(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 869 195**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/45 (2013.01)
G06F 21/62 (2013.01)
H04L 9/32 (2006.01)
G06F 21/32 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.05.2017 PCT/CN2017/086051**

(87) Fecha y número de publicación internacional: **14.12.2017 WO17211199**

(96) Fecha de presentación y número de la solicitud europea: **26.05.2017 E 17809638 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.02.2021 EP 3468134**

(54) Título: **Método y dispositivo para la autenticación de identidad**

(30) Prioridad:

07.06.2016 CN 201610403643

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

LIU, JIAYIN y
WANG, LEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo para la autenticación de identidad

La presente solicitud reivindica prioridad sobre la Solicitud de Patente China No. 201610403643.X, presentada en la Oficina de Patentes de China el 7 de junio de 2016 y titulada "METHOD AND DEVICE FOR IDENTITY AUTHENTICATION".

CAMPO TÉCNICO

La presente divulgación se refiere al campo de las tecnologías de seguridad de la información y, en particular, a un método y dispositivo para la autenticación de identidad.

ANTECEDENTES

Con el continuo desarrollo de las tecnologías de la información, el reconocimiento de características biométricas (rostros, huellas dactilares, iris, etc.) se aplica gradualmente al campo electrónico y al sistema de control de acceso. Es conveniente utilizar reconocimientos biométricos para el cifrado o descifrado, de modo que no es necesario introducir contraseñas. Además, debido a que las características biométricas de los usuarios son únicas, las claves de características biométricas generalmente no se pueden replicar, robar ni olvidar, lo que puede reducir los riesgos de robo de identidad.

En comparación con el reconocimiento de características biométricas como rostros e iris, el reconocimiento de huellas dactilares es relativamente simple y, por lo tanto, las tecnologías de reconocimiento de huellas dactilares son particularmente populares. Actualmente, cuando se utiliza la huella dactilar de un usuario para la autenticación de identidad, generalmente se utiliza una huella dactilar fija. Por ejemplo, la huella dactilar de un usuario se puede utilizar repetidamente para diferentes aplicaciones de teléfono móvil que requieren autenticaciones de identidad, tal como el pago móvil.

Sin embargo, la autenticación de identidad realizada utilizando la información de huella dactilar fija es muy arriesgada y menos segura, y no puede satisfacer un requisito de usuario de una privacidad o seguridad relativamente alta.

El documento US 6.944.773 describe un método de autenticación en línea, que incluye que un usuario presente una o más huellas dactilares para la autenticación durante una transacción en línea, tal como una transacción por Internet. El usuario proporciona las huellas dactilares colocando el dedo correspondiente en la almohadilla de impresión del lector de huellas dactilares asociado con la computadora cliente que está utilizando el usuario. El método incluye recibir a través de la red informática una comunicación que indique que se necesita autenticación, obtener un primer número que indique cuántas huellas dactilares se solicitarán para la autenticación, seleccionar aleatoriamente qué huellas dactilares se solicitarán y enviar a través de la red informática una o más solicitudes de entrada de las huellas dactilares seleccionadas al azar. Una vez que el usuario introduce las huellas dactilares solicitadas, las huellas dactilares se envían a través de la red y el servidor las recibe. El servidor compara las huellas dactilares recibidas con las huellas dactilares almacenadas en la base de datos. Si todas las huellas dactilares coinciden, se autentica el usuario. Si alguna de las huellas dactilares no coincide, no se autentica el usuario.

RESUMEN

En vista de esto, las implementaciones de la presente divulgación proporcionan un método y un dispositivo para la autenticación de identidad, a fin de resolver un problema de que la autenticación de identidad realizada utilizando una huella dactilar fija es muy arriesgada y menos segura, y no puede satisfacer un requisito de usuario de una privacidad o seguridad relativamente alta. La invención se define en las reivindicaciones 1 y 8 independientes.

Para lograr los objetivos descritos anteriormente, en la presente divulgación se utilizan las siguientes soluciones técnicas:

De acuerdo con un primer aspecto, la presente divulgación proporciona un método para la autenticación de identidad, que incluye: seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar; y confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

De acuerdo con otro aspecto, la presente divulgación proporciona un dispositivo para la autenticación de identidad, que incluye: una unidad de selección, configurada para seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; una unidad de recepción, configurada

para recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; una unidad de coincidencia, configurada para comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar; y una unidad de confirmación, configurada para confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

Al utilizar las soluciones técnicas descritas anteriormente, las soluciones técnicas proporcionadas en las implementaciones de la presente divulgación tienen al menos las siguientes ventajas:
De acuerdo con un método y dispositivo para la autenticación de identidad proporcionados en las implementaciones de la presente divulgación, cuando se necesita realizar la autenticación de identidad, se selecciona primero una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; luego, se recibe una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; a continuación, la cantidad predeterminada recibida de información de huella dactilar se compara con la cantidad predeterminada seleccionada de información de huella dactilar; y se confirma que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar. En comparación con un método actual en el que solo se utiliza una huella dactilar fija para la autenticación de identidad, en la presente divulgación, se registra una pluralidad de piezas de información de huella dactilar de un usuario, de modo que cuando el usuario necesita un comportamiento de operación más seguro, una cantidad predeterminada de información de huella dactilar puede seleccionarse de la pluralidad de huellas dactilares registradas, se solicita al usuario que introduzca la información de huella dactilar del dedo correspondiente, y se puede completar una operación correspondiente cuando la información de huella dactilar coincide totalmente. Aumenta la complejidad de la autenticación de identidad, mejora la seguridad y puede satisfacer el requisito del usuario de privacidad o seguridad relativamente alta.

La descripción es simplemente un resumen general de las soluciones técnicas de la presente divulgación. Para comprender más claramente los medios técnicos de la presente divulgación para implementar el contenido de la memoria descriptiva, y para hacer más comprensibles los objetivos, características y ventajas anteriores y otros de la presente divulgación, a continuación, se enumeran las implementaciones específicas de la presente divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Al leer las descripciones detalladas de las siguientes implementaciones preferidas, un experto en la técnica comprende claramente otras ventajas y beneficios. Los dibujos adjuntos se utilizan simplemente para mostrar los objetivos de las implementaciones preferidas, pero no se consideran una limitación de la presente divulgación. Además, el mismo número de referencia se utiliza para indicar la misma parte en todos los dibujos adjuntos. En los dibujos adjuntos:

La FIG. 1 es un diagrama de flujo que ilustra un método para la autenticación de identidad, de acuerdo con una implementación de la presente divulgación;
La FIG. 2 es un diagrama que ilustra una pantalla de teléfono móvil de una instancia de operación, de acuerdo con una implementación de la presente divulgación;
La FIG. 3 es un diagrama que ilustra una pantalla de teléfono móvil de una instancia de operación, de acuerdo con una implementación de la presente divulgación;
La FIG. 4 es un diagrama que ilustra una pantalla de teléfono móvil de una instancia de operación, de acuerdo con una implementación de la presente divulgación;
La FIG. 5 es un diagrama de flujo que ilustra otro método para la autenticación de identidad, de acuerdo con una implementación de la presente divulgación;
La FIG. 6 es un diagrama estructural esquemático que ilustra un dispositivo para la autenticación de identidad, de acuerdo con una implementación de la presente divulgación; y
La FIG. 7 es un diagrama estructural esquemático que ilustra otro dispositivo para la autenticación de identidad, de acuerdo con una implementación de la presente divulgación.

