(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 810 012**

(51) Int. CI.:

G06F 21/32 (2013.01)
G06F 21/30 (2013.01)
G06F 21/35 (2013.01)
G06F 21/45 (2013.01)
G06K 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.08.2015 E 19172346 (9)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2020 EP 3540621**

(54) Título: **Método y aparato de autentificación de identidad, terminal y servidor**

(30) Prioridad:

03.09.2014 CN 201410446657

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2021

(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:

DU, ZHIJUN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método y aparato de autentificación de identidad, terminal y servidor

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de comunicación y, en particular, a los métodos y aparatos de autenticación de identidad, terminales y servidores.

Antecedentes

Con el crecimiento de terminales inteligentes y el desarrollo de aplicaciones de red, un usuario puede acceder a diversos tipos de aplicaciones de red, tales como aplicaciones de comunicación instantánea de tipo social y aplicaciones de tipo comercial, a través de diversos tipos de terminales de cliente de aplicación que se instalan en un terminal. Durante un acceso, la identidad de un usuario en general necesita ser autenticada, de tal modo que el usuario pueda utilizar diversas funciones de aplicación después de que la autenticación de la identidad es exitosa.

En las tecnologías existentes, un usuario en general necesita ingresar una contraseña de autenticación en una interfaz de autenticación durante la autenticación de identidad, y un servidor confirma que el usuario pasa la autenticación de identidad tras verificar que la contraseña de autenticación ingresada es la misma que la contraseña de autenticación durante el registro del usuario. Sin embargo, una contraseña de autenticación es en general una combinación simple de números y letras, y es robada fácilmente por un tercero malintencionado. Por lo tanto, los métodos existentes de modo de autenticación de identidad son relativamente pobres en confiabilidad y son propensos a causar el robo de información del usuario, lo cual resulta en una seguridad de autenticación pobre.

El documento WO 2013/100699 (A1) divulga un método para autenticar a un usuario. El método de autenticación del usuario incluye la obtención de una imagen que incluye un rostro y un movimiento del rostro al manejar una cámara para extraer información característica en una imagen facial y un patrón de movimiento a partir de la imagen obtenida, y comparar la información característica extraída en la imagen facial con la información característica en una imagen facial registrada en un almacenamiento y, cuando la información característica extraída coincide con la información característica registrada, compara el patrón de movimiento extraído con un patrón de movimiento registrado en el almacenamiento y, cuando el patrón de movimiento extraído coincide con el patrón de movimiento registrado, desbloquea un dispositivo.

El documento US 2014/059673 (A1) divulga un sistema y un método para proporcionar autorización segura a un dispositivo electrónico mediante la combinación de dos o más características de seguridad de autenticación procesadas sustancialmente al mismo tiempo cuando al menos uno de los factores es un factor “tolerante”. Al combinar dos factores, tales como el reconocimiento facial y un gesto de pantalla, se pueden analizar sustancialmente al mismo tiempo, excepto cuando se detecta un movimiento único o individualizado.

El documento US 2013/239187 (A1) divulga métodos y sistemas para facilitar la entrada segura del PIN de un usuario para transacciones electrónicas tales como el pago del comerciante, la autorización de pago, o la autorización de acceso. Una respuesta fisiológica del usuario puede indicar cuál de una secuencia aleatoria de números es un número del PIN del usuario. Por ejemplo, el usuario puede pestañear, parpadear o hacer un movimiento facial sutil para proporcionar la indicación.

El documento US 2012/281885 (A1) divulga sistemas para realizar la verificación del interlocutor. Un sistema configurado para practicar el método recibe una solicitud para verificar un interlocutor, genera un estímulo de texto que es único para la solicitud y, en respuesta a la solicitud, indica al interlocutor que pronuncie el estímulo de texto. Luego, el sistema registra una característica de imagen dinámica del interlocutor a medida que el interlocutor pronuncia el estímulo de texto, y realiza la verificación del interlocutor con base en la característica de imagen dinámica y el estímulo de texto. La grabación de la característica de imagen dinámica del interlocutor puede incluir la grabación de video del interlocutor a la vez que habla el estímulo de texto. La característica dinámica puede incluir un patrón de movimiento de cabeza, labios, boca, ojos y/o cejas del interlocutor. La característica de imagen dinámica puede relacionarse con el contenido fonético del interlocutor que habla el estímulo, la métrica de la charla y la expresión facial del interlocutor que responde al contenido del estímulo.

Resumen

La presente solicitud proporciona un método, un aparato, un terminal y un servidor para la autenticación de identidad, para resolver los problemas de mala confiabilidad y baja seguridad de los métodos de autenticación de identidad en las tecnologías existentes.

De acuerdo con un primer aspecto de las realizaciones de la presente solicitud, se proporciona un método de autenticación de identidad como se reivindica en la Reivindicación 1.

De acuerdo con un segundo aspecto de las realizaciones de la presente solicitud, se proporciona un método de autenticación de identidad de acuerdo con la Reivindicación 6.

De acuerdo con un tercer aspecto de las realizaciones de la presente solicitud, se proporciona un aparato de autenticación de identidad de acuerdo con la Reivindicación 8.

De acuerdo con un cuarto aspecto de las realizaciones de la presente solicitud, se proporciona un terminal de acuerdo con la Reivindicación 11.

De acuerdo con un quinto aspecto de las realizaciones de la presente solicitud, se proporciona un servidor de acuerdo con la Reivindicación 12.

Breve descripción de los dibujos

La Figura 1 es un diagrama esquemático de un escenario de autenticación de identidad de acuerdo con una realización de la presente solicitud.

La Figura 2A es un diagrama de flujo de un método de autenticación de identidad de ejemplo de acuerdo con la presente solicitud.

La Figura 2B es un diagrama de flujo de otro método de autenticación de identidad de ejemplo de acuerdo con la presente solicitud.

La Figura 3A es un diagrama de flujo de otro ejemplo de método de autenticación de identidad de acuerdo con la presente solicitud.

La Figura 3B es un diagrama esquemático de un gesto de cabeza humana durante la autenticación del rostro humano en una realización de la presente solicitud.

La Figura 4A es un diagrama de flujo de otro ejemplo de método de autenticación de identidad de acuerdo con la presente solicitud.

La Figura 4B y la Figura 4C son diagramas esquemáticos de puntos clave faciales en una realización de la presente solicitud.

La Figura 5 es un diagrama estructural que ilustra el hardware de un dispositivo donde se ubica un aparato de autenticación de identidad de acuerdo con la presente solicitud.

La Figura 6 es un diagrama de bloques de un ejemplo de aparato de autenticación de identidad de acuerdo con la presente solicitud.

La Figura 7 es un diagrama de bloques de otro ejemplo de aparato de autenticación de identidad de acuerdo con la presente solicitud.

Descripción detallada

Las realizaciones de ejemplo se describirán en el presente documento en detalle, y ejemplos de las mismas se representan en los dibujos adjuntos. Cuando la siguiente descripción involucra los dibujos adjuntos, los números idénticos en diferentes dibujos que acompañan representan elementos idénticos o similares, a menos que se especifique lo contrario. Las implementaciones descritas en las siguientes realizaciones de ejemplo no representan todas las implementaciones que son coherentes con la presente solicitud. Por el contrario, son simplemente ejemplos de aparatos y métodos coherentes con algunos aspectos de la presente solicitud como se describe en detalle en las reivindicaciones adjuntas.

