tecla única utilizando la información de función. La realización de la presente divulgación puede ser modificada sin la operación 460, sin embargo, debe entenderse que la presente divulgación no se limita a la modificación y la realización.

En el modo seguro, el dispositivo electrónico puede transferir los datos biométricos cifrados a partir del SO seguro al SO normal en la operación 465. Por ejemplo, el dispositivo electrónico puede almacenar los datos biométricos cifrados en una memoria (por ejemplo, un sistema de archivos REE) asignada como zona normal.

En el modo seguro, el dispositivo electrónico puede almacenar o registrar los datos biométricos o los datos biométricos cifrados como datos de registro para la autenticación biométrica en la operación 470.

En una realización de la presente divulgación, el dispositivo electrónico puede almacenar o registrar datos biométricos en una zona segura de la memoria accesible en modo seguro.

En una realización de la presente divulgación, el dispositivo electrónico puede almacenar una tecla única utilizada para el cifrado o la información de la función para crear una tecla única en una zona segura accesible en modo seguro, y puede transferir los datos biométricos cifrados al SO normal. El dispositivo electrónico puede almacenar o registrar los datos biométricos cifrados, transferidos a partir del SO seguro, en la zona normal sin limitación de acceso.

El dispositivo electrónico puede transferir la información del resultado relacionada con el registro biométrico a partir del SO seguro al SO normal en la operación 480. En el modo normal, el dispositivo electrónico puede proporcionar información del resultado, indicando que el registro biométrico, al usuario a través de la interfaz de usuario o el componente del dispositivo electrónico en la operación 490.

Mientras tanto, cuando el registro de los datos biométricos ha fallado debido al deterioro de la calidad de los datos sin procesar, etc., el procesador puede realizar un procedimiento de registro de nuevo. Para este propósito, en el modo normal, el dispositivo electrónico puede proporcionar una retroalimentación sobre el fallo de registro (por ejemplo, un

efecto visual, un efecto de audio, etc.) y/o una adquisición de nuevos datos detectados a la interfaz de usuario.

La Figura 5 es un diagrama de flujo que describe un procedimiento para autenticar información biométrica en un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 5, en un modo normal, un dispositivo electrónico puede detectar un evento de entrada biométrica en base a una señal de interrupción transferida a partir de un módulo de sensor biométrico, con el fin de realizar la autenticación biométrica (por ejemplo, el modo de autenticación) en la operación 510. Cuando se realiza una solicitud para realizar la autenticación biométrica en el modo normal, el dispositivo electrónico activa el módulo de sensor biométrico para detectar un objeto reconocido.

Después de detectar el evento de entrada biométrica en la operación 510, el dispositivo electrónico puede transferir una señal de evento al SO seguro en la operación 520. La señal de evento puede ser una señal de interrupción segura. El dispositivo electrónico puede llamar a un SO seguro y conmutar a partir del modo normal a un modo seguro, biométrico en

En el modo seguro, el dispositivo electrónico puede obtener datos detectados a través del módulo de sensor biométrico en la operación 530. En el modo seguro, el dispositivo electrónico puede extraer una característica única de un objeto reconocido en base a los datos detectados en la operación 540. El dispositivo electrónico puede crear datos biométricos para la autenticación biométrica en la operación 545. Los datos biométricos pueden ser un formato preestablecido, por ejemplo, una forma de plantilla.

Mientras tanto, en el modo seguro, el dispositivo electrónico puede recibir datos de registro cifrados almacenados en la zona normal o puede obtener datos de registro cifrados a partir de una memoria asignada como zona segura en la operación 550.

En el modo seguro, el dispositivo electrónico puede descifrar los datos de registro (por ejemplo, los datos de registro cifrados) en la operación 560. Por ejemplo, en el modo seguro, si se obtienen datos de registro cifrados, el dispositivo electrónico puede descifrar los datos de registro cifrados utilizando una tecla única. El procesador puede obtener información de función para crear una tecla única a partir de una memoria asignada como zona segura con limitación de acceso, y puede crear la tecla única utilizando la información de función obtenida.

En el modo seguro, el dispositivo electrónico puede calcular un valor de coincidencia comparando una o más características, calculadas a partir de los datos biométricos, y los datos de registro en la operación 570.

En el modo seguro, el dispositivo electrónico puede determinar si la autenticación biométrica es exitosa en base al valor de coincidencia de una o más características en la operación 580. Por ejemplo, cuando el valor de coincidencia supera un umbral preestablecido, el dispositivo electrónico concluye que la autenticación biométrica es exitosa. Por el contrario, cuando el valor de coincidencia es menor que o igual al umbral preestablecido, el dispositivo electrónico concluye que la autenticación biométrica ha fallado.

El dispositivo electrónico puede transferir la información del resultado de la autenticación biométrica a partir del SO seguro al SO normal en la operación 585. El dispositivo electrónico puede llamar a un SO normal y conmutar a partir del modo seguro al modo normal. En el modo normal, el dispositivo electrónico puede proporcionar la información del resultado de la autenticación biométrica al usuario a través de la interfaz de usuario o del componente del dispositivo electrónico en la operación 590.

Mientras tanto, cuando la autenticación biométrica ha fallado debido al deterioro de la calidad de los datos sin procesar, etc., el dispositivo electrónico puede realizar un procedimiento de autenticación de nuevo. Para este propósito, en el modo normal, el dispositivo electrónico puede proporcionar una retroalimentación sobre un fallo de autenticación (por ejemplo, un efecto visual, un efecto de audio, un efecto táctil, un efecto olfativo, etc.) y/o una adquisición de nuevos datos detectados a la interfaz de usuario.

La Figura 6 es un diagrama de flujo que describe un procedimiento para procesar información biométrica en un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 6, el dispositivo electrónico puede obtener datos biométricos en un modo seguro en la operación 610. El dispositivo electrónico puede seleccionar una función de transformación en el modo seguro en la operación 620. El dispositivo electrónico puede crear pseudodatos utilizando la función de transformación en la operación 630. Los pseudodatos pueden ser transformados a un formato preestablecido, por ejemplo, una forma de una plantilla.

La función de transformación puede incluir una función unidireccional, una función de conjunto de datos, etc. La función de transformación puede utilizar una función que utiliza un valor obtenible en un dispositivo de hardware seguro separado o cuando funciona en el modo seguro.

En diversas realizaciones de la presente divulgación, el dispositivo electrónico puede volver a transformar los pseudodatos creados mediante el uso de información adicional de los datos biométricos en el modo seguro. La

información adicional puede incluir información creada cuando se crean los datos biométricos, la puntuación de coincidencia entre los datos biométricos, el número de intentos, la información sobre el dedo si los datos biométricos son una huella dactilar, la información preestablecida cuando el usuario registra sus datos biométricos, etc. La función de transformación y la información adicional pueden almacenarse como metadatos de los datos biométricos. Los metadatos de los datos biométricos pueden almacenarse en una memoria asignada como zona accesible en un modo seguro.

El dispositivo electrónico puede cifrar los pseudodatos transformados en el modo seguro en la operación 640. Por ejemplo, el dispositivo electrónico puede crear una tecla única en base a un identificador de dispositivo único en el modo seguro.

El dispositivo electrónico puede utilizar los datos transformados o los datos transformados cifrados como datos de registro para el reconocimiento o la autenticación biométricos en el modo seguro en la operación 650.

En una realización de la presente divulgación, el dispositivo electrónico puede almacenar pseudodatos como datos de registro. El dispositivo electrónico puede almacenar pseudodatos en la zona normal. El dispositivo electrónico puede controlar la función de aplicación biométrica en base a los pseudodatos en el modo normal.

En una realización de la presente divulgación, cuando los datos biométricos han sido registrados como pseudodatos (por ejemplo, pseudodatos registrados), el dispositivo electrónico puede transformar los datos biométricos, recién introducidos para realizar la autenticación biométrica, en pseudodatos en el modo seguro utilizando una función de transformación. Después de esto, el dispositivo electrónico puede determinar si la autenticación biométrica ha tenido éxito comparando los pseudodatos transformados con los pseudodatos registrados.

En una realización de la presente divulgación, cuando se divulga la información biométrica, el dispositivo electrónico puede cambiar la función de transformación y puede actualizar los metadatos de los datos biométricos utilizando la función de transformación cambiada.

La Figura 7 es un diagrama que ilustra una arquitectura de red que incluye un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación.

Con referencia a la Figura 7, el dispositivo 701 electrónico incluye un bus 710, un procesador 720, una memoria 730, una interfaz 740 de entrada/salida, una pantalla 750, y una interfaz 760 de comunicación.

El bus 710 puede ser un circuito el cual conecta los componentes antes mencionados entre sí para comunicar señales (por ejemplo, mensajes de control) entre ellos.