DESCRIPCIÓN DE LAS IMPLEMENTACIONES

A continuación, se describen las implementaciones de ejemplo de la presente divulgación con más detalle con referencia a los dibujos adjuntos. Aunque los dibujos adjuntos muestran implementaciones de ejemplo de la presente divulgación, debe entenderse que las implementaciones pueden implementarse de diversas formas y no estarán limitadas por las implementaciones descritas aquí. En cambio, estas implementaciones se proporcionan para que un experto en la técnica comprenda más a fondo la presente divulgación y el alcance de la presente divulgación.

Una implementación de la presente divulgación proporciona un método para la autenticación de identidad. Como se muestra en la FIG. 1, el método incluye los siguientes pasos.

101. Seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario.

La cantidad predeterminada se puede configurar en base a un requisito real. Por ejemplo, la cantidad predeterminada se puede establecer en 2 o 3.

En la presente implementación de la presente divulgación, la pluralidad de piezas de información de huella dactilar del usuario puede registrarse de antemano. Cuando se registra la información de huella dactilar, también se debe registrar la información de identificación de huella dactilar correspondiente a la información de huella dactilar, y la información de identificación de huella dactilar puede ser el nombre, un número de identidad (ID), etc. de una huella dactilar. Por ejemplo, se registran la información de huella dactilar correspondiente al dedo anular izquierdo del usuario, la información de huella dactilar correspondiente al dedo índice izquierdo y la información de huella dactilar correspondiente al pulgar derecho.

La cantidad predeterminada de información de huella dactilar se puede seleccionar aleatoriamente de la pluralidad de huellas dactilares registradas en una secuencia de selección aleatoria, o la cantidad predeterminada de información de huella dactilar se puede seleccionar aleatoriamente de la pluralidad de huellas dactilares registradas en una secuencia de selección predeterminada del sistema.

En la implementación actual de la presente divulgación, cuando se necesita realizar una autenticación de identidad de un nivel de importancia alto en la interacción del producto, el sistema inicia la autenticación avanzada. Como tal, se puede activar el paso 101.

102. Recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar.

La información de solicitud de entrada de huella dactilar se utiliza para solicitar que se introduzca la información de huella dactilar correspondiente a la información de identificación de huella dactilar. La información de solicitud de entrada de huella dactilar puede ser información de solicitud de texto, información de solicitud de imagen, información de solicitud de audio, información de solicitud de vídeo, etc. Además, el usuario puede introducir la información de huella dactilar correspondiente en base a la información de solicitud de entrada de huella dactilar.

Por ejemplo, cuando el usuario necesita realizar un pago utilizando huellas dactilares en un teléfono móvil, el sistema selecciona aleatoriamente dos piezas de información de huella dactilar: información de huella dactilar del dedo índice derecho e información de huella dactilar del dedo anular izquierdo. Como se muestra en la FIG. 2, el sistema emite información de solicitud "introduzca la información de huella dactilar del dedo índice derecho" por primera vez y el usuario introduce la información de huella dactilar del dedo índice derecho del usuario en base a la información de solicitud. Una vez que el sistema recibe la información de huella dactilar introducida por el usuario, como se muestra en la FIG. 3, el sistema emite información de solicitud "introduzca la información de huella dactilar del dedo anular izquierdo" por segunda vez y el usuario introduce la información de huella dactilar del dedo anular izquierdo del usuario en base a la información de solicitud.

103. Comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar.

En la presente implementación de la presente divulgación, cada una de las informaciones de huella dactilar recibida se puede comparar con la información de huella dactilar introducida en respuesta a una petición de solicitud. Por ejemplo, después de que se recibe la información de huella dactilar introducida por el usuario, la información de huella dactilar se compara con la información de huella dactilar introducida en respuesta a una solicitud inmediata actual, si la información de huella dactilar coincide con la información de huella dactilar introducida en respuesta a la petición de solicitud actual, a continuación, se solicita la información de la siguiente huella dactilar a ser introducida; y si la información de huella dactilar no coincide con la información de huella dactilar introducida en respuesta a la petición de solicitud actual, se indica un error de autenticación de identidad.

104. Confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

Por ejemplo, cuando el usuario necesita realizar el pago con huella dactilar utilizando un teléfono móvil, el sistema selecciona aleatoriamente tres piezas de información de huella dactilar: información de huella dactilar del pulgar izquierdo, del dedo índice izquierdo y del pulgar derecho. El sistema solicita que se introduzca la información de huella dactilar del pulgar izquierdo por primera vez. Cuando el sistema detecta que la información de huella dactilar introducida por el usuario coincide con la información de huella dactilar registrada del pulgar izquierdo, el sistema solicita introducir la información de huella dactilar del dedo índice izquierdo por segunda vez. Cuando el sistema detecta que la información de huella dactilar introducida por el usuario coincide con la información de huella dactilar registrada del dedo índice izquierdo, el sistema solicita introducir la información de huella dactilar del pulgar derecho por tercera vez. Cuando el sistema detecta que la información de huella dactilar introducida por el usuario coincide con la información de huella dactilar registrada del pulgar derecho, indica que la información de huella dactilar recibida coincide con la información de huella dactilar introducida en respuesta a la petición de solicitud y la autenticación de

identidad del usuario tiene éxito. Como tal, el pago con huella dactilar se puede completar y se solicita información de solicitud que indique que el pago tiene éxito. Los detalles se muestran en la FIG. 4.

De acuerdo con un método para la autenticación de identidad proporcionado en la presente implementación de la presente divulgación, cuando es necesario realizar la autenticación de identidad, primero se selecciona una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; luego, se recibe una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; a continuación, la cantidad predeterminada recibida de información de huella dactilar se compara con la cantidad predeterminada seleccionada de información de huella dactilar; y se confirma que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar. En comparación con un método actual en el que solo se utiliza una huella dactilar fija para la autenticación de identidad, en la presente divulgación, se registra una pluralidad de piezas de información de huella dactilar de un usuario, de modo que cuando el usuario necesita un comportamiento de operación de nivel de seguridad alto, una cantidad predeterminada de información de huella dactilar puede seleccionarse de la pluralidad de huellas dactilares registradas, se solicita al usuario que introduzca la información de huella dactilar del dedo correspondiente, y se puede completar una operación correspondiente cuando la información de huella dactilar coincide totalmente. Aumenta la complejidad de la autenticación de identidad, mejora la seguridad y puede satisfacer un requisito del usuario de privacidad o seguridad relativamente alta.

Además, una implementación de la presente divulgación proporciona otro método para la autenticación de identidad. Como se muestra en la FIG. 5, el método incluye los siguientes pasos.

201. Registrar cada una de las informaciones de huella dactilar introducida por un usuario y la información de identificación de huella dactilar correspondiente a cada una de las informaciones de huella dactilar.

La información de identificación de huella dactilar puede ser nombre, número de identidad, etc. de una huella dactilar, por ejemplo, la huella dactilar del dedo anular izquierdo y la huella dactilar del dedo meñique derecho.