Los términos utilizados en la presente solicitud se utilizan simplemente para describir realizaciones específicas en lugar de limitar la presente solicitud. Las formas singulares “a”, “el” y “dicho” que se utilizan en la presente solicitud y las reivindicaciones adjuntas también pretenden incluir formas plurales, a menos que el contexto indique claramente otros significados. Debe entenderse además que, el término “y/o” utilizado en el presente documento se refiere a, e incluye cualquiera o todas las combinaciones posibles de uno o más artículos asociados enumerados.

Debe entenderse que, aunque se pueden utilizar términos tales como “primero”, “segundo” y “tercero” para describir diversos tipos de información en la presente solicitud, esas piezas de información no se limitan estos términos. Estos términos se utilizan simplemente para distinguir información del mismo tipo entre sí. Por ejemplo, sin apartarse del alcance de la presente solicitud, la primera información también puede denominarse como segunda información y, de manera similar, la segunda información puede denominarse alternativamente como primera información. Dependiendo en el contexto, “si” como se utiliza en el presente documento puede interpretarse como “cuando”, “a la vez que” o “en respuesta a la determinación de eso”.

En un escenario de comunicación con base en Internet, un usuario puede acceder a diversos tipos de aplicaciones de red a través de diversos tipos de terminales de aplicación instalados en un terminal de la misma. Durante un proceso de acceso, una identidad del usuario en general necesita ser autenticada. Sin embargo, en las tecnologías existentes, la identidad de un usuario en general se autentica a través de una contraseña de autenticación, y la contraseña de

autenticación es en general una combinación simple de números y letras, la cual es robada fácilmente por un tercero malintencionado. Por lo tanto, los métodos de autenticación de identidad existentes son relativamente poco confiables y tienen poca seguridad. En consecuencia, con referencia a la Figura 1, la cual es un diagrama esquemático de un escenario de aplicación para implementar la autenticación de identidad de acuerdo con una realización de la presente solicitud, la autenticación de identidad para un usuario se completa a través de interacciones entre un terminal mantenido de ese modo y un servidor. Las comunicaciones entre el terminal y el servidor pueden completarse con base en una red. La red incluye diversos tipos de redes inalámbricas o redes por cable, las cuales no están limitadas en las realizaciones de la presente solicitud. El terminal puede ser un teléfono móvil, una tableta, un ordenador personal, etc. En el escenario de aplicación como se muestra en la Figura 1, se pueden implementar dos bases de datos en el servidor, las cuales son una base de datos de información de rasgos faciales humanos y una base de datos de información rápida de autenticación dinámica del rostro humano, respectivamente.

En una fase de registro del rostro, el terminal puede adquirir información de rasgos faciales humanos de un usuario registrado, la cual se envía al servidor. El servidor almacena la información de rasgos faciales humanos del usuario registrado en la base de datos de información de rasgos faciales. En una fase de autenticación de identidad, la autenticación del rostro humano se puede realizar primero. En este punto, un usuario envía información de rasgos faciales humanos adquirida al servidor. Una vez que se verifica que la información de rasgos faciales humanos coincide con la información de rasgos faciales humanos del usuario que se almacena en los datos de información de rasgos faciales, el servidor puede determinar de manera preliminar que una autenticación de identidad se realiza actualmente en el propio usuario. Luego se realiza la autenticación dinámica del rostro humano. En este punto, el servidor puede regresar al usuario la información rápida de autenticación dinámica del rostro humano adquirida a partir de la base de datos de información rápida de autenticación dinámica del rostro humano. El terminal reconoce un gesto facial humano presentado por el usuario para obtener información de reconocimiento de gestos de la información rápida de autenticación dinámica del rostro humano, y envía la información de reconocimiento de gestos al servidor. Tras verificar que la información de reconocimiento de gestos es coherente con la información rápida de autenticación dinámica del rostro humano, el servidor sabe que el usuario actual que se autenticará es un usuario en vivo, así finalmente determina que la autenticación de identidad del usuario es exitosa. Para facilitar la descripción, en las realizaciones de la presente solicitud, la información de rasgos faciales humanos de un usuario adquirida en la fase de registro del rostro se denomina como segunda información de rasgos faciales humanos, y la información de rasgos faciales humanos del usuario adquirida en la fase de autenticación facial se denomina como la primera información de rasgos faciales humanos. Las realizaciones de la presente solicitud se describen en detalle a continuación.

La Figura 2A es un diagrama de flujo de una realización de un método de autenticación de identidad de acuerdo con la presente solicitud. Esta realización se describe a partir de la perspectiva de un terminal que implementa una autenticación de identidad.

La etapa 201 recibe información rápida de autenticación dinámica del rostro humano enviada por un servidor durante la autenticación de identidad de un usuario.

En esta realización de la presente solicitud, el servidor puede extraer aleatoriamente información rápida de autenticación dinámica del rostro humano a partir de datos de información rápida de autenticación dinámica del rostro humano y regresa la información rápida de autenticación dinámica del rostro humano al terminal. La información rápida de autenticación dinámica del rostro humano puede incluir al menos un tipo de la siguiente información: información rápida de acción de expresión, tal como cerrar el(los) ojo(s), abrir la boca o girar la cabeza; o información rápida de lectura de voz, tal como hacer un pago de 20 dólares.

Opcionalmente, antes de recibir la información rápida de autenticación dinámica del rostro humano del servidor, el terminal puede primero adquirir información de rasgos faciales humanos del usuario, y utilizar la información de rasgos faciales humanos adquirida durante la autenticación de identidad como primera información facial humana del usuario. Después de que la primera información de rasgos faciales humanos del usuario se envía al servidor, el servidor envía la información rápida de autenticación dinámica del rostro humano al terminal cuando verifica que la primera información de rasgos faciales humanos coincide con la segunda información de rasgos faciales almacenada.

Cuando se adquiere información de rasgos faciales humanos del usuario, el terminal puede iniciar un dispositivo de generación de imagen integrado al mismo, tal como una cámara, para detectar un rostro humano del usuario y seguir el rostro humano del usuario cuando se detecta el rostro humano. Durante el seguimiento del rostro humano, el terminal adquiere imágenes del rostro humano de acuerdo con un intervalo de tiempo preestablecido, determina si una imagen del rostro respectiva cumple una condición de extracción de característica preestablecida para cada imagen del rostro adquirida, y extrae información de rasgos faciales humanos del usuario a partir de esa imagen del rostro si esa imagen del rostro cumple la condición de extracción de característica.

Después de recibir la primera información de rasgos faciales humanos del usuario, el servidor puede buscar en la base de datos de información de rasgos faciales con base en el nombre de usuario del usuario para obtener la segunda información de rasgos faciales correspondiente al nombre de usuario, y luego compara la primera información de rasgos faciales humanos y la segunda información de rasgos faciales humanos utilizando un enfoque de comparación predefinido. Si un valor de comparación de características cae dentro de un rango de similitud preestablecido, se puede determinar que la primera información de rasgos faciales humanos coincide con la segunda información de

rasgos faciales. En respuesta a la determinación de que la primera información de rasgos faciales humanos coincide con la segunda información de rasgos faciales humanos, se puede determinar que la autenticación del rostro humano es exitosa para el usuario. En este caso, el servidor envía la información rápida de autenticación dinámica del rostro humano al terminal.

La etapa 202 obtiene información de reconocimiento de gestos de la información rápida de autenticación dinámica del rostro humano mediante el reconocimiento de un gesto facial presentado por el usuario.