El procesador 720 recibe un comando a partir de cualquiera de los componentes antes mencionados, (por ejemplo, la memoria 730, la interfaz 740 de entrada/salida, la pantalla 750, y la interfaz 760 de comunicación), a través del bus 710, interpreta el comando, y ejecuta una operación o procesamiento de datos de acuerdo con el comando descifrado.

La memoria 730 puede almacenar el comando o datos recibidos a partir del procesador 720 u otro componente (por ejemplo, la interfaz 740 de entrada/salida, la pantalla 750, la interfaz 760 de comunicación, etc.) generado por el procesador 720 u otro componente. La memoria 730 puede almacenar módulos de programación que incluyen un kernel 731, un software 732 intermedio, una Interfaz 733 de Programación de Aplicación (API), una o más aplicaciones 734, etc. Cada módulo de programación puede implementarse como software, firmware, hardware, y cualquier combinación de estos.

El kernel 731 puede controlar o gestionar los recursos del sistema (por ejemplo, el bus 710, el procesador 720, la memoria 730, etc.) para su uso en la ejecución de la operación o función implementada con el software 732 intermedio, la API 733, o la(s) aplicación(es) 734. El kernel 731 también puede proporcionar una interfaz que permita al software 732 intermedio, a la API 733, o a la(s) aplicación(es) 734 acceder a los componentes del dispositivo 701 electrónico para controlarlos o gestionarlos.

El software 732 intermedio puede funcionar como una retransmisión de los datos comunicados entre la API 733 o la(s) aplicación(es) 734 y el kernel 731. El software 732 intermedio puede ejecutar el control de las solicitudes de tareas a partir de la(s) aplicación(es) 734 de tal manera que se asigne la prioridad para su uso del recurso del sistema (por ejemplo, el bus 710, el procesador 720, y la memoria 730) del dispositivo electrónico a al menos una de la(s) aplicación(es) 734.

La API 733 es la interfaz para la(s) aplicación(es) 734 para controlar la función proporcionada por el kernel 731 o el software 732 intermedio y puede incluir al menos una interfaz o función (por ejemplo, comando) para el control de archivos, control de ventana, control de imagen, o control de texto.

De acuerdo con diversas realizaciones, la(s) aplicación(es) 734 puede(n) incluir una aplicación de Servicio de Mensajería Corta/Servicio de Mensajería Multimedia (SMS/MMS), una aplicación de correo electrónico, una aplicación de calendario, una aplicación de alarma, una aplicación de atención médica (por ejemplo, una aplicación de medición de la cantidad de movimiento o del nivel de azúcar en la sangre), y una aplicación de información ambiental (por ejemplo, aplicaciones de presión atmosférica, humedad, y temperatura). De manera adicional o alternativa, la(s)

aplicación(es) 734 puede(n) estar relacionada(s) con el intercambio de información entre el dispositivo 701 electrónico y otro dispositivo electrónico externo (por ejemplo, un dispositivo 704 electrónico). Los ejemplos de la aplicación de intercambio de información pueden incluir una aplicación de retransmisión de notificación para retransmitir información específica al dispositivo 704 electrónico externo y una aplicación de gestión de dispositivos para gestionar el dispositivo electrónico externo.

Por ejemplo, la aplicación de retransmisión de notificación puede estar proporcionada con una función de retransmisión de la información de alarma generada por las otras aplicaciones (por ejemplo, la aplicación de SMS/MMS, la aplicación de correo electrónico, la aplicación de asistencia médica, y la aplicación de información ambiental) del dispositivo electrónico a un dispositivo electrónico externo (por ejemplo, el dispositivo 704 electrónico). De manera adicional o alternativa, la aplicación de retransmisión de notificación puede proporcionar el usuario con la información de notificación recibida a partir de un dispositivo electrónico externo (por ejemplo, el dispositivo 704 electrónico). La aplicación del dispositivo electrónico puede gestionar (por ejemplo, instalar, eliminar, actualizar, etc.) la función de un dispositivo electrónico externo (por ejemplo, el encendido/apagado del propio dispositivo 704 electrónico (o de una parte del mismo) o el ajuste del brillo (o la resolución) de la pantalla) el cual se comunica con el dispositivo 701 electrónico o el servicio (por ejemplo, el servicio de comunicación o de mensajería) proporcionado por el dispositivo electrónico externo o por una aplicación que se ejecuta en el dispositivo externo.

De acuerdo con diversas realizaciones, la(s) aplicación(es) 734 puede(n) incluir una aplicación designada de acuerdo con la propiedad (por ejemplo, el tipo) de un dispositivo electrónico externo (por ejemplo, el dispositivo 704 electrónico). Si el dispositivo electrónico externo es un reproductor de MP3, la(s) aplicación(es) 734 puede(n) incluir una aplicación de reproducción de música. Del mismo modo, si el dispositivo electrónico externo es un aparato médico móvil, la(s) aplicación(es) 734 puede(n) incluir una aplicación de atención médica. De acuerdo con una realización, la(s) aplicación(es) 734 puede(n) incluir al menos una de las aplicaciones designadas al dispositivo 701 electrónico o las aplicaciones recibidas a partir del dispositivo electrónico externo (por ejemplo, un servidor 706 y el dispositivo 704 electrónico).

La interfaz 740 de entrada/salida entrega un comando o datos introducidos por un usuario a través de un dispositivo de entrada/salida (por ejemplo, un sensor, un teclado, una pantalla táctil, etc.) al procesador 720, la memoria 730, y/o la interfaz 760 de comunicación, a través del bus 710. Por ejemplo, la interfaz 740 de entrada/salida puede proporcionar el procesador 720 con los datos correspondientes a un toque realizado por el usuario en la pantalla táctil. La interfaz 740 de entrada/salida puede emitir el comando o los datos (los cuales se reciben a partir del procesador 720, la memoria 730, o la interfaz 760 de comunicación, a través del bus 710) a través del dispositivo de entrada/salida (por ejemplo, un altavoz, una pantalla, etc.). Por ejemplo, la interfaz 740 de entrada/salida puede emitir los datos de voz procesados por el procesador 720 al usuario a través del altavoz.

La pantalla 750 puede presentar diversas informaciones (por ejemplo, datos multimedia, datos de texto, etc.) al usuario.

La interfaz 760 de comunicación puede establecer una conexión de comunicación del dispositivo 701 electrónico con un dispositivo externo (por ejemplo, el dispositivo 704 electrónico, el servidor 706, etc.). Por ejemplo, la interfaz 760 de comunicación puede conectarse a una red 762 a través de un enlace inalámbrico o por cable para la comunicación con el dispositivo externo. Los ejemplos de la tecnología de comunicación inalámbrica pueden incluir Wi-Fi, Bluetooth (BT), Comunicación de Campo Cercano (NFC), GPS, y la tecnología de comunicación celular (por ejemplo, Evolución a Largo Plazo (LTE), LTE-Avanzada (LTE-A), Acceso Múltiple por División de Código (CDMA), Banda ancha CDMA (WCDMA), Sistema Universal de Telecomunicaciones Móviles (UMTS), Banda ancha inalámbrica (WiBro), y Sistema General para Comunicaciones Móviles (GSM)). Los ejemplos de la tecnología de comunicación por cable pueden incluir el Bus Serie Universal (USB), la Interfaz Multimedia de Alta Definición (HDMI), el Estándar Recomendado 232 (RS-232), y el Servicio Telefónico Ordinario (POTS).

De acuerdo con una realización de la presente divulgación, la red 762 puede ser una red de telecomunicaciones. La red de comunicación puede incluir al menos uno de una red informática, Internet, el Internet de las Cosas, y una red telefónica. De acuerdo con una realización de la presente divulgación, el protocolo de comunicación entre el dispositivo 701 electrónico y un dispositivo externo (por ejemplo, un protocolo de capa de transporte, un protocolo de capa de enlace de datos, un protocolo de capa física, etc.) puede ser soportado por al menos una de las aplicaciones 734, la API 733, el software 732 intermedio, el kernel 731, y la interfaz 760 de comunicación.

La Figura 8 es un diagrama de bloques que ilustra una configuración de un dispositivo electrónico de acuerdo con diversas realizaciones de la presente divulgación. El dispositivo electrónico ilustrado en la Figura 8 puede ser la totalidad o una parte del dispositivo 701 electrónico ilustrado en la Figura 7.

Con referencia a la Figura 8, el dispositivo 801 electrónico incluye un Procesador 810 de Aplicación (AP), un módulo 820 de comunicación, una tarjeta 824 de módulo de identificación de abonado (SIM), una memoria 830, un módulo 840 de sensor, un dispositivo 850 de entrada, un módulo 860 de pantalla, una interfaz 870, un módulo 880 de audio, un módulo 891 de cámara, un módulo 895 de gestión de energía, una batería 896, un indicador 897, y un motor 898.

El AP 810 puede funcionar un SO y/o programas de aplicación para controlar una pluralidad de componentes de hardware y/o software conectados al AP 810 y realizar procesamiento de datos y operaciones sobre datos multimedia.