En la presente implementación de la presente divulgación, cada una de las informaciones de huella dactilar introducida por el usuario y la información de identificación de huella dactilar correspondiente a cada una de las informaciones de huella dactilar puede registrarse de antemano para la invocación durante la autenticación de identidad del usuario.

En un proceso de registro de la información de huella dactilar introducida por el usuario, se puede solicitar la información de huella dactilar correspondiente a la información de identificación de huella dactilar que necesita introducirse, de modo que se registren la información de huella dactilar del usuario y la información de identificación de huella dactilar correspondiente a la información de huella dactilar. Por ejemplo, cuando se solicita la información de huella dactilar del dedo índice izquierdo que necesita introducirse, el usuario puede introducir la información de huella dactilar del dedo índice izquierdo en base a la información de solicitud y el sistema registra la información de huella dactilar y un identificador del dedo índice izquierdo correspondiente a la información de huella dactilar.

Después de que el usuario introduce la información de la huella dactilar, se puede emitir cada una de las informaciones de identificación de huella dactilar, de modo que el usuario selecciona la información de huella dactilar introducida actualmente que el sistema puede registrar como información de la huella dactilar de qué dedo.

202. Detectar si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada en un proceso de registro de la información de huella dactilar introducida por el usuario.

Vale la pena señalar que si la información de huella dactilar introducida actualmente no existe en la información de huella dactilar registrada, indica que la información de huella dactilar introducida actualmente no se ha registrado, es información de huella dactilar introducida recientemente y puede registrarse por el sistema.

203. Dejar de registrar la información de huella dactilar introducida actualmente y emitir información de alarma que indica que una huella dactilar se introduce repetidamente si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada.

La información de alarma puede ser información de alarma de texto, información de alarma de imagen, información de alarma de audio, información de alarma de vídeo, etc.

Vale la pena señalar que si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada, indica que la información de huella dactilar introducida actualmente se ha registrado y no es necesario registrar la información de huella dactilar y luego se detiene el registro de la información de huella dactilar introducida actualmente y se emite la información de alarma que indica que una huella dactilar se introduce repetidamente, solicitando así al usuario que cambie un dedo para introducir la información de huella dactilar.

204. Seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario cuando es necesario realizar la autenticación de identidad del usuario.

La cantidad predeterminada se puede configurar en función de una demanda real. En la presente implementación de la presente divulgación, cuando se necesita una privacidad o seguridad relativamente alta, la cantidad predeterminada puede ser mayor, y cuando se necesita una privacidad o seguridad relativamente baja, la cantidad predeterminada puede ser menor.

En la presente implementación de la presente divulgación, antes del paso 204, el método incluye además detectar si el usuario inicia sesión actualmente; y, en caso negativo, emitir información de solicitud solicitando al usuario que inicie sesión utilizando una cuenta. La información de solicitud puede ser información de solicitud de texto, información de solicitud de imagen, información de solicitud de audio, información de solicitud de vídeo, etc. El paso 204 incluye: si, en caso positivo, obtener información de cuenta de inicio de sesión del usuario; y seleccionar una cantidad predeterminada de información de huella dactilar de una pluralidad de huellas dactilares registradas correspondientes a la información de cuenta.

Vale la pena señalar que en la presente implementación de la presente divulgación, en un proceso de registro de información de huella dactilar del usuario, se puede registrar una pluralidad de piezas de información de huella dactilar correspondientes respectivamente a diferentes usuarios en base a información de cuenta del usuario. Cuando es necesario realizar la autenticación de identidad del usuario, se puede determinar una pluralidad de huellas dactilares registradas correspondientes a un usuario en base a la información de cuenta de inicio de sesión del usuario y se puede seleccionar una cantidad predeterminada de información de huella dactilar, para realizar la autenticación de identidad en diferentes usuarios.

En la presente implementación de la presente divulgación, después del paso 204, el método incluye además la emisión de información de solicitud en base a la información de identificación de huella dactilar correspondiente a la información de huella dactilar en una secuencia predeterminada de reconocimiento de huellas dactilares o una secuencia de reconocimiento aleatoria, para satisfacer los requisitos de diferentes usuarios. La secuencia predeterminada de reconocimiento de huellas dactilares se puede preconfigurar en base a una demanda real. Por ejemplo, para facilitar una operación de usuario, la secuencia predeterminada de reconocimiento de huellas dactilares se puede configurar para que preferiblemente solicite introducir las huellas dactilares seleccionadas de la mano izquierda y solicite introducir las huellas dactilares seleccionadas de la mano derecha después de introducir las huellas dactilares seleccionadas de la mano izquierda.

205. Recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar.

La información de solicitud de entrada de huella dactilar se utiliza para solicitar que se introduzca la información de huella dactilar correspondiente a la información de identificación de huella dactilar, de modo que el usuario puede introducir la información de huella dactilar correspondiente en base a la información de solicitud.

Además, el método incluye detectar si la información de huella dactilar introducida por el usuario se recibe dentro de un período de tiempo predeterminado cada vez que se emite información de solicitud; y, en caso negativo, confirmar que la autenticación de identidad falla y emitir información de alarma que indica que se agotó un tiempo de operación. El período de tiempo predeterminado comienza a partir de un momento en el que se emite la información de solicitud y la duración correspondiente del período de tiempo se puede configurar en base a una demanda real. Por ejemplo, la duración del período de tiempo se puede establecer en 10 segundos, 20 segundos, etc.

Por ejemplo, la duración del período de tiempo predeterminado se puede establecer en 15 segundos. Cuando se emite información de solicitud que solicita introducir información de huella dactilar del dedo índice derecho, si la información de huella dactilar introducida por el usuario no se recibe dentro de los 15 segundos a partir del momento en que se emite la información de solicitud, indica que la operación ha expirado el tiempo y no hay necesidad de esperar a recibir la información de huella dactilar introducida por el usuario. Como tal, se puede detectar si la operación de usuario expira el tiempo sin realizar la autenticación de identidad y sin emitir la información de alarma que indica que una operación expira el tiempo.

206. Comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar.

En la presente implementación de la presente divulgación, el paso 206 puede incluir comparar cada una de las informaciones de huella dactilar recibida con la información de huella dactilar introducida en respuesta a una petición de solicitud. El paso 206 puede incluir además después de recibir la cantidad predeterminada de información de huella dactilar, comparar la información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar.

207. Confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

En la presente implementación de la presente divulgación, el paso 207 puede incluir confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

Por ejemplo, cuando es necesario realizar la autenticación de identidad del usuario, el sistema selecciona aleatoriamente dos piezas de información de huella dactilar: información de huella dactilar del pulgar derecho y del dedo índice derecho. El sistema le solicita introducir la información de huella dactilar del pulgar derecho por primera vez. Cuando detecta que la información de huella dactilar introducida por el usuario coincide con la información de huella dactilar registrada del pulgar derecho, el sistema solicita introducir la información de huella dactilar del dedo índice derecho por segunda vez. Cuando el sistema detecta que la información de huella dactilar introducida por el usuario coincide con la información de huella dactilar registrada del dedo índice derecho, indica que la información de huella dactilar recibida coincide con la información de huella dactilar introducida en respuesta a la petición de solicitud y, como tal, la autenticación de identidad del usuario tiene éxito.