En esta realización de la presente solicitud, después de recibir la información rápida de autenticación dinámica del rostro humano, el terminal muestra la información rápida de autenticación dinámica del rostro humano en una interfaz de autenticación de identidad. El usuario puede presentar un gesto facial humano correspondiente de acuerdo con la información. Cuando reconoce el gesto facial humano, el terminal puede seguir el rostro humano del usuario para obtener información de seguimiento del rostro. La información de seguimiento del rostro humano puede incluir al menos uno de la información de posición del punto clave facial e información del gesto de cabeza humana. Luego, el terminal obtiene información de reconocimiento del gesto del usuario analizando la información de seguimiento del rostro humano. Por ejemplo, a través de la información de posición del punto clave facial, puede conocerse si el usuario cierra el(los) ojo(s) o abre la boca de acuerdo con la información rápida de acción de expresión, o puede conocerse la forma de la boca del usuario cuando lee la información rápida de lectura de voz (existe una relación de correspondencia entre la pronunciación y la forma de la boca de cada palabra, y la información de reconocimiento de gestos del usuario puede determinarse con base en la forma de la boca). Además, se puede saber si el usuario gira su cabeza, baja la cabeza, etc., a través de la información del gesto de la cabeza.

La etapa 203 envía la información de reconocimiento del gesto al servidor para permitir que el servidor confirme que la autenticación de identidad es exitosa para el usuario, tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro humano.

El servidor puede necesitar realizar autenticación de identidad para diversos usuarios al mismo tiempo. Si se envían diferentes piezas de información rápida de autenticación dinámica a diferentes usuarios, el servidor puede registrar una relación de correspondencia entre el nombre de usuario del usuario y la información rápida de autenticación dinámica del rostro humano después de enviar la información rápida de autenticación dinámica del rostro humano al terminal en la etapa 201. En esta etapa, después de que el terminal envía la información de reconocimiento del gesto al servidor, el servidor adquiere la información rápida de autenticación dinámica del rostro humano correspondiente de acuerdo con el nombre de usuario del usuario y verifica que la información de reconocimiento del gesto sea coherente con la información rápida de autenticación dinámica del rostro humano. Esto indica que el usuario es un usuario en vivo y, en este caso, se determina que la autenticación de identidad es exitosa para el usuario.

Además, si la información rápida de autenticación dinámica del rostro humano en la etapa 201 es información rápida de lectura de voz, el terminal también puede obtener información de audio del usuario además de la forma de la boca del usuario. Mediante el reconocimiento de voz de la información de audio, se obtiene la información de voz leída por el usuario, de tal modo que el servidor puede comparar si la información de voz es coherente con la información rápida de lectura de voz, y determinar que la autenticación de identidad es exitosa para el usuario si estos son coherentes.

La Figura 2B es un diagrama de flujo de otra realización de un método de autenticación de identidad de acuerdo con la presente solicitud. Esta realización se describe a partir la perspectiva de un servidor que implementa la autenticación de identidad:

La etapa 211 envía información rápida de autenticación dinámica del rostro humano a un terminal cuando se realiza una autenticación de identidad de un usuario.

La etapa 212 recibe información de reconocimiento del gesto enviada por el terminal, siendo la información de reconocimiento del gesto información de reconocimiento del gesto obtenida por el terminal a través del reconocimiento de un gesto facial humano que es presentado por el usuario de acuerdo con la información rápida de autenticación dinámica del rostro humano.

La etapa 213 determina que la autenticación de identidad del usuario es exitosa tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro humano.

Cabe señalar que, la única diferencia entre el proceso de autenticación de identidad como se muestra en la Figura 2B y el proceso de autenticación de identidad como se muestra en la Figura 2A es una diferencia en las entidades de ejecución. Específicamente, la Figura 2A se describe a partir de la perspectiva de un terminal, a la vez que la Figura 2B se describe a partir de la perspectiva de un servidor. Por lo tanto, los procesos relacionados de implementaciones en la realización de la Figura 2B puede hacer referencia a la descripción anterior de la Figura 2A, y no se describen repetidamente en este documento.

Como puede verse a partir de la realización anterior, esta realización puede realizar la autenticación de identidad de usuario que tiene una alta seguridad a través de autenticación dinámica del rostro humano. En comparación con los métodos de autenticación existentes que utilizan una contraseña de autenticación, un tercero malintencionado no robará la información de autenticación, lo que mejorará la confiabilidad de la autenticación. Además, un usuario puede

ser reconocido como un usuario en vivo a través de la autenticación dinámica del rostro humano, mejorando así la precisión de la autenticación de identidad y reduciendo los riesgos potenciales de seguridad durante la autenticación.

La Figura 3A es otra realización de un método de autenticación de identidad de acuerdo con la presente solicitud. Esta realización ilustra un proceso de registro del rostro humano en detalle.

Etapa 301: Un usuario se registra con un servidor a través de un terminal.

Etapa 302: El terminal sigue el rostro humano del usuario cuando se detecta el rostro humano del usuario.

En general, un dispositivo de generación de imagen, tal como una cámara, está integrado en el terminal. En esta realización, el dispositivo de generación de imagen puede configurarse para que inicie automáticamente para que detecte un rostro humano del usuario de forma predeterminada durante el registro del usuario. En general, el usuario puede sostener el terminal con una mano para alinear el dispositivo de generación de imagen con el rostro del usuario. Cuando se detecta el rostro a través del dispositivo de generación de imagen, el terminal puede seguir el rostro del usuario de acuerdo con un algoritmo de seguimiento del rostro humano. Debe observarse que esta realización de la presente solicitud puede emplear diversos tipos de algoritmos de seguimiento del rostro existentes, los cuales no se describen en detalle en el presente documento.

Etapa 303: El terminal adquiere una imagen del rostro de acuerdo con un intervalo de tiempo preestablecido durante el seguimiento del rostro.

Durante el seguimiento del rostro, el terminal adquiere imágenes del rostro de acuerdo con un intervalo de tiempo preestablecido utilizando el dispositivo de generación de imagen. El intervalo de tiempo se define para impedir la extracción de imágenes del rostro que son sustancialmente las mismas. Por ejemplo, el intervalo de tiempo preestablecido puede ser de 3 segundos.

Etapa 304: Se determina si una resolución de la imagen del rostro cumple con un umbral de resolución preestablecido. Si es afirmativo, se realiza la etapa 305. De lo contrario, el proceso actual finaliza.

Una resolución de la imagen del rostro adquirida en la etapa 303 puede examinarse primero para eliminar la(s) imagen(es) del rostro que tiene(n) una resolución insuficiente. En este caso, el terminal puede invocar una función de determinación difusa preestablecida para determinar si la resolución de la imagen del rostro cumple con el umbral de resolución. Puede utilizarse una función de determinación difusa en una tecnología de procesamiento de reconocimiento de imagen existente para esta función de determinación difusa, la cual no está limitada en esta realización de la presente solicitud. Para una imagen del rostro que satisfaga el umbral de resolución, se realiza la etapa 305. Una imagen del rostro que no satisface el umbral de resolución se descarta directamente, y se regresa entonces a la etapa 303.

Etapa 305: El terminal extrae la información del gesto de la cabeza a partir de la imagen del rostro.

Después de determinar que la imagen del rostro adquirida es una imagen del rostro clara en la etapa 304, el terminal extrae información del gesto de la cabeza de la imagen del rostro. La Figura 3B muestra un diagrama esquemático de un gesto de la cabeza en una realización de la presente solicitud. La información del gesto de la cabeza en esta realización puede incluir al menos uno de los siguientes ángulos: un ángulo de descenso/elevación de la cabeza, un ángulo de giro del rostro y un ángulo de inclinación de la cabeza.