El AP 810 puede implementarse en la forma de un Sistema en Chip (SoC). De acuerdo con una realización, el AP 810 puede incluir una Unidad de Procesamiento de Gráficos (GPU) (no se muestra).

El módulo 820 de comunicación (por ejemplo, la interfaz 160 de comunicación) puede realizar una comunicación de datos con otro dispositivo electrónico (por ejemplo, el dispositivo 704 electrónico, el servidor 706, etc.) a través de una red. De acuerdo con una realización, el módulo 820 de comunicación puede incluir un módulo 821 de celular, un módulo 823 de WiFi, un módulo 825 de BT, un módulo 827 de GPS, un módulo 828 de NFC, y un módulo 829 de Radio Frecuencia (RF).

El módulo 821 de celular es responsable de la comunicación de voz, y vídeo, mensajería de texto, y servicios de acceso a Internet a través de una red de comunicación (por ejemplo, LTE, LTE-A, CDMA, WCDMA, UMTS, WiBro, y redes GSM). El módulo 821 de celular puede realizar la identificación y autenticación de los dispositivos electrónicos en la red de comunicación, utilizando la tarjeta 824 SIM. De acuerdo con una realización, el módulo 821 de celular puede realizar al menos una de las funciones del AP 810. Por ejemplo, el módulo 821 de celular puede realizar al menos una parte de la función de control multimedia.

De acuerdo con una realización, el módulo 821 de celular puede incluir un Procesador de Comunicación (CP). El módulo 821 de celular puede implementarse en la forma de un SoC. Aunque el módulo 821 de celular (por ejemplo, el procesador de comunicación), la memoria 830, y el módulo 895 de gestión de energía se representan como componentes independientes separados del AP 810, la presente divulgación no se limita a ello, sino que puede ser realizada de manera que el AP incluya al menos uno de los componentes (por ejemplo, el módulo 821 de celular).

De acuerdo con una realización, cada uno de los AP 810 y el módulo 821 de celular (por ejemplo, el procesador de comunicación) puede cargar un comando o datos recibidos a partir de al menos uno de los componentes en una memoria no volátil o volátil y procesar el comando o los datos. El AP 810 o el módulo 821 de celular pueden almacenar los datos recibidos a partir de otros componentes o generados por al menos uno de los otros componentes en la memoria no volátil.

Cada uno de los módulos 823 de WiFi, módulos 825 de BT, el módulo 827 de GPS, y módulo 828 de NFC puede incluir un procesador para procesar los datos transmitidos/recibidos. Aunque el módulo 821 de celular, el módulo 823 de WiFi, el módulo 825 de BT, el módulo 827 de GPS, y el módulo 828 de NFC se representan como bloques independientes, al menos dos de ellos (por ejemplo, un procesador de comunicación correspondiente al módulo 821 de celular y un procesador de Wi-Fi correspondiente al módulo 823 de WiFi) pueden estar integrados en forma de un SoC.

El módulo 829 de RF es responsable de la comunicación de datos, por ejemplo, transmitir/recibir señales de RF. Aunque no se representa, el módulo 829 de RF puede incluir un transceptor, un Módulo de Amplificación de Energía (PAM), un filtro de frecuencia, y un Amplificador de Bajo Ruido (LNA). El módulo 829 de RF también puede incluir los elementos para transmitir/recibir una onda eléctrica en el espacio libre, por ejemplo, un conductor o un cable conductor. Aunque la Figura 8 se dirige al caso en el que el módulo 823 de WiFi, el módulo 825 de BT, el módulo 827 de GPS, y el módulo 828 de NFC comparten el módulo 829 de RF, la presente divulgación no se limita a ello, sino que puede realizarse de manera que al menos uno del módulo 823 de WiFi, el módulo 825 de BT, el módulo 827 de GPS, y el módulo 828 de NFC transmita/reciba señales de RF utilizando un módulo de RF independiente.

La tarjeta 824 SIM puede estar diseñada de modo que sea insertada en una ranura formada en una posición predeterminada del dispositivo electrónico. La tarjeta 824 SIM puede almacenar información de identificación única (por ejemplo, un Identificador de Tarjeta de Circuito Integrado (ICCID)), o información de abonado (por ejemplo, una Identidad de Abonado Móvil Internacional (IMSI)).

La memoria 830 (por ejemplo, la memoria 130) puede incluir al menos una de una memoria 832 interna y una memoria 834 externa. La memoria 832 interna puede incluir al menos una de una memoria volátil (por ejemplo, la Memoria Dinámica de Acceso Aleatorio (DRAM), RAM estática (SRAM), RAM Dinámica sincrónica (SDRAM) o una memoria no volátil (por ejemplo, una Memoria de Solo Lectura Programable Una Vez (OTPROM), una ROM programable (PROM), una ROM Borrable y Programable (EPROM), una ROM Borrable y Programable Eléctricamente (EEPROM), una ROM máscara, ROM flash, UNA memoria flash NAND, y una memoria flash NOR).

De acuerdo con una realización, la memoria 832 interna puede ser una Unidad de Estado Sólido (SSD). La memoria 834 externa puede ser una unidad flash tal como una flash compacta (CF), una Digital Segura (SD), una micro Micro-SD, una Mini-SD, una Digital extrema (xD), y una Tarjeta de Memoria. La memoria 834 externa puede conectarse al dispositivo 801 electrónico a través de diversas interfaces de manera funcional. De acuerdo con una realización, el dispositivo 801 electrónico puede incluir un dispositivo de almacenamiento (o un medio de almacenamiento) tal como un disco duro.

El módulo 840 de sensor puede medir una cantidad física o verificar el estado de funcionamiento del dispositivo 801 electrónico y convertir la información medida o verificada en una señal eléctrica. El módulo 840 de sensor puede incluir al menos uno de un sensor 840A gestual, un sensor 840B Giroscópico, un sensor 840C atmosférico, un sensor 840D magnético, un sensor 840E de aceleración, un sensor 840F de agarre, un sensor 840G de proximidad, un sensor 840H de color (por ejemplo, un sensor Rojo, Verde, Azul (RGB)), un sensor 8401 bio, un sensor 840J de temperatura/humedad, un sensor 840K de iluminancia, y un sensor 840M Ultravioleta (UV). De manera adicional o

alternativa, el módulo 840 de sensor puede incluir un sensor de nariz electrónica (no se muestra), un sensor de Electromiografía (EMG) (no se muestra), un sensor de Electroencefalograma (EEG) (no se muestra), un sensor de Electrocardiograma (ECG) (no se muestra), un sensor de infrarrojos (IR) (no se muestra), un sensor de iris (no se muestra), y un sensor de huellas dactilares (no se muestra). El módulo 840 de sensor puede incluir además un circuito de control para controlar al menos uno de los sensores incluidos en el mismo.

El dispositivo 850 de entrada puede incluir un panel 852 táctil, un sensor 854 de lápiz (digital), unas teclas 856, y un dispositivo 858 de entrada ultrasónica. El panel 852 táctil puede ser uno de un capacitivo, un resistivo, un infrarrojo, y un panel táctil de tipo microondas. El panel 852 táctil puede incluir además un circuito de control. En el caso del panel táctil de tipo capacitivo, es posible detectar el contacto físico o la aproximación. El panel 852 táctil puede incluir además una capa táctil. En este caso, el panel 852 táctil puede proporcionar el usuario con una reacción o retroalimentación háptica.

El sensor 854 de lápiz (digital) puede ser implementado con una hoja de la misma manera o similar a una entrada táctil del usuario o una hoja de reconocimiento separada. Las teclas 856 pueden incluir botones físicos, una tecla óptica, un teclado, etc. El dispositivo 858 de entrada ultrasónica es un dispositivo capaz de verificar datos mediante la detección de una onda sonora a través de un micrófono 888 y puede implementarse para el reconocimiento inalámbrico. De acuerdo con una realización, el dispositivo 801 electrónico puede recibir una entrada de usuario por medio de un dispositivo externo (por ejemplo, un ordenador o un servidor) conectado a él a través del módulo 820 de comunicación.

La pantalla 860 (por ejemplo, el módulo 150 de pantalla) puede incluir un panel 862, un dispositivo 864 de holograma, y un proyector 866. El panel 862 puede ser un panel de Pantalla de Cristal Líquido (LCD) o un panel de Diodo Emisor de Luz Orgánico de Conjunto Activo (AMOLED). El panel 862 puede ser implementado de modo que sea flexible, transparente, y/o portátil. El panel 862 puede implementarse como un módulo integrado con el panel 852 táctil. El dispositivo 864 de holograma puede presentar una imagen tridimensional en el aire utilizando una interferencia de luz. El proyector 866 puede proyectar una imagen en un monitor. El monitor puede colocarse dentro o fuera del dispositivo electrónico. De acuerdo con una realización, la pantalla 860 puede incluir un circuito de control para controlar el panel 862, el dispositivo 864 de holograma, y el proyector 866.