El método incluye además confirmar que la autenticación de identidad falla y emitir información de alarma que indica que la autenticación de identidad falla cuando la cantidad predeterminada recibida de información de huella dactilar no coincide con la cantidad predeterminada seleccionada de información de huella dactilar. Cuando la cantidad predeterminada recibida de información de huella dactilar no coincide con la cantidad predeterminada seleccionada de información de huella dactilar, es decir, hay una o más piezas de información de huella dactilar que no coinciden con la información de huella dactilar seleccionada. Indica que el usuario no realiza la operación actual o el usuario introduce la información de huella dactilar incorrecta y, en consecuencia, la autenticación de identidad falla y se emite la información de alarma que indica que la autenticación de identidad falla.

De acuerdo con otro método para la autenticación de identidad proporcionado en la presente implementación de la presente divulgación, cuando es necesario realizar la autenticación de identidad, primero se selecciona una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; luego, se recibe una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; a continuación, la cantidad predeterminada recibida de información de huella dactilar se compara con la cantidad predeterminada seleccionada de información de huella dactilar; y se confirma que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar. En comparación con un método actual en el que solo se utiliza una huella dactilar fija para la autenticación de identidad, en la presente divulgación, se registra una pluralidad de piezas de información de huella dactilar de un usuario, de modo que cuando el usuario necesita un comportamiento de operación más seguro, una cantidad predeterminada de información de huella dactilar puede seleccionarse de la pluralidad de huellas dactilares registradas, se solicita al usuario que introduzca la información de huella dactilar del dedo correspondiente, y se puede completar una operación correspondiente cuando la información de huella dactilar coincide totalmente. Aumenta la complejidad de la autenticación de identidad, mejora la seguridad y puede satisfacer uno requisito del usuario de privacidad o seguridad relativamente alta.

Además, en una implementación específica del método mostrada en la FIG. 1, una implementación de la presente divulgación proporciona un dispositivo para la autenticación de identidad. Como se muestra en la FIG. 6, el dispositivo puede incluir una unidad 61 de selección, una unidad 62 de recepción, una unidad 63 de coincidencia y una unidad 64 de confirmación.

La unidad 61 de selección puede estar configurada para seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario. En la presente implementación de la presente divulgación, cuando se necesita realizar la identificación de identidad con un nivel de seguridad relativamente alto, la unidad 61 de selección se activa para funcionar.

La unidad 62 de recepción puede estar configurada para recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar. La unidad 62 de recepción es un módulo de función principal para recibir la información de huella dactilar introducida en el dispositivo y activa la unidad 63 de coincidencia para realizar la autenticación de identidad.

La unidad 63 de coincidencia puede estar configurada para comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar. La unidad 63 de coincidencia es un módulo de función principal para realizar el reconocimiento y la autenticación de huella dactilar en la información de huella dactilar recibida en el dispositivo.

La unidad 64 de confirmación puede estar configurada para confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

Vale la pena señalar que la implementación del dispositivo actual corresponde a la implementación del método anterior. Para más detalles, se puede hacer referencia a las descripciones correspondientes en la FIG. 1. Para facilitar la lectura, los detalles en la implementación del método anterior se omiten en la implementación del dispositivo actual. Sin embargo, debería quedar claro que el dispositivo en la presente implementación puede implementar correspondientemente todo el contenido en la implementación del método anterior.

De acuerdo con un dispositivo para la autenticación de identidad proporcionado en la presente implementación de la presente divulgación, cuando es necesario realizar la autenticación de identidad, primero se selecciona una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; luego, se recibe una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; a continuación, la cantidad predeterminada recibida de información de huella dactilar se compara con la cantidad predeterminada seleccionada de información de huella dactilar; y se confirma que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar. En comparación con un método actual en el que solo se utiliza una huella dactilar fija para la autenticación de identidad, en la presente divulgación, se registra una pluralidad de piezas de información de huella dactilar de un usuario, de modo que cuando el usuario necesita un comportamiento de operación más seguro, una cantidad predeterminada de información de huella dactilar puede seleccionarse de la pluralidad de huellas dactilares registradas, se solicita al usuario que introduzca la información de huella dactilar del dedo correspondiente, y se puede completar una operación correspondiente cuando la información de huella dactilar coincida totalmente. Aumenta la complejidad de la autenticación de identidad, mejora la seguridad y puede satisfacer el requisito del usuario de privacidad o seguridad relativamente alta.

Además, en una implementación específica del método mostrada en la FIG. 5, una implementación de la presente divulgación proporciona otro dispositivo para la autenticación de identidad. Como se muestra en la FIG. 7, el dispositivo puede incluir una unidad 71 de selección, una unidad 72 de recepción, una unidad 73 de coincidencia y una unidad 74 de confirmación.

La unidad 71 de selección puede estar configurada para seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario. En la presente implementación de la presente divulgación, cuando se necesita realizar la identificación de identidad con un nivel de seguridad relativamente alto, la unidad 71 de selección se activa para funcionar.

La unidad 72 de recepción puede estar configurada para recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar. La unidad 72 de recepción es un módulo de función principal para recibir la información de huella dactilar introducida en el dispositivo y activa la unidad 73 de coincidencia para realizar la autenticación de identidad.

La unidad 73 de coincidencia puede estar configurada para comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar. La unidad 73 de coincidencia es un módulo de función principal para realizar el reconocimiento y la autenticación de huella dactilar en la información de huella dactilar recibida en el dispositivo.

La unidad 74 de confirmación puede estar configurada para confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

La unidad 73 de coincidencia puede estar configurada para comparar cada una de las informaciones de huella dactilar recibida con la información de huella dactilar introducida en respuesta a una petición de solicitud.

La unidad 74 de confirmación puede estar configurada para confirmar que la autenticación de identidad tiene éxito cuando la información de huella dactilar recibida coincide con la información de huella dactilar introducida en respuesta a la petición de solicitud.

El dispositivo incluye además una unidad 75 de detección y una unidad 76 de salida.

La unidad 75 de detección puede estar configurada para detectar si la información de huella dactilar introducida por el usuario se recibe dentro de un período de tiempo predeterminado cada vez que se emite información de solicitud.

La unidad 74 de confirmación puede estar configurada además para confirmar que la autenticación de identidad falla si la unidad 75 de detección detecta que la información de huella dactilar introducida por el usuario no se recibe dentro del período de tiempo predeterminado.

La unidad 76 de salida puede estar configurada para emitir información de alarma que indique que una operación ha expirado el tiempo.

La unidad 74 de confirmación puede estar configurada además para confirmar que la autenticación de identidad falla cuando la cantidad predeterminada recibida de información de huella dactilar no coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

La unidad 76 de salida puede estar configurada además para emitir información de alarma que indica que la autenticación de identidad falla.

La unidad 75 de detección puede estar configurada además para detectar si el usuario está en estado de inicio de sesión.

La unidad 76 de salida puede estar configurada además para emitir información de solicitud que solicita al usuario que inicie sesión utilizando una cuenta si la unidad 75 de detección detecta que el usuario aún no ha iniciado sesión.

La unidad 71 de selección puede incluir un módulo 711 de adquisición y un módulo 712 de selección.

El módulo 711 de adquisición puede estar configurado para obtener información de cuenta de inicio de sesión del usuario si se detecta que el usuario ha iniciado sesión.