Etapa 306: El terminal determina si cada ángulo incluido en la información del gesto de la cabeza cae dentro de un rango de ángulo preestablecido respectivo. En caso afirmativo, se realiza la etapa 307. De lo contrario, el proceso actual finaliza.

En esta realización de la presente solicitud, se puede determinar si la imagen del rostro es una imagen del rostro frontal del usuario a través de la información del gesto de la cabeza. En este punto, el terminal puede determinar si cada ángulo incluido en la información del gesto de la cabeza cae dentro de un rango de ángulo preestablecido respectivo. Por ejemplo, un rango de ángulo preestablecido es de 0 a 10 grados. Para una imagen del rostro correspondiente a la información del gesto de la cabeza cuyo resultado de determinación es positivo, se realiza la etapa 307. Una imagen del rostro correspondiente a la información del gesto de la cabeza cuyo resultado de determinación es negativo se descarta directamente, y se regresa entonces a la etapa 303.

Etapa 307: El terminal extrae información de los rasgos faciales del usuario a partir de la imagen del rostro.

En esta realización de la presente solicitud, se puede emplear un algoritmo de extracción de característica de Retroproyección Lineal (LBP) para extraer valor(es) del vector de rasgos faciales a partir de la imagen del rostro como la información de la(s) característica(s) facial(es) del usuario. Aparentemente, esta realización de la presente solicitud no impone alguna de las limitaciones en un algoritmo específico para la extracción de rasgos faciales. Cualquier algoritmo de extracción de rasgos faciales utilizado en cualquier tecnología de procesamiento de imágenes existente puede ser aplicable a esta realización de la presente solicitud, tal como un algoritmo de extracción de característica de Gabor en transformada de Fourier con ventana, etc.

Para garantizar la precisión de la autenticación del rostro en la fase posterior de la autenticación de identidad, la información de rasgos faciales de un usuario puede extraerse a partir de múltiples imágenes del rostro para este mismo usuario registrado durante la fase de registro del rostro. El número de imágenes del rostro puede ser preestablecido, cinco, por ejemplo. De manera correspondiente, de acuerdo con el número establecido de imágenes del rostro, la etapa 303 anterior a la etapa 307 puede realizarse repetidamente para obtener un número de imágenes del rostro que cumpla con el número preestablecido, y para extraer información de rasgos faciales del mismo.

Etapa 308: El terminal envía la información de la(s) característica(s) facial(es) al servidor.

Etapa 309: El servidor almacena la(s) relación(es) de correspondencia entre un nombre de usuario del usuario registrado y los rasgos faciales, y finaliza el proceso actual.

En esta realización, después de recibir la información de la(s) característica(s) facial(es) a partir del terminal, el servidor puede almacenar la(s) relación(es) de correspondencia entre el nombre de usuario del usuario registrado y la(s) característica(s) facial(es) en la base de datos de información de rasgos faciales, y almacenar las relaciones de correspondencia entre el nombre de usuario y la información de múltiples rasgos faciales tras recibir la información de los múltiples rasgos faciales.

La Figura 4A es otra realización de un método de autenticación de identidad de acuerdo con la presente solicitud. Esta realización describe un proceso de autenticación de una identidad de un usuario en detalle, con base en el proceso de registro del rostro como se muestra en la Figura 3.

Etapa 401: Se inicia la autenticación de identidad de un usuario.

Etapa 402: Un terminal adquiere la primera información de rasgos faciales del usuario.

Durante la autenticación de identidad, el terminal adquiere la información de rasgos faciales del usuario utilizando un enfoque que es el mismo que el de adquirir información de rasgos faciales en el proceso de registro del rostro como se muestra en la Figura 3 anterior, y es específicamente el mismo como la etapa 302 a la etapa 307 como se muestra en la Figura 3. Los detalles de los mismos no se describen repetidamente en el presente documento.

En esta etapa, el terminal puede adquirir al menos una parte de la primera información de rasgos faciales.

Etapa 403: El terminal envía la primera información de rasgos faciales del usuario a un servidor.

Etapa 404: El servidor verifica si la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario que está almacenada. Si es afirmativo, se realiza la etapa 405. De lo contrario, se finaliza el proceso actual.

En esta realización de la presente solicitud, después de recibir la primera información de rasgos faciales del usuario, el servidor puede buscar la base de datos de información de rasgos faciales con base en un nombre de usuario del usuario para obtener la segunda información de rasgos faciales correspondiente al nombre de usuario, y luego comparar la primera información de rasgos faciales y la segunda información de rasgos faciales de una manera de comparación preestablecida. Si un valor de comparación de característica cae dentro de un rango de similitud preestablecido, se puede determinar que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales.

Se dice que la información de rasgos faciales en esta realización de la presente solicitud es un vector de rasgos faciales extraído a través del algoritmo LBP como un ejemplo.

En un caso, se puede utilizar una comparación de distancias Euclidianas para comparar la primera información de rasgos faciales y lo segundos rasgos faciales. En este caso, se calcula una suma de cuadrados de una diferencia entre un segundo vector de rasgos faciales y un primer vector de rasgos faciales. Si la suma de los cuadrados es menor que un umbral preestablecido, se puede determinar que la autenticación de identidad se realiza en el propio usuario.

En otro caso, se puede utilizar una comparación de distancias de coseno para comparar la primera información de rasgos faciales y la segunda información de rasgos faciales. Si un primer vector de rasgos faciales es V1 y un segundo vector de rasgos faciales es V2, se puede calcular el siguiente valor de fórmula: $V2 * V1/(|V1| * |V2|)$. Si el valor de la fórmula es mayor que un umbral preestablecido, se puede determinar que la autenticación de identidad se realiza en el propio usuario.

Etapa 405: El servidor envía información rápida de autenticación dinámica del rostro al terminal.

En respuesta a la verificación de que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales, el servidor confirma que la autenticación de identidad se realiza en el propio usuario y comienza a realizar un proceso de autenticación dinámica del rostro en este punto. El servidor puede extraer aleatoriamente una pieza de información rápida de autenticación dinámica del rostro a partir de la base de datos de información rápida de autenticación dinámica del rostro.

En esta realización, la información rápida de autenticación dinámica del rostro puede incluir información rápida de acción de expresión o información rápida de lectura de voz. Una acción incitada por la información rápida de acción de expresión es en general una acción que un usuario puede presentar fácilmente a través de un gesto facial, por ejemplo, abrir una boca, cerrar el(los) ojo(s), girar la cabeza, etc. Para la información rápida de lectura de voz, la información en general es corta, de tal modo que el usuario puede leerla fácilmente en voz alta durante la autenticación, y el terminal puede reconocer fácilmente un gesto facial del usuario cuando el usuario lo lee.

Etapa 406: El terminal obtiene información de seguimiento del rostro por seguimiento de un rostro del usuario.

Después de recibir la información rápida de autenticación dinámica del rostro, el terminal puede generar la información rápida de autenticación dinámica del rostro en una interfaz de autenticación. El usuario puede presentar un gesto facial correspondiente de acuerdo con la información. Durante la presentación, el terminal adquiere información de seguimiento facial del usuario a través de un algoritmo de seguimiento facial. La información de seguimiento del rostro puede incluir al menos un tipo de la siguiente información: información de posición del punto clave facial e información del gesto de la cabeza.

Etapa 407: El terminal analiza la información de seguimiento facial para obtener información de reconocimiento de gestos del usuario.