La interfaz 870 puede incluir, un HDMI 872, un (USB) 874, una interfaz 876 óptica, y un D-subminiatura 878 (D-sub). La interfaz 870 puede incluir la interfaz 160 de comunicación que se muestra en la Figura 1. De manera adicional o alternativa, la interfaz 870 puede incluir una interfaz de Enlace Móvil de Alta Definición (MHL), una interfaz de tarjeta SD/MMC, y una interfaz estándar de Asociación de Datos por Infrarrojo (IrDA).

El módulo 880 de audio puede convertir el sonido en una señal eléctrica y viceversa. Al menos una parte del módulo 880 de audio puede incluirse en la interfaz 140 de entrada/salida como se muestra en la Figura 1. El módulo 880 de audio puede procesar la información de sonido de entrada o salida a través de un altavoz 882, un receptor 884, un auricular 886, y el micrófono 888.

El módulo 891 de cámara es un dispositivo capaz de tomar imágenes fijas y en movimiento y, de acuerdo con una realización, incluye al menos un sensor de imagen (por ejemplo, un sensor frontal, un sensor posterior, etc.), una lente (no se muestra), un Procesador de Señal de Imagen (ISP) (no se muestra), y un flash (por ejemplo, un LED o una lámpara de xenón) (no se muestra).

El módulo 895 de gestión de energía puede gestionar la energía del dispositivo 801 electrónico. Aunque no se muestra, el módulo 895 de gestión de energía puede incluir un Circuito Integrado de Gestión de Energía (PMIC), un Circuito Integrado de cargador (CI), una batería, y un indicador de batería o combustible.

El PMIC puede estar integrado en un circuito integrado o en un semiconductor SoC. La carga se puede clasificar en carga inalámbrica y carga por cable. El CI de cargador puede cargar la batería y proteger el cargador contra la sobretensión o la sobre corriente. De acuerdo con una realización, el CI de cargador puede incluir al menos uno de un cargador con cable y/o un CI de cargador inalámbrico. Los ejemplos de tecnología de carga inalámbrica incluyen la carga inalámbrica por resonancia y la carga inalámbrica por ondas electromagnéticas, y se necesita un circuito adicional para la carga inalámbrica, tal como un bucle de bobina, un circuito de resonancia, un diodo, etc.

El indicador de la batería puede medir la energía residual de la batería 896, una tensión de carga, una corriente, una temperatura, etc. La batería 896 puede almacenar o generar energía y suministrar la energía almacenada o generada al dispositivo 801 electrónico. La batería 896 puede incluir una batería recargable o una batería solar.

El indicador 897 puede visualizar un estado de funcionamiento del dispositivo 801 electrónico o de una parte del dispositivo electrónico, un estado de arranque, un estado de mensajería, un estado de carga, etc. El motor 898 puede convertir la señal electrónica en una vibración mecánica. Aunque no se muestra, el dispositivo 801 electrónico puede incluir una unidad de procesamiento (por ejemplo, una GPU) para soportar una Televisión móvil. La unidad de procesamiento para el soporte de la Televisión móvil puede ser capaz de procesar los datos de los medios de comunicación que cumplen con los estándares de difusión tales como la Difusión Digital Multimedia (DMB), la Difusión Digital de Vídeo (DVB), el flujo de medios, etc.

Los componentes enumerados anteriormente del dispositivo electrónico de la presente divulgación pueden

implementarse en una o más partes, y los nombres de los componentes correspondientes pueden cambiarse dependiendo del tipo de dispositivo electrónico. El dispositivo electrónico de la presente divulgación puede incluir al menos uno de los componentes antes mencionados, con omisión o adición de algunos componentes. Los componentes del dispositivo electrónico de la presente divulgación pueden combinarse de manera selectiva en una entidad para realizar las funciones de los componentes igualmente como antes de la combinación.

El término "módulo", de acuerdo con diversas realizaciones de la divulgación, significa, pero no se limita a, una unidad de uno de un software, hardware, y firmware o cualquier combinación de estos. El término "módulo" puede utilizarse indistintamente con los términos "unidad", "lógica", "bloque lógico", "componente", o "circuito". El término "módulo" puede designar una unidad más pequeña de un componente o una parte de este. El término "módulo" puede ser la unidad más pequeña para realizar al menos una función o una parte de esta. El módulo puede ser implementado de manera mecánica o electrónica. Por ejemplo, un módulo puede incluir al menos uno de un chip de Circuito Integrado Específico de la Aplicación (ASIC), un Conjunto de Puerta Programables en Campo (FPGA), y un Dispositivo de Lógica Programable conocido o por desarrollar para determinadas operaciones.

De acuerdo con diversas realizaciones de la presente divulgación, los dispositivos (por ejemplo, los módulos o sus funciones) o los procedimientos pueden implementarse mediante instrucciones de programa de ordenador almacenadas en un medio de almacenamiento legible por ordenador. En el caso de que las instrucciones sean ejecutadas por al menos un procesador (por ejemplo, el procesador 120), el al menos un procesador puede ejecutar las funciones correspondientes a las instrucciones. El medio de almacenamiento legible por ordenador puede ser la memoria 130. Al menos una parte del módulo de programación puede ser implementado (por ejemplo, ejecutado) por el procesador 120. Al menos una parte del módulo de programación puede incluir módulos, programas, rutinas, un conjunto de instrucciones, y/ procedimientos para la ejecución de al menos una función.

El medio de almacenamiento legible por ordenador incluye medios magnéticos tal como un disquete y una cinta magnética, medios ópticos que incluyen un Disco Compacto (CD) ROM y un DVD ROM, un medio magnetoóptico tal como un disco floptical, y el dispositivo de hardware diseñado para almacenar y ejecutar comandos de programa tales como ROM, RAM, y la memoria flash. Los comandos del programa incluyen el código de lenguaje ejecutable por los ordenadores que utilizan el intérprete, así como los códigos de lenguaje de máquina creados por un compilador. El antes mencionado dispositivo de hardware puede implementarse con uno o más módulos de software para ejecutar las operaciones de las diversas realizaciones de la presente divulgación.

Aunque la presente divulgación se ha mostrado y descrito con referencia a diversas realizaciones de esta, los expertos en la técnica entenderán que se pueden realizar varios cambios de forma y detalles en la misma sin apartarse del alcance de la presente divulgación tal como la definen las reivindicaciones adjuntas.

REIVINDICACIONES

1. Dispositivo electrónico (101) para procesar información biométrica, el dispositivo electrónico (101) comprende:

un módulo (140) de sensor biométrico; y

un procesador (120), que proporciona un Entorno de Ejecución Enriquecido y un Entorno de Ejecución Fiable, configurado para:

- recibir, a través de un sistema operativo normal que funciona en el Entorno de Ejecución Enriquecido, una señal del módulo (140) de sensor biométrico;

en respuesta a la recepción de la señal, obtener, a través de un sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, datos sin procesar del módulo (140) de sensor biométrico, en donde el módulo (140) de sensor biométrico genera los datos sin procesar al detectar un objeto biométrico;

- crear, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, datos biométricos basados en los datos sin procesar;

- realizar, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, la autenticación biométrica basada en los datos biométricos creados; y

- proporcionar, desde el sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, información de resultado de autenticación biométrica al sistema operativo normal que funciona en el Entorno de Ejecución Enriquecido,

en el que los datos sin procesar del módulo de sensor biométrico solo son accesibles por el sistema operativo seguro que funciona en el Entorno de Ejecución Fiable.

2. El dispositivo electrónico (101) de la reivindicación 1, que comprende además:

- una memoria (130) que incluye una zona normal (131), una zona segura (132),

en donde la zona normal (131) es accesible por el sistema operativo normal que funciona en el Entorno de Ejecución Enriquecido, y

en donde la zona segura (132) es accesible por el sistema operativo seguro que funciona en el Entorno de Ejecución Fiable.

3. El dispositivo electrónico (101) de la reivindicación 2, en el que el procesador (120) está configurado además para:

- realizar el registro biométrico almacenando los datos biométricos creados en la zona segura (132).

4. El dispositivo electrónico (101) de la reivindicación 2, en el que el procesador (120) está configurado además para:

- realizar el registro biométrico cifrando los datos biométricos creados, y almacenando los datos biométricos creados en la zona segura (132).

5. El dispositivo electrónico (101) de la reivindicación 3, en el que una unidad de coincidencia de datos (320) del procesador (120) está configurada además para:

- realizar una autenticación biométrica haciendo coincidir los datos biométricos creados con los datos biométricos almacenados.