El módulo 712 de selección puede estar configurado para seleccionar una cantidad predeterminada de información de huella dactilar de una pluralidad de huellas dactilares registradas correspondientes a la información de cuenta obtenida por el módulo 711 de adquisición.

El dispositivo incluye además una unidad 77 de registro.

La unidad 77 de registro puede estar configurada para registrar cada una de las informaciones de huella dactilar introducida por el usuario y la información de identificación de huella dactilar correspondiente a cada una de las informaciones de huella dactilar.

La unidad 75 de detección puede estar configurada además para detectar si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada en un proceso de registro de la información de huella dactilar introducida por el usuario.

La unidad 77 de registro puede estar configurada además para detener el registro de la información de huella dactilar introducida actualmente si la unidad 75 de detección detecta que la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada.

La unidad 76 de salida puede estar configurada además para emitir información de alarma que indica que se ha introducido repetidamente una huella dactilar.

La unidad 76 de salida puede estar configurada además para emitir información de solicitud en base a información de identificación de huella dactilar correspondiente a la información de huella dactilar en una secuencia predeterminada de reconocimiento de huella dactilar o una secuencia de reconocimiento aleatoria. La información de solicitud se utiliza para solicitar que se introduzca la información de huella dactilar correspondiente a la información de identificación de huella dactilar.

Vale la pena señalar que la implementación del dispositivo actual corresponde a la implementación del método anterior. Para más detalles, se puede hacer referencia a las descripciones correspondientes en la FIG. 5. Para facilitar la lectura, los detalles en la implementación del método anterior se omiten en la implementación del dispositivo actual. Sin embargo, debería quedar claro que el dispositivo en la presente implementación puede implementar correspondientemente todo el contenido en la implementación del método anterior.

El dispositivo para la autenticación de identidad incluye un procesador y una memoria. La unidad de selección, la unidad de recepción, la unidad de coincidencia, la unidad de confirmación, la unidad de detección, la unidad de salida, la unidad de registro, etc. se almacenan en la memoria como unidades de programa, y el procesador ejecuta las unidades de programa almacenadas en la memoria para implementar las funciones correspondientes.

El procesador incluye un núcleo y el núcleo invoca una unidad de programa correspondiente de la memoria. Puede haber uno o más núcleos y los parámetros del núcleo se ajustan para resolver el problema de que la autenticación de identidad realizada utilizando solo una huella dactilar fija es muy arriesgada y menos segura, y no puede satisfacer un requisito de usuario de privacidad o seguridad relativamente alta.

La memoria puede incluir una memoria no permanente, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil en un medio legible por computadora, por ejemplo, una memoria de solo lectura (ROM) o una memoria flash (flash RAM). La memoria incluye al menos un chip de almacenamiento.

De acuerdo con otro dispositivo para la autenticación de identidad proporcionado en la presente implementación de la presente divulgación, cuando es necesario realizar la autenticación de identidad, primero se selecciona una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; luego, se recibe una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; a continuación, la cantidad predeterminada recibida de información de huella dactilar se compara con la cantidad predeterminada seleccionada de información de huella dactilar; y se confirma que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar. En comparación con un método actual en el que solo se utiliza una huella dactilar fija para la autenticación de identidad, en la presente divulgación, se registra una pluralidad de piezas de información de huella dactilar de un usuario, de modo que cuando el usuario necesita un comportamiento de operación más seguro, una cantidad predeterminada de información de huella dactilar puede seleccionarse de la pluralidad de huellas dactilares registradas, se solicita al usuario que introduzca la información de huella dactilar del dedo correspondiente, y se puede completar una operación correspondiente cuando la información de huella dactilar coincida totalmente. Aumenta la complejidad de la autenticación de identidad, mejora la seguridad y puede satisfacer un requisito del usuario de privacidad o seguridad relativamente alta.

La presente solicitud proporciona además un producto de programa informático. Cuando se ejecuta en un dispositivo de procesamiento de datos, el producto de programa informático es aplicable para ejecutar código de programa para inicialización, que puede incluir los siguientes pasos del método: seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario; recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar; comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar; y confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

Un experto en la técnica debe comprender que las implementaciones de la presente solicitud pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente solicitud puede utilizar una forma de implementaciones de solo hardware, implementaciones de solo software o implementaciones con una combinación de software y hardware. Además, la presente solicitud puede utilizar una forma de producto de programa informático que se implementa en uno o más medios de almacenamiento utilizables por computadora (que incluyen, entre otros, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluyen código de programa utilizable por computadora.

La presente solicitud se describe con referencia a los diagramas de flujo y/o diagramas de bloques del método y dispositivo para la autenticación de identidad y el producto de programa informático de acuerdo con las implementaciones de la presente solicitud. Debe entenderse que se pueden utilizar instrucciones de programa informático para implementar cada uno de los procesos y/o cada uno de los bloques en los diagramas de flujo y/o los diagramas de bloques y una combinación de un proceso y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programa informático se pueden proporcionar para una computadora de propósito general, una computadora dedicada, un procesador integrado o un procesador de otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por una computadora o un procesador de otro dispositivo de procesamiento de datos programable generan un dispositivo para implementar una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático se pueden almacenar en una memoria legible por computadora que pueden instruir a la computadora u otro dispositivo de procesamiento de datos programable para trabajar de una manera específica, de modo que las instrucciones almacenadas en la memoria legible por computadora generen un artefacto que incluye un dispositivo de instrucción. El dispositivo de instrucción implementa una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Alternativamente, estas instrucciones de programa informático pueden cargarse en una computadora u otro dispositivo de procesamiento de datos programable, de modo que se ejecuten una serie de operaciones y pasos en la computadora o en el otro dispositivo programable, generando un procesamiento implementado por computadora. Por lo tanto, las instrucciones ejecutadas en la computadora o en el otro dispositivo programable proporcionan pasos para implementar una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

En una configuración típica, el dispositivo informático incluye uno o más procesadores (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria no permanente, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil en un medio legible por computadora, por ejemplo, una memoria de solo lectura (ROM) o una memoria flash (flash RAM). La memoria es un ejemplo del medio legible por computadora.

El medio legible por computadora incluye medios persistentes, no persistentes, móviles e inamovibles que pueden almacenar información utilizando cualquier método o tecnología. La información puede ser una instrucción legible por computadora, una estructura de datos, un módulo de programa u otros datos. Un ejemplo de un medio de almacenamiento informático incluye, entre otros, una memoria de acceso aleatorio de cambio de fase (PRAM), una memoria de acceso aleatorio estática (SRAM), una memoria de acceso aleatorio dinámica (DRAM), otro tipo de memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otra tecnología de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otro almacenamiento óptico, una cinta magnética en casete, almacenamiento en cinta y disco u otro dispositivo de almacenamiento magnético o cualquier otro medio que no sea de transmisión que pueda configurarse para almacenar información a la que puede acceder un dispositivo informático. Como se describe en la memoria descriptiva, el medio legible por computadora no incluye un medio legible por computadora transitorio (medio transitorio) tal como una señal de datos modulada y un portador.

Las descripciones anteriores son simplemente implementaciones de la presente solicitud. Para un experto en la técnica, la presente solicitud puede tener diversos cambios.