Por ejemplo, si la información rápida de autenticación dinámica del rostro es “abrir una boca”, el usuario correspondientemente realiza una acción de abrir la boca. El terminal puede obtener información de posición del punto clave facial, la cual es específicamente información de posición del punto clave de la boca, siguiendo el rostro del usuario. La Figura 4B y la Figura 4C son diagramas esquemáticos de información de la posición del punto clave facial en esta realización de la presente solicitud. La Figura 4B muestra información extraída de la(s) posición(es) del punto clave de una boca de un usuario en un estado normal. La Figura 4C muestra información extraída de la(s) posición(es) del punto clave de la boca del usuario después de que el usuario presenta un gesto de abrir la boca. Al comparar la información extraída respectiva de la(s) posición(es) del punto clave en la Figura 4B y la Figura 4C, es decir, al comparar las distancias de coordenadas respectivas entre las posiciones de los puntos clave superior e inferior de la boca, la información de reconocimiento de gestos del usuario se puede obtener como “abrir una boca”.

En otro ejemplo, si la información rápida de autenticación dinámica del rostro es “girar la cabeza”, el usuario correspondientemente realiza una acción de girar la cabeza. El terminal puede obtener información del gesto de la cabeza, la cual específicamente puede incluir tres ángulos como se muestra en la Figura 3B, siguiendo el rostro del usuario. Si los valores angulares de los tres ángulos cumplen con los rangos de valores de ángulo respectivos definidos por “girar la cabeza”, la información de reconocimiento de gestos del usuario se puede obtener como “girar la cabeza”.

Etapa 408: El terminal envía la información de reconocimiento de gestos al servidor.

Etapa 409: El servidor verifica si la información de reconocimiento de gestos es coherente con la información rápida de autenticación dinámica del rostro. Si es afirmativo, se ejecuta la etapa 410. De lo contrario, se finaliza el proceso actual.

Etapa 410: El servidor determina que la autenticación de identidad para el usuario es exitosa y se finaliza el proceso actual.

Como se puede ver en la realización anterior, esta realización combina la autenticación del rostro con la autenticación dinámica para realizar una autenticación de alta seguridad para la identidad de un usuario, y puede verificar preliminarmente si es el propio usuario a través de la autenticación del rostro. En comparación con los métodos de autenticación existentes que utilizan una contraseña de autenticación, un tercero malintencionado no roba fácilmente la información de autenticación, lo que mejora la confiabilidad de la autenticación. Además, después de que el usuario es confirmado, el usuario puede ser reconocido como un usuario en vivo a través de la autenticación dinámica del rostro, mejorando así la precisión de la autenticación de identidad y reduciendo los riesgos potenciales de seguridad durante la autenticación.

En correspondencia a las realizaciones de los métodos de autenticación de identidad en la presente solicitud, la presente solicitud proporciona además realizaciones de un aparato, un terminal y un servidor para la autenticación de identidad.

Una realización de un aparato de autenticación de identidad en la presente solicitud puede aplicarse individualmente a un terminal y un servidor. Una realización del aparato puede implementarse mediante software, o puede implementarse mediante hardware o una combinación de software y hardware. Una implementación de software se utiliza como ejemplo. Como un aparato lógico, el aparato está formado por el(los) procesador(es) de un dispositivo en el cual se ubica el aparato para leer las instrucciones correspondientes del programa de ordenador a partir de un almacenamiento no volátil en la memoria para su ejecución. La Figura 5 muestra un diagrama estructural de hardware de un dispositivo donde se ubica un aparato de autenticación de identidad de ejemplo de acuerdo con la presente solicitud a partir de la perspectiva del nivel de hardware. Además del(los) procesador(es), la memoria, una interfaz de red y un almacenamiento no volátil como se muestra en la Figura 5, el dispositivo donde se ubica el aparato en general puede incluir otros componentes de hardware adicionales de acuerdo con las funciones reales del dispositivo. Por

ejemplo, un terminal puede incluir una cámara, una pantalla táctil, un componente de comunicación, etc. Un servidor puede incluir un chip delantero responsable del procesamiento de paquetes, etc.

La Figura 6 muestra un diagrama de bloques de una realización de un aparato de autenticación de identidad de acuerdo con la presente solicitud. El aparato de autenticación de identidad puede aplicarse en un terminal. El aparato incluye una unidad 610 receptora, una unidad 620 de reconocimiento y una unidad 630 de envío.

La unidad 610 receptora está configurada para recibir información rápida de autenticación dinámica del rostro enviada por un servidor durante una autenticación de identidad de un usuario.

La unidad 620 de reconocimiento está configurada para obtener información de reconocimiento de gestos de la información rápida de autenticación dinámica del rostro mediante reconocimiento del gesto facial presentado por el usuario.

La unidad 630 de envío está configurada para enviar la información de reconocimiento del gesto al servidor para permitir que el servidor confirme que la autenticación de identidad del usuario es exitosa tras verificar que la información de reconocimiento del gesto sea coherente con la información rápida de autenticación dinámica del rostro.

En una implementación opcional, la unidad 620 de reconocimiento puede incluir (no se muestra en la Figura 6):

una subunidad de obtención de información del rostro configurada para obtener información de seguimiento del rostro mediante seguimiento del rostro del usuario cuando el usuario presenta un gesto facial de acuerdo con la información rápida de autenticación dinámica del rostro; y

una subunidad de análisis de información del rostro configurada para analizar la información de seguimiento facial para obtener información de reconocimiento del gesto del usuario.

La subunidad de análisis de información del rostro puede configurarse específicamente para obtener información de reconocimiento del gesto de expresión del usuario mediante el análisis de la información de posición del punto clave facial cuando la información de seguimiento del rostro es la información de posición del punto clave facial, u obtener información de reconocimiento de giro de la cabeza del usuario mediante el análisis de la información del gesto de la cabeza cuando la información de seguimiento del rostro es la información del gesto de la cabeza.

La información rápida de autenticación dinámica del rostro puede incluir al menos un tipo de la siguiente información: información rápida de acción de expresión, o información rápida de lectura de voz.

En otra implementación opcional, el aparato puede incluir además (no se muestra en la Figura 6) una unidad de adquisición configurada para adquirir información de rasgos faciales del usuario, y utilizar la información de rasgos faciales adquirida durante la autenticación de identidad como primera información de rasgos faciales del usuario.

La unidad 630 de envío puede configurarse adicionalmente para enviar la primera información de rasgos faciales del usuario al servidor para permitir que el servidor envíe la información rápida de autenticación dinámica del rostro tras verificar que la primera información de rasgos faciales coincida con la segunda información de rasgos faciales del usuario que está almacenada.

Opcionalmente, la unidad de adquisición puede configurarse adicionalmente para adquirir información de rasgos faciales del usuario cuando el usuario realiza el registro, y utilizar la información de rasgos faciales adquirida durante el registro como la segunda información de rasgos faciales del usuario. La unidad 630 de envío puede configurarse además para enviar la segunda información de rasgos faciales al servidor para permitir que el servidor almacene una relación de correspondencia entre el nombre de usuario del usuario y la segunda información de rasgos faciales.

Opcionalmente, la unidad de adquisición puede incluir una subunidad de seguimiento del rostro configurada para seguir el rostro del usuario cuando se detecta el rostro del usuario; una subunidad de adquisición de imagen configurada para adquirir una imagen del rostro de acuerdo con un intervalo de tiempo preestablecido durante el seguimiento del rostro; una subunidad de determinación de condición configurada para determinar si la imagen del rostro cumple con una condición de extracción de característica preestablecida; y una subunidad de extracción de característica configurada para extraer información de rasgos faciales del usuario a partir de la imagen del rostro en caso de que se cumpla la característica de condición de extracción.