6. El dispositivo electrónico (101) de la reivindicación 3, en el que el procesador (120) está configurado además para:

- recibir, a través del sistema operativo normal que funciona en el Entorno de Ejecución Enriquecido, otra señal del módulo sensor biométrico (140);

en respuesta a la recepción de otra señal, obtener, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, datos sin procesar adicionales, a través de una interfaz (220) de entrada/salida segura, desde el módulo (140) de sensor biométrico, en donde el módulo (140) de sensor biométrico genera los datos sin procesar adicionales al detectar un objeto biométrico;

- crear, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, datos biométricos adicionales basados en los datos sin procesar adicionales; y

- realizar, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, la autenticación biométrica basada en los datos biométricos adicionales creados y los datos biométricos almacenados.

7. El dispositivo electrónico (101) de la reivindicación 6, en el que la otra señal es una señal de evento de entrada biométrica.

8. El dispositivo electrónico (101) de la reivindicación 1, en el que la señal es una señal de interrupción.

9. El dispositivo electrónico (101) de la reivindicación 1, en el que un módulo (221) de procesamiento biométrico del procesador está configurado además para:

- crear, a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable, los datos biométricos basándose en los datos sin procesar obteniendo una característica a partir de los datos sin procesar y creando los datos biométricos basándose en la característica obtenida.

10. El dispositivo electrónico (101) de la reivindicación 9, en el que el módulo (221) de procesamiento biométrico del procesador está configurado además para:

- crear una clave única basada en un identificador de dispositivo único y cifrar los datos biométricos por la clave única basada en el identificador de dispositivo único.

11. El dispositivo electrónico (101) de la reivindicación 1, en donde los datos sin procesar se obtienen del módulo de sensor biométrico a través del sistema operativo seguro que funciona en el Entorno de Ejecución Fiable sin estar sujetos a procesamiento, y/o en donde los datos sin procesar son accesibles por el sistema operativo seguro que funciona en el Entorno de Ejecución Fiable a través de una interfaz (220) de entrada/salida segura.

12. El dispositivo electrónico (101) de la reivindicación 1, en el que, basándose en un dedo, que se va a reconocer, que se pone en contacto con el módulo de sensor biométrico, el cual comprende un sensor de huella dactilar, el módulo de sensor biométrico está configurado para recibir la señal y generar los datos sin procesar.

13. El dispositivo electrónico (101) de la reivindicación 1, en el que tanto la señal recibida como los datos sin procesar se generan basándose en un dedo, que se va a reconocer, que se pone en contacto con el módulo de sensor biométrico.

FIG. 1

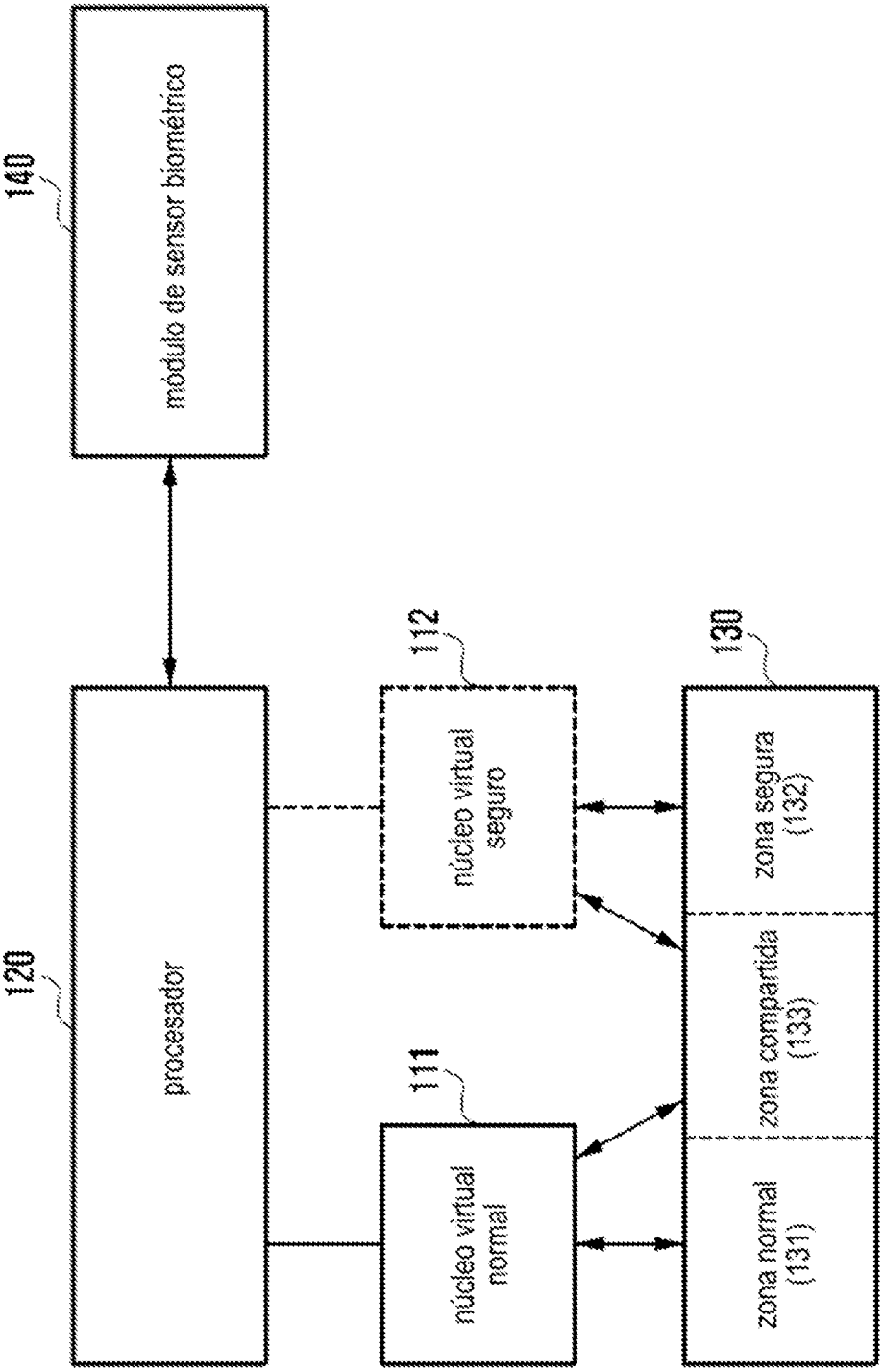

101
140
módulo de sensor biométrico
120
procesador
112
núcleo virtual seguro
111
núcleo virtual normal
130
zona segura (132)
zona compartida (133)
zona normal (131)