REIVINDICACIONES

1. Un método para la autenticación de identidad, el método que comprende:
seleccionar (101) una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario;
emitir, en una secuencia predeterminada de reconocimiento de huella dactilar o en una secuencia de reconocimiento aleatoria, información de solicitud de entrada de huella dactilar en base a información de identificación de huella dactilar, la información de solicitud de entrada de huella dactilar corresponde a la cantidad predeterminada seleccionada de información de huella dactilar, en donde la información de solicitud de entrada de huella dactilar se utiliza para solicitar que el usuario introduzca sucesivamente información de huella dactilar correspondiente a la información de identificación de huella dactilar;
recibir (102, 205) una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar, la cantidad predeterminada recibida de información de huella dactilar pertenece a una pluralidad de huellas dactilares recibidas del usuario;
Comparar (103, 206) la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar, en donde comparar (103, 206) comprende comparar sucesivamente cada una de las informaciones de huella dactilar introducida en respuesta a una petición de solicitud con una huella dactilar correspondiente de la cantidad predeterminada seleccionada de la información de huella dactilar;
confirmar (104, 207) que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar, en donde confirmar (104, 207) comprende confirmar que la autenticación de identidad tiene éxito cuando cada una de las informaciones de huella dactilar introducida en respuesta a la petición de solicitud coincide sucesivamente con una huella dactilar registrada correspondiente de la cantidad predeterminada seleccionada de la información de huella dactilar, antes de que se solicite la siguiente información de huella dactilar a ser introducida; y
Indicar un error de autenticación de identidad si una información de huella dactilar actual de la información de huella dactilar introducida en respuesta a una petición de solicitud actual no coincide con una huella dactilar correspondiente de la información de huella dactilar predeterminada seleccionada.

2. El método de acuerdo con la reivindicación 1, que comprende, además:
detectar si la información de huella dactilar introducida por el usuario se recibe dentro de un período de tiempo predeterminado cada vez que se emite información de solicitud; y
en caso negativo, confirmar que la autenticación de identidad falla y emitir información de alarma que indica que una operación expira el tiempo.

3. El método de acuerdo con la reivindicación 1, que comprende además:
confirmar que la autenticación de identidad falla y emitir información de alarma que indica que la autenticación de identidad falla cuando la cantidad predeterminada recibida de información de huella dactilar no coincide con la cantidad predeterminada seleccionada de información de huella dactilar.

4. El método de acuerdo con la reivindicación 1, en donde antes de seleccionar la cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario, el método comprende, además:
detectar si el usuario inicia sesión actualmente; y
en caso negativo, emitir información solicitando al usuario que inicie sesión utilizando una cuenta; y
la selección de una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario comprende:
en caso afirmativo, obtener información de cuenta de inicio de sesión del usuario; y
seleccionar una cantidad predeterminada de información de huella dactilar de una pluralidad de huellas dactilares registradas correspondientes a la información de cuenta.

5. El método de acuerdo con la reivindicación 1, en donde antes de seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario, el método comprende, además:
registrar (201) cada una de las informaciones de huella dactilar introducida por el usuario y la información de identificación de huella dactilar correspondiente a cada una de las informaciones de huella dactilar;
detectar (202) si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada en un proceso de registro de la información de huella dactilar introducida por el usuario; y
en caso afirmativo, detener (203) el registro de la información de huella dactilar introducida actualmente y emitir información de alarma que indica que se ha introducido repetidamente una huella dactilar.

6. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en donde la información de identificación de huella dactilar comprende un nombre o un número de identidad (ID) asociado con la huella dactilar.

7. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en donde la cantidad predeterminada de información de huella dactilar se selecciona en base a un nivel de seguridad.

8. Un dispositivo para la autenticación de identidad, el dispositivo que comprende una pluralidad de módulos configurados para realizar el método de una cualquiera de las reivindicaciones 1 a 7.

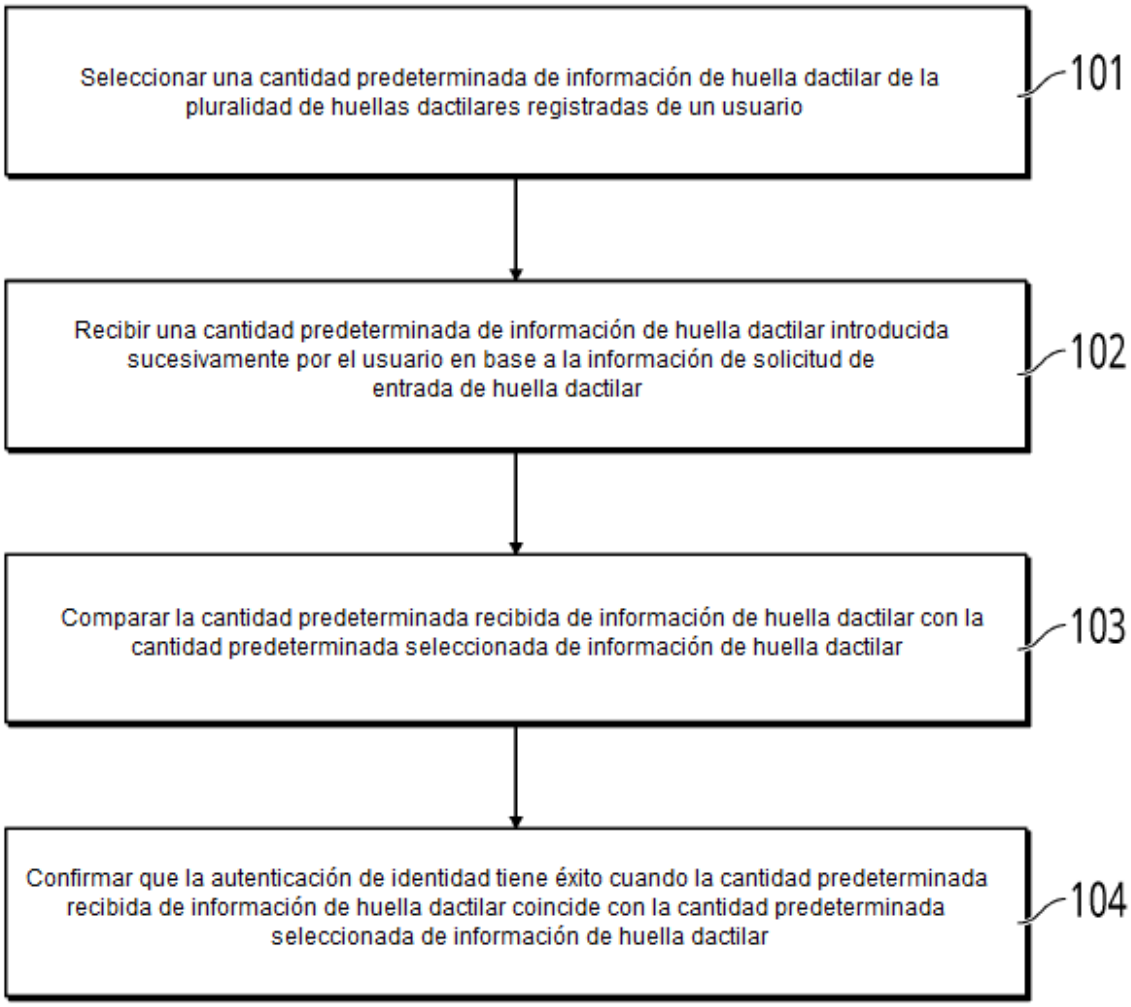
Seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario
101
Recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar
102
Comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar
103
Confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar
104