La subunidad de determinación de condición puede incluir, además:

un módulo de determinación de resolución configurado para determinar si una resolución de la imagen del rostro cumple con un umbral de resolución preestablecido;

un módulo de extracción de información del gesto configurado para extraer información del gesto de la cabeza a partir de la imagen del rostro si se cumple el umbral de resolución, la información del gesto de la cabeza incluye al menos uno de los siguientes ángulos: un ángulo de descenso/elevación de la cabeza, un ángulo de giro del rostro o un ángulo de inclinación de la cabeza;

un módulo de determinación de ángulo configurado para determinar si cada ángulo que se incluye en la información del gesto de la cabeza cae dentro de un rango de ángulo preestablecido respectivo; y

un módulo de determinación de juicio configurado para determinar que la imagen del rostro cumple con la característica de condición de extracción si cada ángulo cae dentro del rango de ángulo preestablecido respectivo.

La subunidad de extracción de característica puede configurarse específicamente para extraer un valor de vector de rasgos faciales a partir de la imagen del rostro como la información de rasgos faciales del usuario utilizando un algoritmo de extracción de característica preestablecida, en donde el algoritmo de extracción de característica preestablecida puede incluir un algoritmo de extracción de característica de Retroproyección Lineal (LBP), o un algoritmo de extracción de característica de Gabor en transformada de Fourier con ventana.

La Figura 7 muestra un diagrama de bloques de otra realización de un aparato de autenticación de identidad de acuerdo con la presente solicitud. El aparato de autenticación de identidad puede aplicarse en un servidor. El aparato incluye una unidad 710 de envío, una unidad 720 receptora y una unidad 730 de determinación.

La unidad 710 de envío está configurada para enviar información rápida de autenticación dinámica del rostro a un terminal durante la autenticación de identidad de un usuario.

La unidad 720 receptora está configurada para recibir información de reconocimiento de gestos enviada por el terminal, siendo la información de reconocimiento de gestos la información de reconocimiento de gestos obtenida por el terminal a través del reconocimiento de un gesto facial que es presentado por el usuario de acuerdo con la información rápida de autenticación dinámica del rostro.

La unidad 730 de determinación está configurada para determinar que la autenticación de identidad del usuario es exitosa en respuesta a la verificación que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

En una implementación opcional, la unidad 720 receptora puede configurarse adicionalmente para recibir la primera información de rasgos faciales del usuario enviada por el terminal.

El aparato puede incluir además (no se muestra en la Figura 7) una unidad de verificación configurada para verificar si la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario que está almacenada.

La unidad 710 de envío puede configurarse específicamente para enviar la información rápida de autenticación dinámica del rostro al terminal en respuesta a una coincidencia entre ellos.

Opcionalmente, la unidad 720 receptora puede configurarse adicionalmente para recibir la segunda información de rasgos faciales del usuario enviada por el terminal cuando el usuario realiza un registro. El aparato puede incluir además (no se muestra en la Figura 7) una unidad de almacenamiento configurada para almacenar una relación de correspondencia entre un nombre de usuario del usuario y la segunda información de rasgos faciales.

Opcionalmente, la unidad de verificación puede incluir una subunidad de búsqueda de característica configurada para buscar la relación de correspondencia con base en el nombre de usuario del usuario para obtener la segunda información de rasgos faciales correspondiente al nombre de usuario; una subunidad de comparación de característica configurada para comparar la primera información de rasgos faciales y la segunda información de rasgos faciales de una manera de comparación preestablecida; y una subunidad de determinación de coincidencia configurada para determinar que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales si un valor de comparación de característica cae dentro de un rango de similitud preestablecido. La manera de comparación preestablecida utilizada por la subunidad de comparación de característica puede incluir un método de comparación de distancia euclidiana, o un método de comparación de distancia coseno.

Los detalles de los procesos de implementaciones de las funciones y los efectos de las diversas unidades en los aparatos anteriores pueden referirse a los procesos de implementaciones de las etapas correspondientes en los métodos anteriores, y no se describen repetidamente en el presente documento.

Dado que las realizaciones del aparato corresponden básicamente a las realizaciones del método, las partes relacionadas pueden referirse a partes respectivas de la descripción de las realizaciones del método. Las realizaciones del aparato descritas anteriormente son simplemente de ejemplo. Las unidades que se describen como componentes individuales pueden o no estar físicamente separadas. Un componente que se muestra como una unidad puede o no ser una unidad física, es decir, puede estar ubicado en un solo lugar o distribuido entre múltiples unidades de red. Algunos o todos los módulos pueden seleccionarse de acuerdo con un requisito real para lograr el objetivo de las soluciones de la presente solicitud. Un experto en la técnica puede comprender e implementar la presente solicitud sin hacer ningún esfuerzo creativo.

Como se puede ver en las realizaciones anteriores, se puede realizar una autenticación altamente segura en una identidad de un usuario a través de la autenticación dinámica del rostro durante la autenticación de identidad del

usuario. En comparación con los métodos de autenticación existentes que utilizan una contraseña de autenticación, un tercero malintencionado no robará fácilmente la información de autenticación, lo que mejorará la confiabilidad de la autenticación. Además, un usuario puede ser reconocido como un usuario en vivo a través de la autenticación dinámica del rostro, mejorando así la precisión de la autenticación de identidad y reduciendo los riesgos potenciales de seguridad durante la autenticación.

Un experto en la técnica puede encontrar fácilmente otras soluciones de implementación de la presente solicitud después de considerar la especificación y practicar la invención divulgada en el presente documento. La presente solicitud está destinada a cubrir cualquiera de las variaciones, usos o cambios adaptativos de la presente solicitud. Estas variaciones, usos o cambios adaptativos siguen los principios generales de la presente solicitud e incluyen conocimiento común o medidas técnicas convencionales en el presente campo técnico que no se divulgan en la presente solicitud. La especificación y las realizaciones se consideran simplemente a modo de ejemplo, y el alcance real de la presente solicitud se especifica en las reivindicaciones del presente documento.

Debe observarse que la presente solicitud no se limita a las estructuras precisas que se han descrito anteriormente y se ilustran en los dibujos adjuntos. Se pueden hacer diversas modificaciones y cambios a la presente solicitud sin apartarse del alcance de la misma. El alcance de la presente solicitud solo está limitado por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de autenticación de identidad, en donde el método comprende:

adquirir (303) información de rasgos faciales de un usuario y utilizar la información de rasgos faciales adquirida durante la autenticación de identidad como primera información de rasgos faciales del usuario; y

enviar (308) la primera información de rasgos faciales del usuario a un servidor para permitir que el servidor envíe información rápida de autenticación dinámica del rostro en respuesta a la verificación de que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario que está almacenada;

recibir (201) la información rápida de autenticación dinámica del rostro enviada por el servidor durante la autenticación de identidad del usuario;

obtener (202) información de reconocimiento del gesto de la información rápida de autenticación dinámica del rostro mediante el reconocimiento de un gesto facial presentado por el usuario; y

enviar (203) la información de reconocimiento de gestos al servidor para permitir que el servidor confirme que la autenticación de identidad es exitosa para el usuario tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

2. El método de la reivindicación 1, en donde obtener (202) la información de reconocimiento del gesto de la información rápida de autenticación dinámica del rostro mediante el reconocimiento del gesto facial presentado por el usuario, comprende:

obtener (202) información de seguimiento del rostro siguiendo un rostro del usuario cuando el usuario presenta un gesto facial de acuerdo con la información rápida de autenticación dinámica del rostro; y

analizar la información de seguimiento del rostro para obtener la información de reconocimiento de gestos del usuario.