FIG. 2

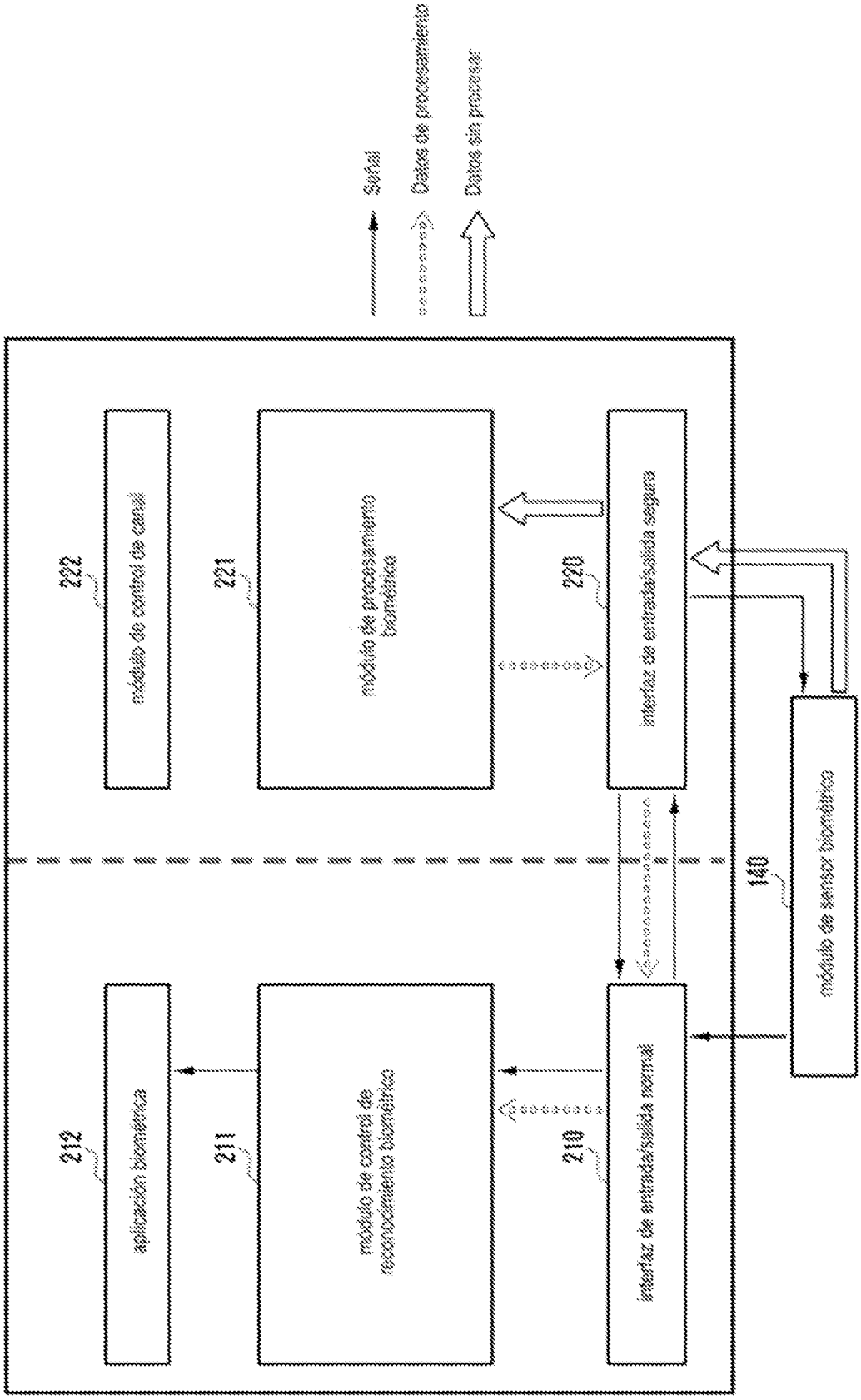

Serial
Datos de procesamiento
Datos sin procesar
222
módulo de control de canal
221
módulo de procesamiento biométrico
220
interfaz de entrada/salida segura
140
módulo de sensor biométrico
212
aplicación biométrica
211
módulo de control de reconocimiento biométrico
210
interfaz de entrada/salida normal

FIG. 3

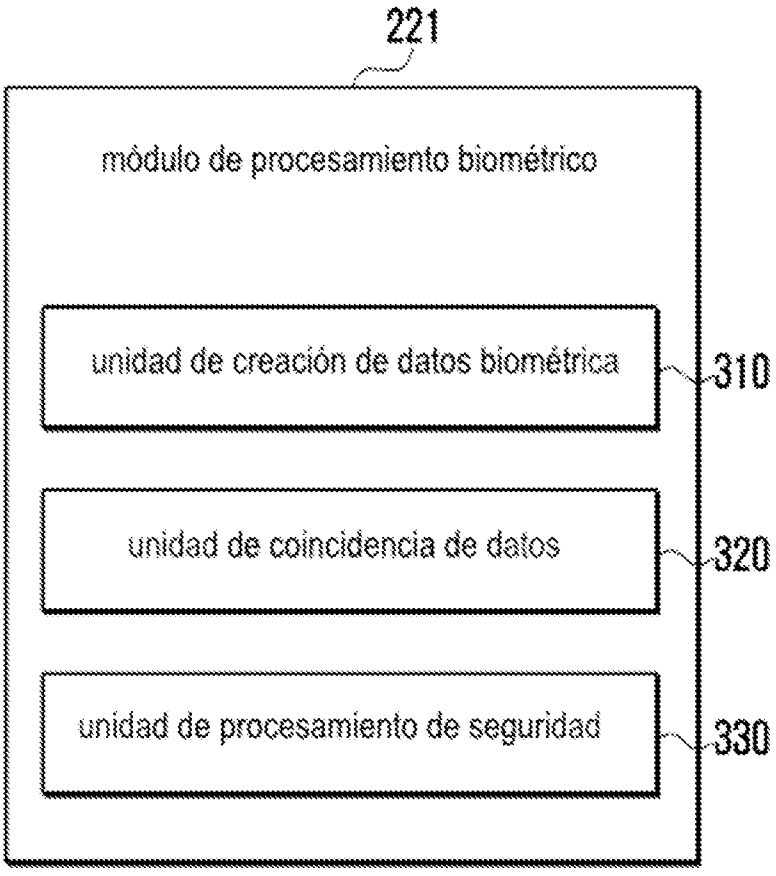

221
módulo de procesamiento biométrico
unidad de creación de datos biométrica
310
unidad de coincidencia de datos
320
unidad de procesamiento de seguridad
330

FIG. 4

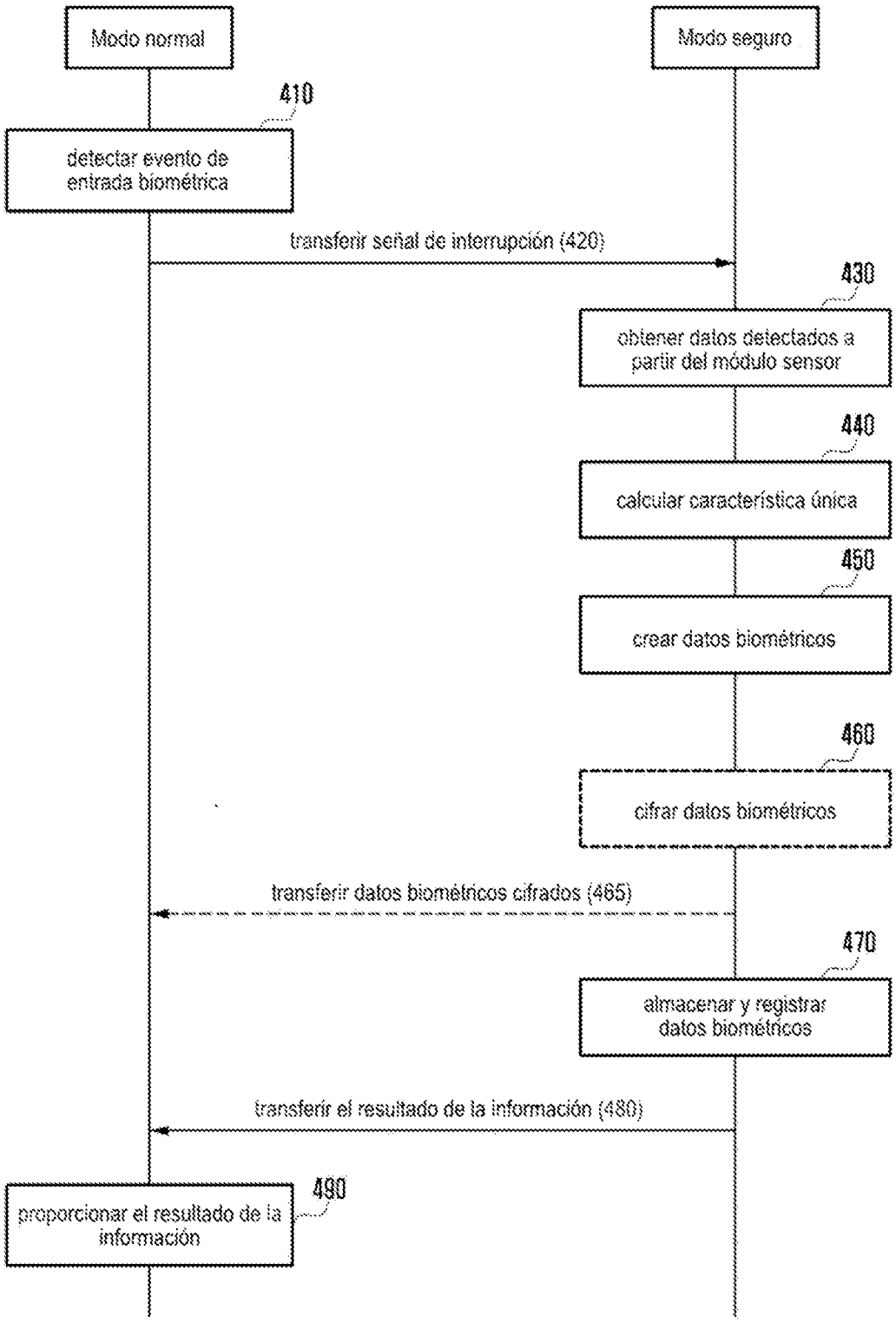

Modo normal
Modo seguro
410
detectar evento de entrada biométrica
transferir señal de interrupción (420)
430
obtener datos detectados a partir del módulo sensor
440
calcular característica única
450
crear datos biométricos
460
cifrar datos biométricos
transferir datos biométricos cifrados (465)
470
almacenar y registrar datos biométricos
transferir el resultado de la información (480)
490
proporcionar el resultado de la información