FIG. 1


China Unicom
16:00
60%
Pago con huella dactilar
1
Por favor, introduzca información de huella dactilar del dedo índice derecho
Cancelar

FIG. 2

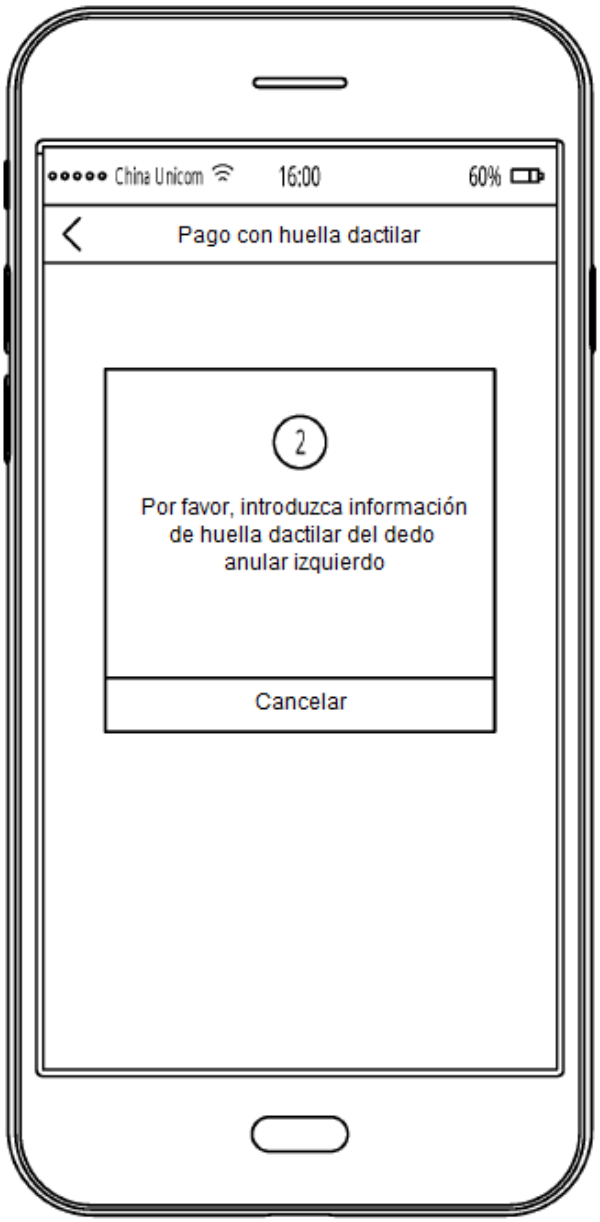
China Unicom
16:00
60%
Pago con huella dactilar
2
Por favor, introduzca información de huella dactilar del dedo anular izquierdo
Cancelar

FIG. 3


China Unicom
16:00
60%
Pago con huella dactilar
Pago con éxito
Cancelar

FIG. 4

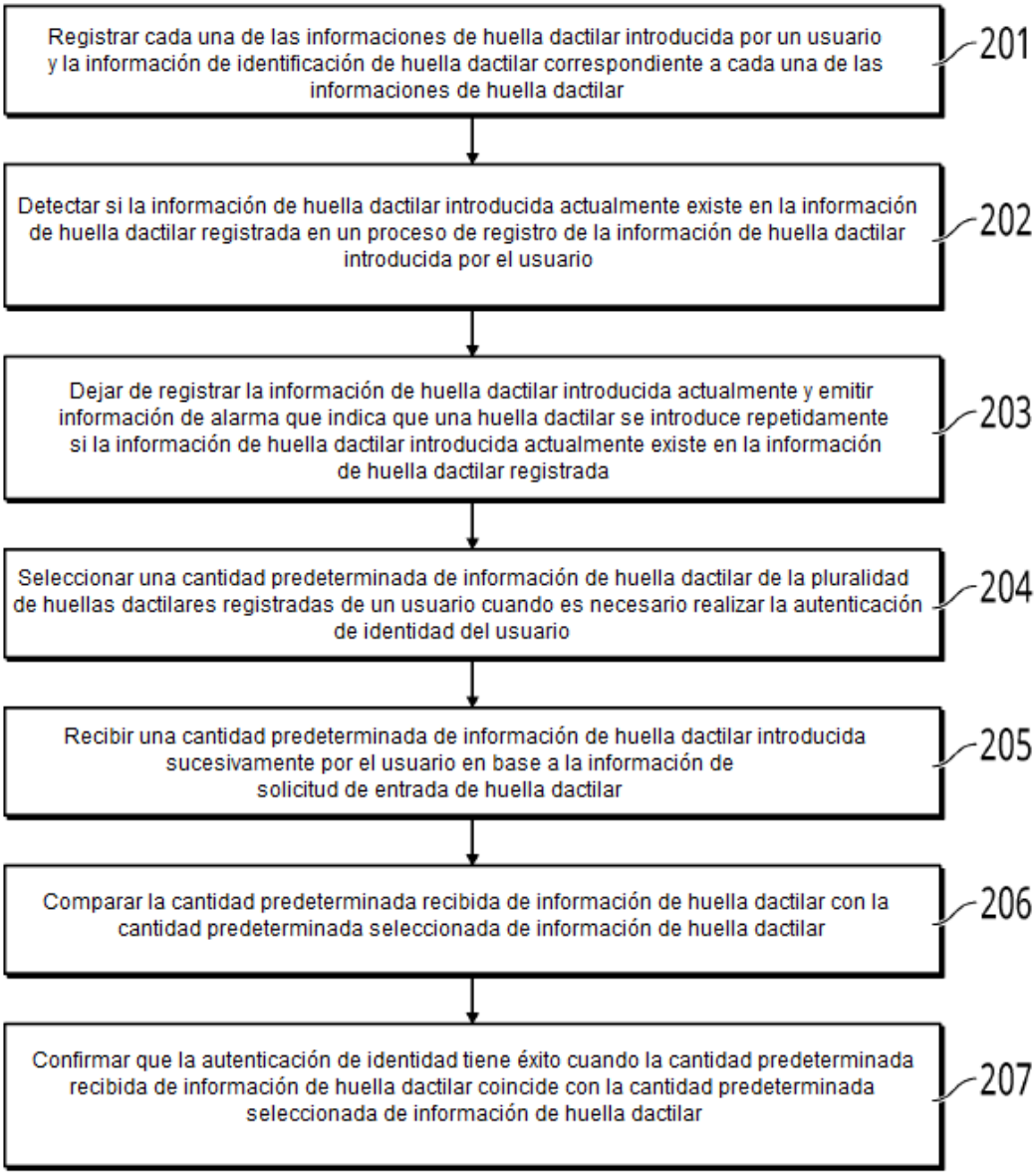
Registrar cada una de las informaciones de huella dactilar introducida por un usuario y la información de identificación de huella dactilar correspondiente a cada una de las informaciones de huella dactilar
201
Detectar si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada en un proceso de registro de la información de huella dactilar introducida por el usuario
202
Dejar de registrar la información de huella dactilar introducida actualmente y emitir información de alarma que indica que una huella dactilar se introduce repetidamente si la información de huella dactilar introducida actualmente existe en la información de huella dactilar registrada
203
Seleccionar una cantidad predeterminada de información de huella dactilar de la pluralidad de huellas dactilares registradas de un usuario cuando es necesario realizar la autenticación de identidad del usuario
204
Recibir una cantidad predeterminada de información de huella dactilar introducida sucesivamente por el usuario en base a la información de solicitud de entrada de huella dactilar
205
Comparar la cantidad predeterminada recibida de información de huella dactilar con la cantidad predeterminada seleccionada de información de huella dactilar
206
Confirmar que la autenticación de identidad tiene éxito cuando la cantidad predeterminada recibida de información de huella dactilar coincide con la cantidad predeterminada seleccionada de información de huella dactilar
207