3. El método de la reivindicación 2, en donde el análisis de la información de seguimiento del rostro para obtener la información de reconocimiento del gesto del usuario comprende:

cuando la información de seguimiento del rostro es información de posición del punto clave facial, obtener información de reconocimiento del gesto de expresión del usuario mediante el análisis de la información de posición del punto clave facial; o

cuando la información de seguimiento del rostro es información del gesto de la cabeza, obtener información de reconocimiento de giro de la cabeza del usuario mediante el análisis de la información del gesto de la cabeza.

4. El método de una cualquiera de las reivindicaciones 1-3, en donde la información rápida de autenticación dinámica del rostro comprende al menos un tipo de la siguiente información:

información rápida de acción de expresión o información rápida de lectura de voz.

5. El método de cualquier reivindicación precedente, en donde el método comprende, además:

adquirir (303) información de rasgos faciales del usuario cuando el usuario realiza el registro, y utilizar la información de rasgos faciales adquirida durante el registro como la segunda información de rasgos faciales del usuario; y

enviar (308) la segunda información de rasgos faciales al servidor para permitir que el servidor almacene (309) una relación de correspondencia entre el nombre de usuario del usuario y la segunda información de rasgos faciales.

6. Un método de autenticación de identidad, en donde el método comprende:

recibir la primera información de rasgos faciales de un usuario enviada por un terminal;

verificar si la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario almacenada;

si la primera información de rasgos faciales coincide con la segunda información de rasgos faciales, entonces

enviar información rápida de autenticación dinámica del rostro al terminal durante la autenticación de identidad del usuario;

recibir información de reconocimiento del gesto enviada por el terminal, siendo la información de reconocimiento del gesto la información de reconocimiento del gesto obtenida por el terminal a través del reconocimiento de un gesto facial que es presentada por el usuario de acuerdo con la información rápida de autenticación dinámica del rostro; y

determinar que la autenticación de identidad es exitosa para el usuario tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

7. El método de la reivindicación 6, en donde el método comprende, además:

recibir la segunda información de rasgos faciales del usuario enviada por el terminal cuando el usuario realiza el registro; y

almacenar una relación de correspondencia entre un nombre de usuario del usuario y la segunda información de rasgos faciales,

y en donde opcionalmente se verifica si la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario que está almacenada, comprende:

buscar para la relación de correspondencia con base en el nombre de usuario del usuario para obtener la segunda información de rasgos faciales correspondiente al nombre de usuario;

comparar la primera información de rasgos faciales con la segunda información de rasgos faciales de una manera de comparación preestablecida; y

determinar que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales si un valor de comparación de características cae dentro de un rango de similitud preestablecido.

8. Un aparato de autenticación de identidad, en donde el aparato comprende:

una unidad de adquisición configurada para adquirir (303) información de rasgos faciales de un usuario, y utilizar la información de rasgos faciales adquirida durante la autenticación de identidad del usuario como primera información de rasgos faciales del usuario;

una unidad (610) receptora configurada para recibir (201) información rápida de autenticación dinámica del rostro enviada por un servidor durante la autenticación de identidad de un usuario;

una unidad (620) de reconocimiento configurada para obtener (202) información de reconocimiento del gesto de la información rápida de autenticación dinámica del rostro mediante el reconocimiento de un gesto facial presentado por el usuario; y

una unidad (620) de envío, configurada para:

enviar (308) la primera información de rasgos faciales del usuario al servidor para permitir que el servidor envíe la información rápida de autenticación dinámica del rostro en respuesta a la verificación de que la primera información de rasgos faciales coincida con la segunda información de rasgos faciales del usuario almacenada; y

enviar (203) la información de reconocimiento de gestos al servidor para permitir al servidor que confirme que la autenticación de identidad del usuario es exitosa tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

9. El aparato de la reivindicación 8, en donde la unidad (620) de reconocimiento comprende:

una subunidad de obtención de información del rostro configurada para obtener información de seguimiento del rostro siguiendo un rostro del usuario cuando el usuario presenta un gesto facial de acuerdo con la información rápida de autenticación dinámica del rostro; y

una subunidad de análisis de información facial configurada para analizar la información de seguimiento facial para obtener la información de reconocimiento del gesto del usuario,

y en donde opcionalmente la subunidad de análisis de información facial está configurada específicamente para:

obtener información de reconocimiento del gesto de expresión del usuario mediante el análisis de información de posición del punto clave facial cuando la información de seguimiento del rostro es la información de posición del punto clave facial; u

obtener información de reconocimiento de giro de la cabeza del usuario mediante el análisis de la información del gesto de la cabeza cuando la información de seguimiento del rostro es la información del gesto de la cabeza.

10. El aparato de la reivindicación 8 o la reivindicación 9, en donde:

la unidad de adquisición está configurada además para adquirir información de rasgos faciales del usuario durante el registro del usuario, y utilizar la información de rasgos faciales adquirida durante el registro como la segunda información de rasgos faciales del usuario; y

la unidad (620) de envío está configurada además para enviar (308) la segunda información de rasgos faciales al servidor para permitir que el servidor almacene una relación de correspondencia entre un nombre de usuario del usuario y la segunda información de rasgos faciales.

11. Un terminal que comprende:

procesador(es) y memoria configurada para almacenar instrucciones ejecutables por el(los) procesador(es), en donde el(los) procesador(es) está(n) configurado(s) para:

adquirir (303) información de rasgos faciales de un usuario durante la autenticación de identidad y utilizar la información de rasgos faciales adquirida como primera información de rasgos faciales del usuario;

enviar (308) la primera información de rasgos faciales del usuario a un servidor para permitir que el servidor envíe información rápida de autenticación dinámica del rostro en respuesta a la verificación de que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario almacenada;

recibir (201) la información rápida de autenticación dinámica del rostro enviada por el servidor durante la autenticación de identidad del usuario;

obtener (202) información de reconocimiento del gesto de la información rápida de autenticación dinámica del rostro mediante el reconocimiento de un gesto facial presentado por el usuario; y

enviar (203) la información de reconocimiento del gesto al servidor para permitir que el servidor confirme que el usuario pasa la autenticación de identidad tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

12. Un servidor que comprende:

procesador(es) y memoria configurada para almacenar instrucciones ejecutables por el(los) procesador(es), en donde el(los) procesador(es) está(n) configurado(s) para:

recibir (308), a partir de un terminal, la primera información de rasgos faciales de un usuario adquirida por el terminal durante la autenticación de identidad del usuario;

en respuesta a la verificación que la primera información de rasgos faciales coincide con la segunda información de rasgos faciales del usuario que está almacenada, enviar información rápida de autenticación dinámica del rostro al terminal durante la autenticación de identidad del usuario;

recibir (203) información de reconocimiento del gesto enviada por el terminal, la información de reconocimiento siendo la información de reconocimiento del gesto obtenida por el terminal a través del reconocimiento de un gesto facial que es presentado por el usuario de acuerdo con la información rápida de autenticación dinámica del rostro; y

determinar que el usuario pasa la autenticación de identidad tras verificar que la información de reconocimiento del gesto es coherente con la información rápida de autenticación dinámica del rostro.