FIG. 5

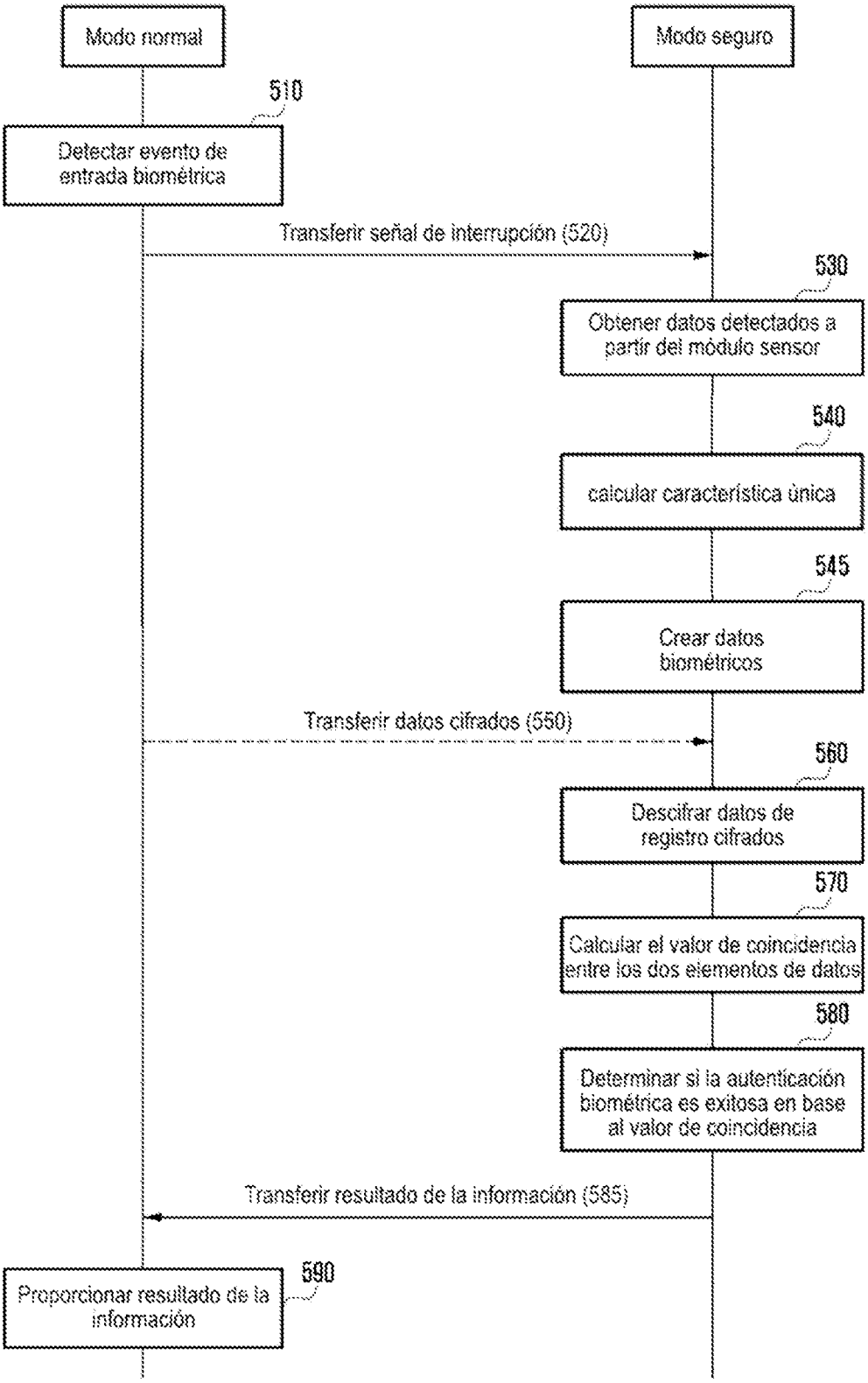

Modo normal
Modo seguro
510
Detectar evento de entrada biométrica
Transferir señal de interrupción (520)
530
Obtener datos detectados a partir del módulo sensor
540
calcular característica única
545
Crear datos biométricos
Transferir datos cifrados (550)
560
Descifrar datos de registro cifrados
570
Calcular el valor de coincidencia entre los dos elementos de datos
580
Determinar si la autenticación biométrica es exitosa en base al valor de coincidencia
Transferir resultado de la información (585)
590
Proporcionar resultado de la información

FIG. 6

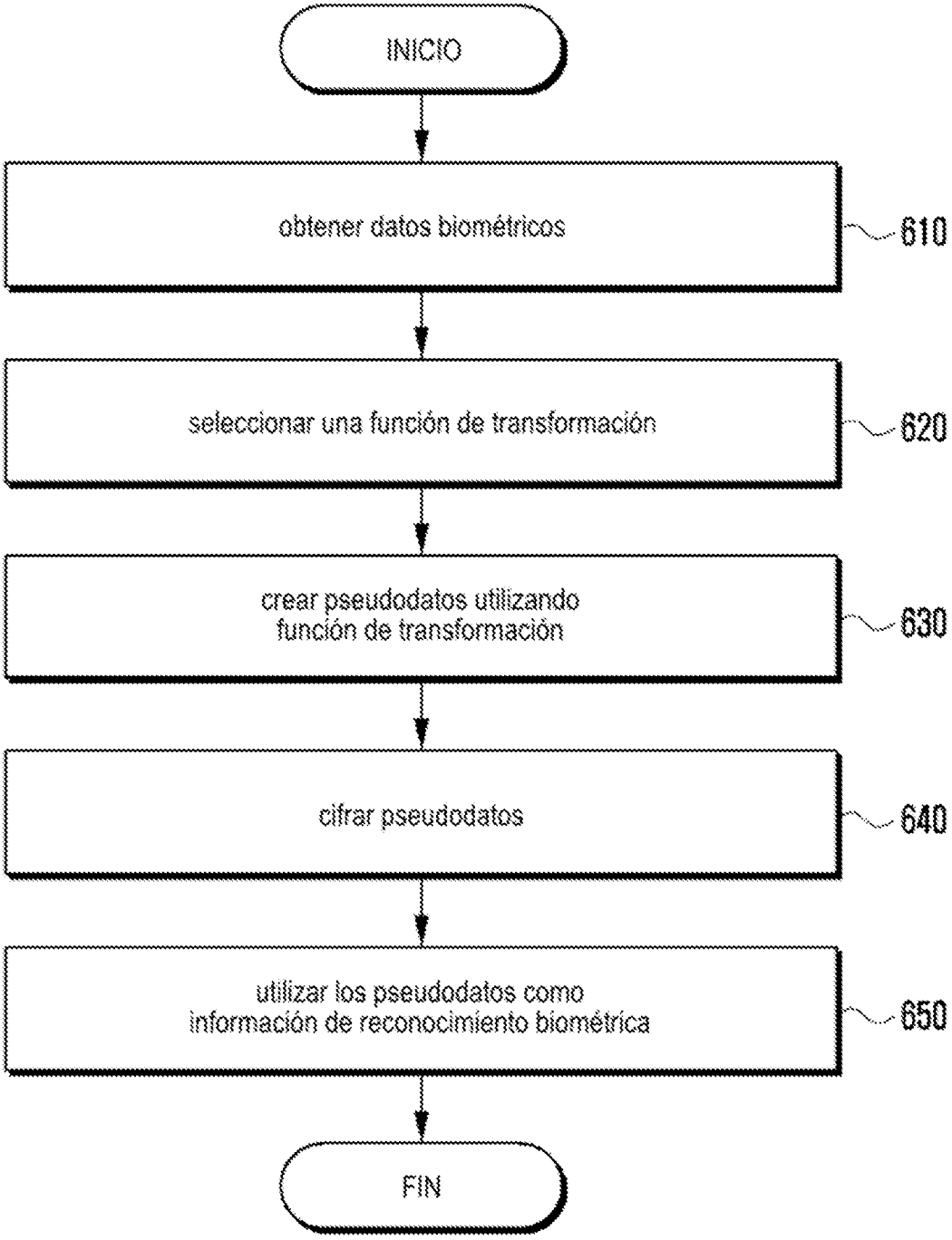

INICIO
obtener datos biométricos
610
seleccionar una función de transformación
620
crear pseudodatos utilizando función de transformación
630
cifrar pseudodatos
640
utilizar los pseudodatos como información de reconocimiento biométrica
650
FIN