FIG. 5

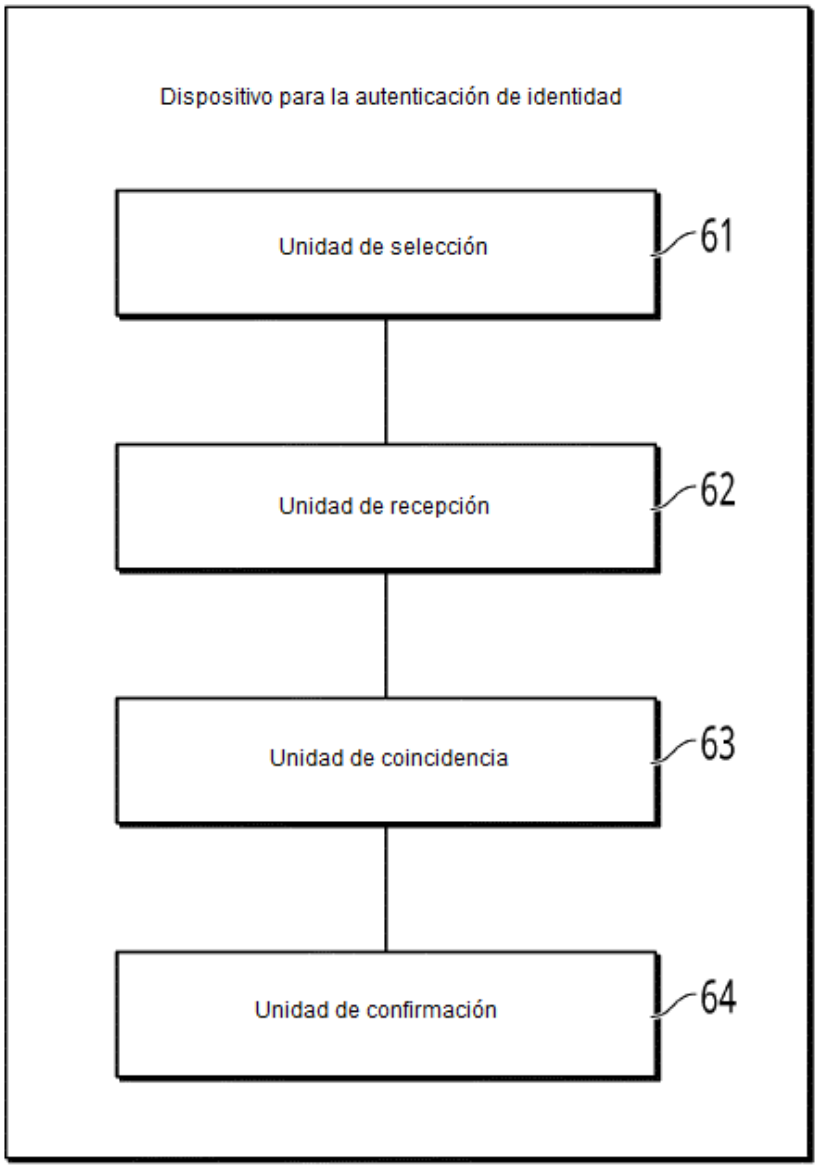
Dispositivo para la autenticación de identidad
Unidad de selección
61
Unidad de recepción
62
Unidad de coincidencia
63
Unidad de confirmación
64

FIG. 6

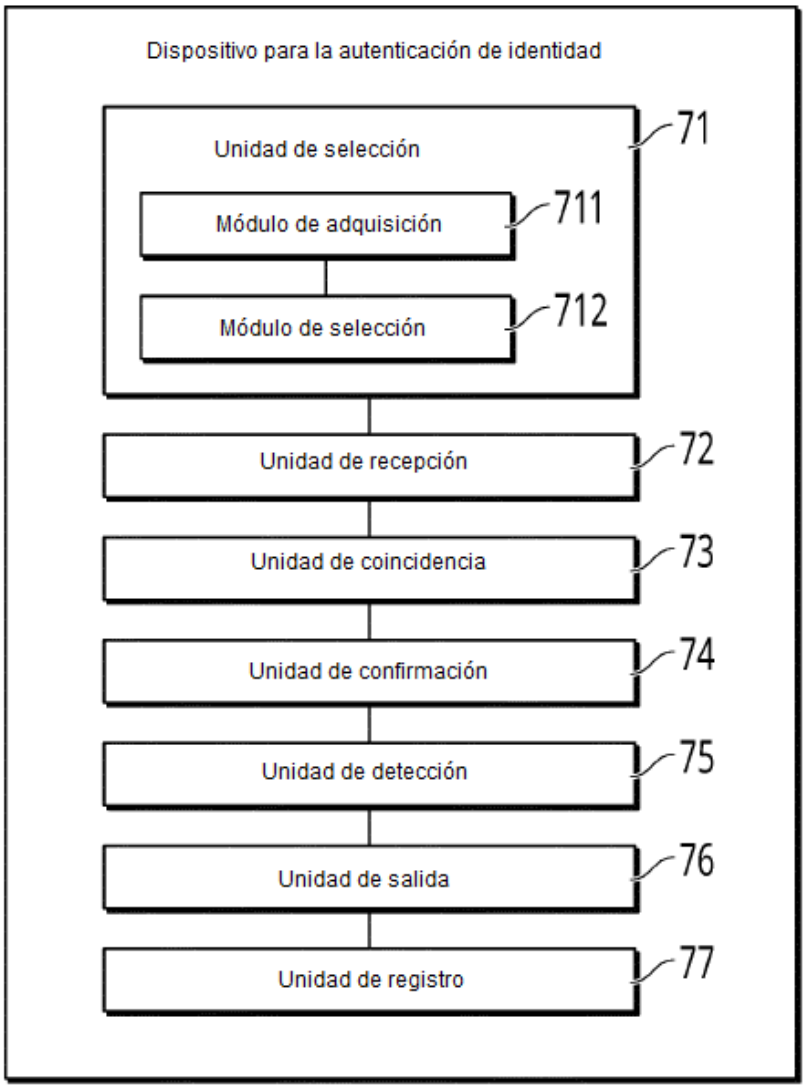
Dispositivo para la autenticación de identidad
Unidad de selección
71
Módulo de adquisición
711
Módulo de selección
712
Unidad de recepción
72
Unidad de coincidencia
73
Unidad de confirmación
74
Unidad de detección
75
Unidad de salida
76
Unidad de registro
77

FIG. 7