FIG. 7

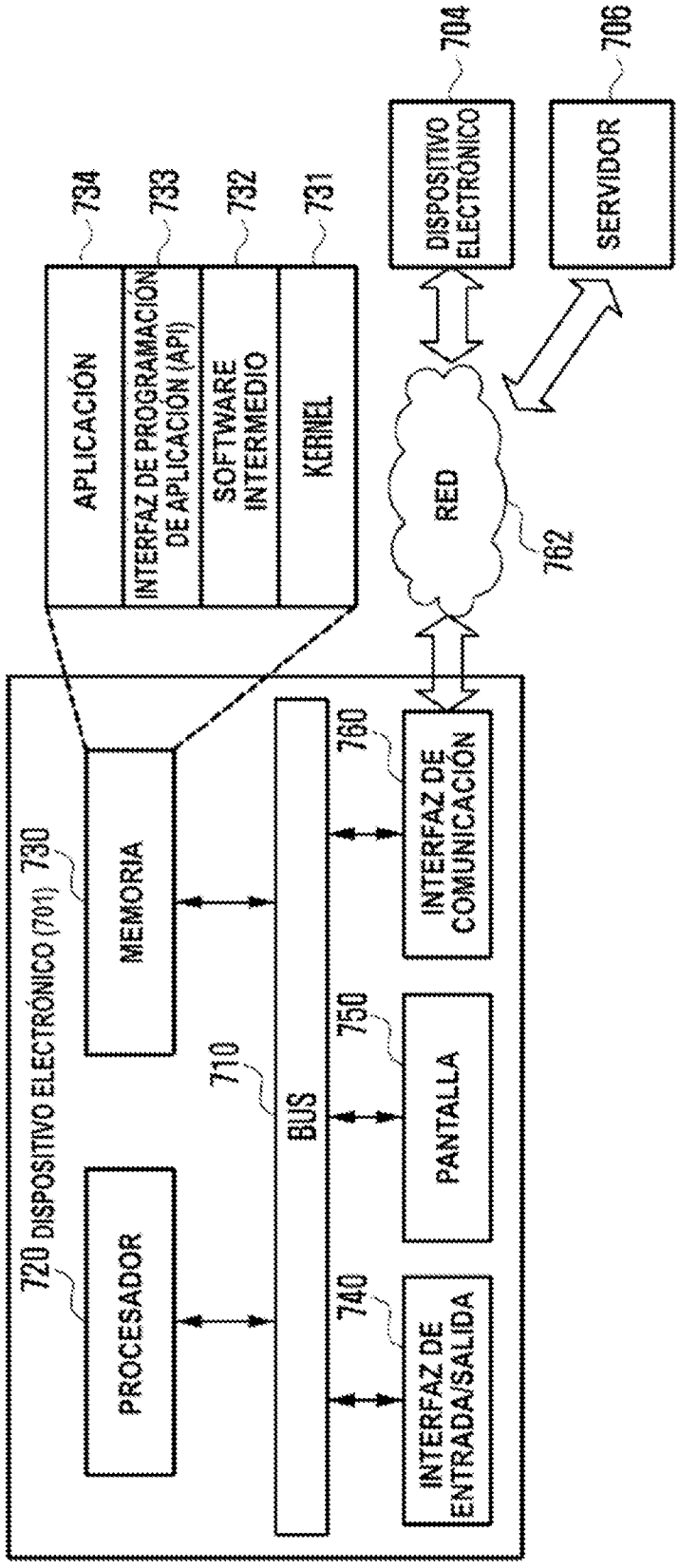
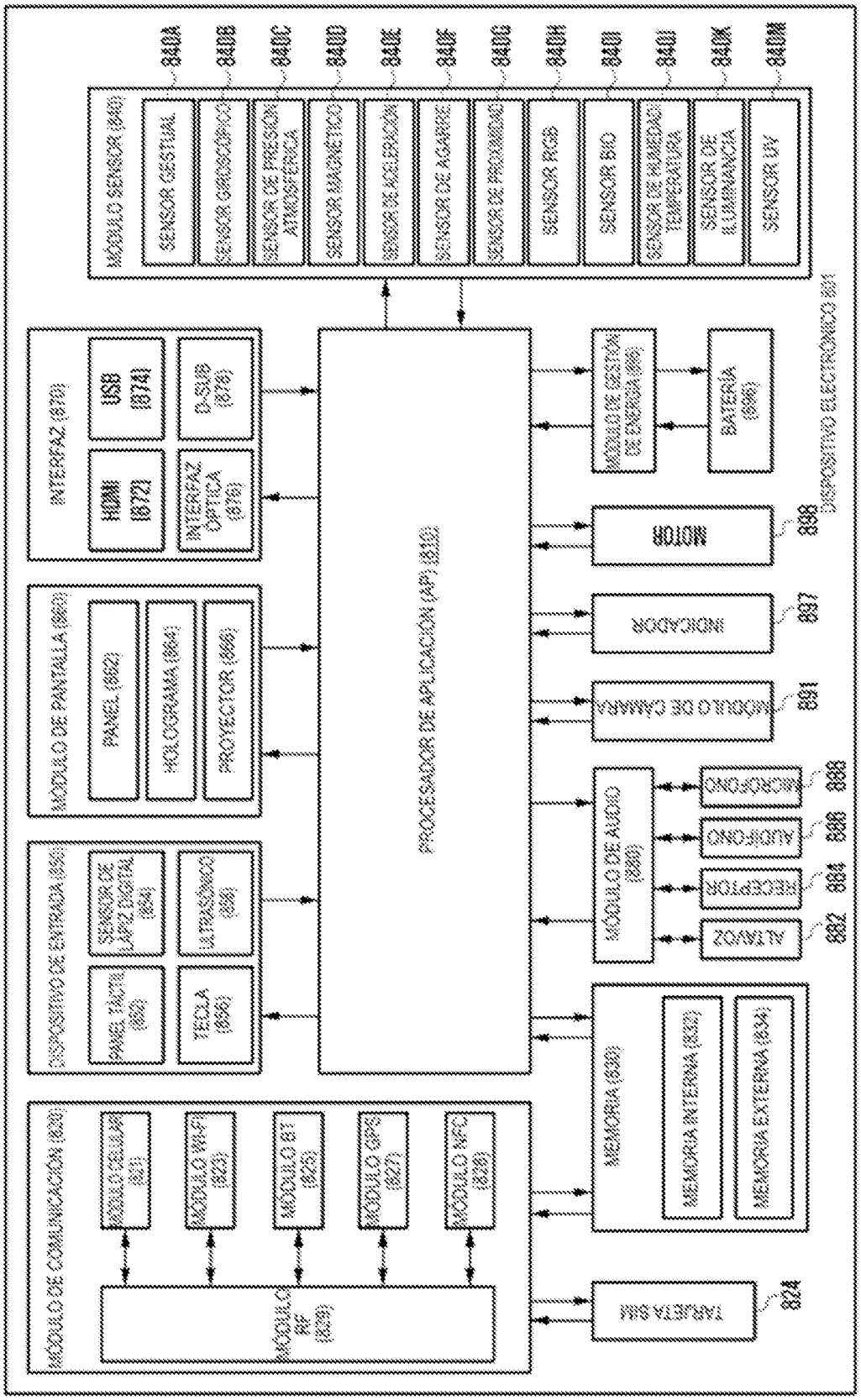

734
733
732
731
APLICACIÓN
INTERFAZ DE PROGRAMACIÓN DE APLICACIÓN (API)
SOFTWARE INTERMEDIO
KERNEL
704
DISPOSITIVO ELECTRÓNICO
706
SERVIDOR
RED
762
720 DISPOSITIVO ELECTRÓNICO (701)
730
MEMORIA
760
INTERFAZ DE COMUNICACIÓN
710
BUS
750
PANTALLA
PROCESADOR
740
INTERFAZ DE ENTRADA/SALIDA

FIG. 8


DISPOSITIVO ELECTRÓNICO 601
MÓDULO SENSOR (640)
SENSOR GESTUAL
SENSOR GIROSCÓPICO
SENSOR DE PRESIÓN ATMOSFÉRICA
SENSOR MAGNÉTICO
SENSOR DE ACELERACIÓN
SENSOR DE AGARRE
SENSOR DE PROXIMIDAD
SENSOR RGB
SENSOR BIO
SENSOR DE HUMEDAD/ TEMPERATURA
SENSOR DE ILUMINANCIA
SENSOR UV
640A
640B
640C
640D
640E
640F
640G
640H
640I
640J
640K
640M
INTERFAZ (670)
USB (674)
D-SUB (676)
HDMI (672)
INTERFAZ ÓPTICA (678)
MÓDULO DE PANTALLA (660)
PANEL (662)
HOLOGRAMA (664)
PROYECTOR (666)
DISPOSITIVO DE ENTRADA (650)
SENSOR DE LÁPIZ DIGITAL (654)
ULTRASÓNICO (658)
PANEL TÁCTIL (652)
TECLA (656)
PROCESADOR DE APLICACIÓN (AP) (610)
MÓDULO DE GESTIÓN DE ENERGÍA (695)
BATERÍA (696)
MOTOR
INDICADOR
CÁMARA
MÓDULO DE AUDIO (680)
ALTAVOZ
RECEPTOR
AUDÍFONO
MICRÓFONO
698
697
691
682
684
686
688
MÓDULO DE COMUNICACIÓN (620)
MÓDULO CELULAR (621)
MÓDULO Wi-Fi (623)
MÓDULO BT (625)
MÓDULO GPS (627)
MÓDULO NFC (628)
MÓDULO RF (629)
MEMORIA (630)
MEMORIA INTERNA (632)
MEMORIA EXTERNA (634)
TARJETA SIM
624