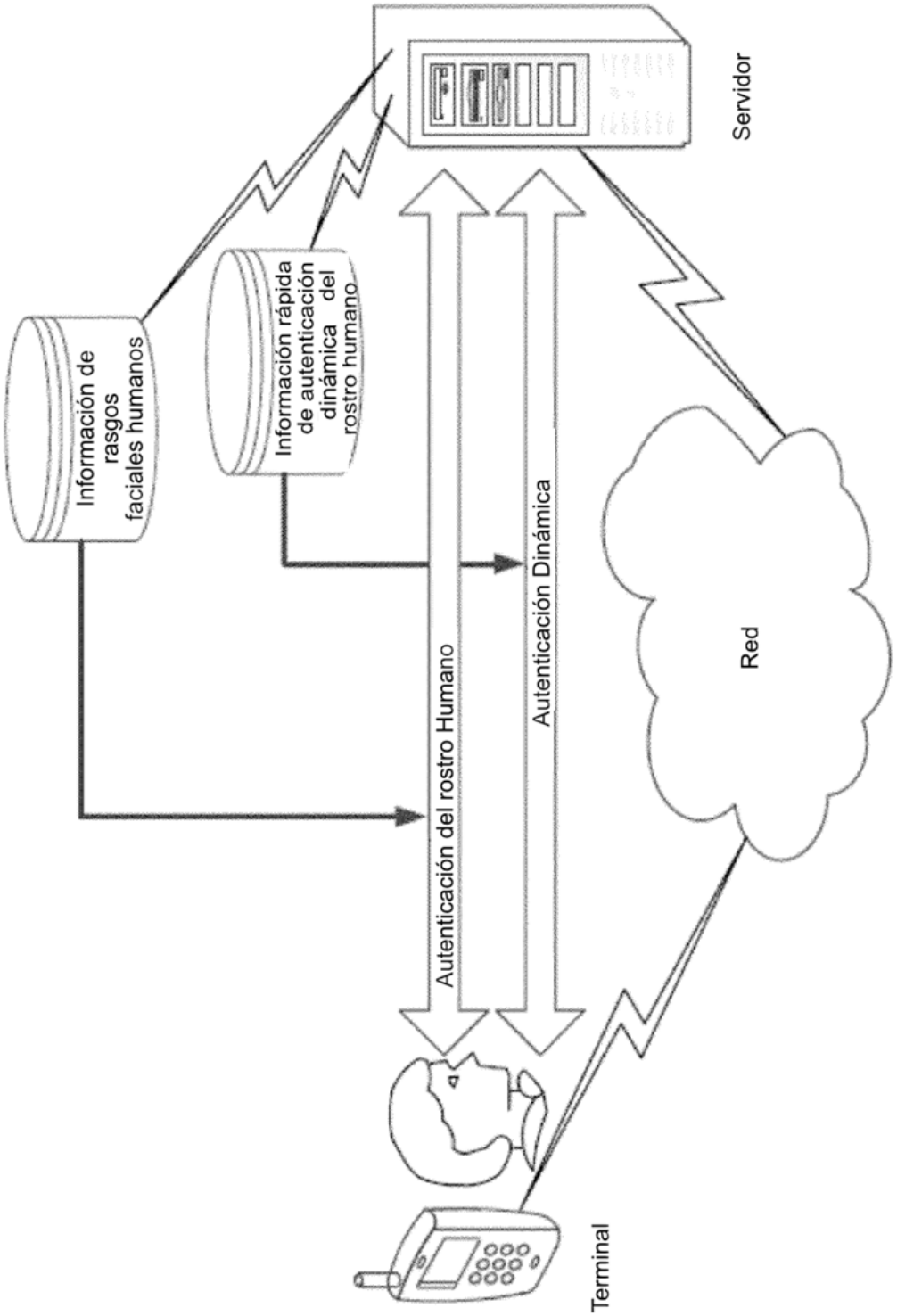
Servidor
Información de rasgos faciales humanos
Información rápida de autenticación dinámica del rostro humano
Autenticación del rostro Humano
Autenticación Dinámica
Red
Terminal

FIG. 1

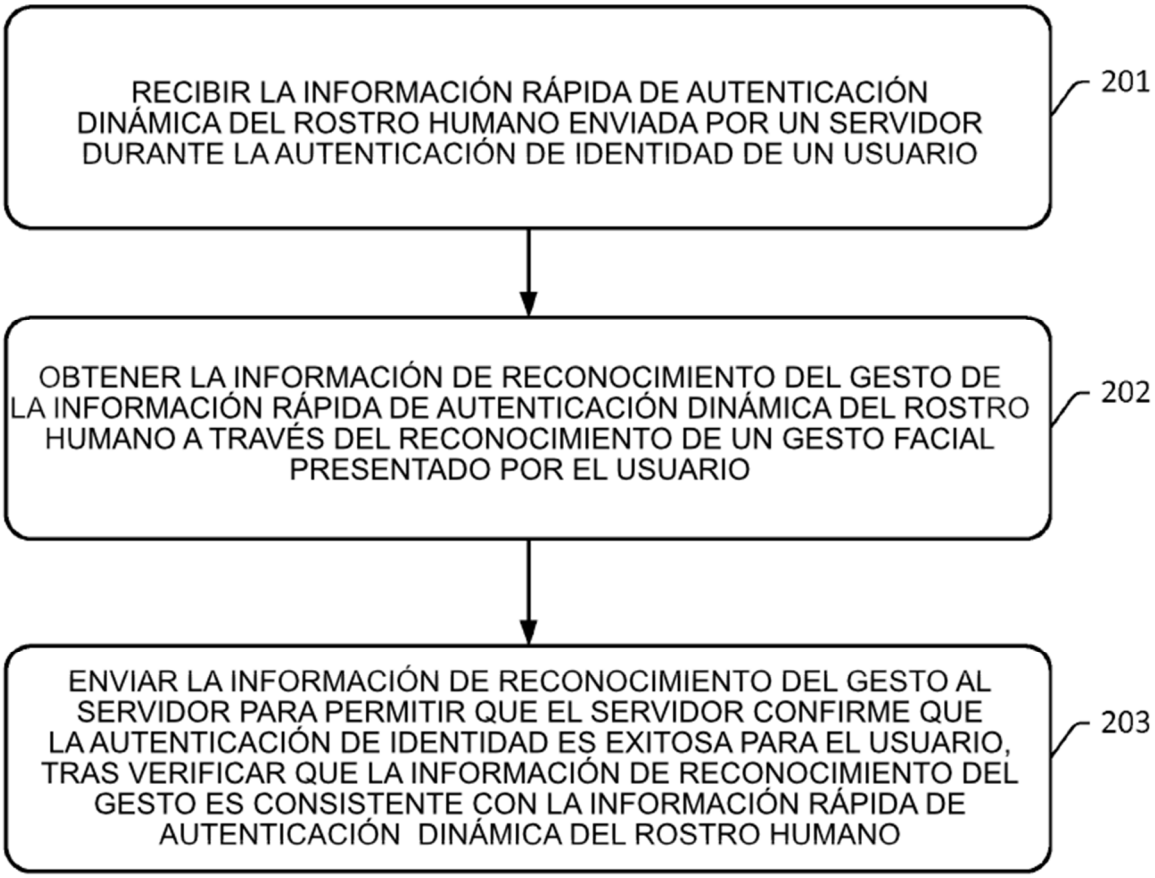
RECIBIR LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO ENVIADA POR UN SERVIDOR DURANTE LA AUTENTICACIÓN DE IDENTIDAD DE UN USUARIO
201
OBTENER LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO DE LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO A TRAVÉS DEL RECONOCIMIENTO DE UN GESTO FACIAL PRESENTADO POR EL USUARIO
202
ENVIAR LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO AL SERVIDOR PARA PERMITIR QUE EL SERVIDOR CONFIRME QUE LA AUTENTICACIÓN DE IDENTIDAD ES EXITOSA PARA EL USUARIO, TRAS VERIFICAR QUE LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO ES CONSISTENTE CON LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO
203

FIG. 2A

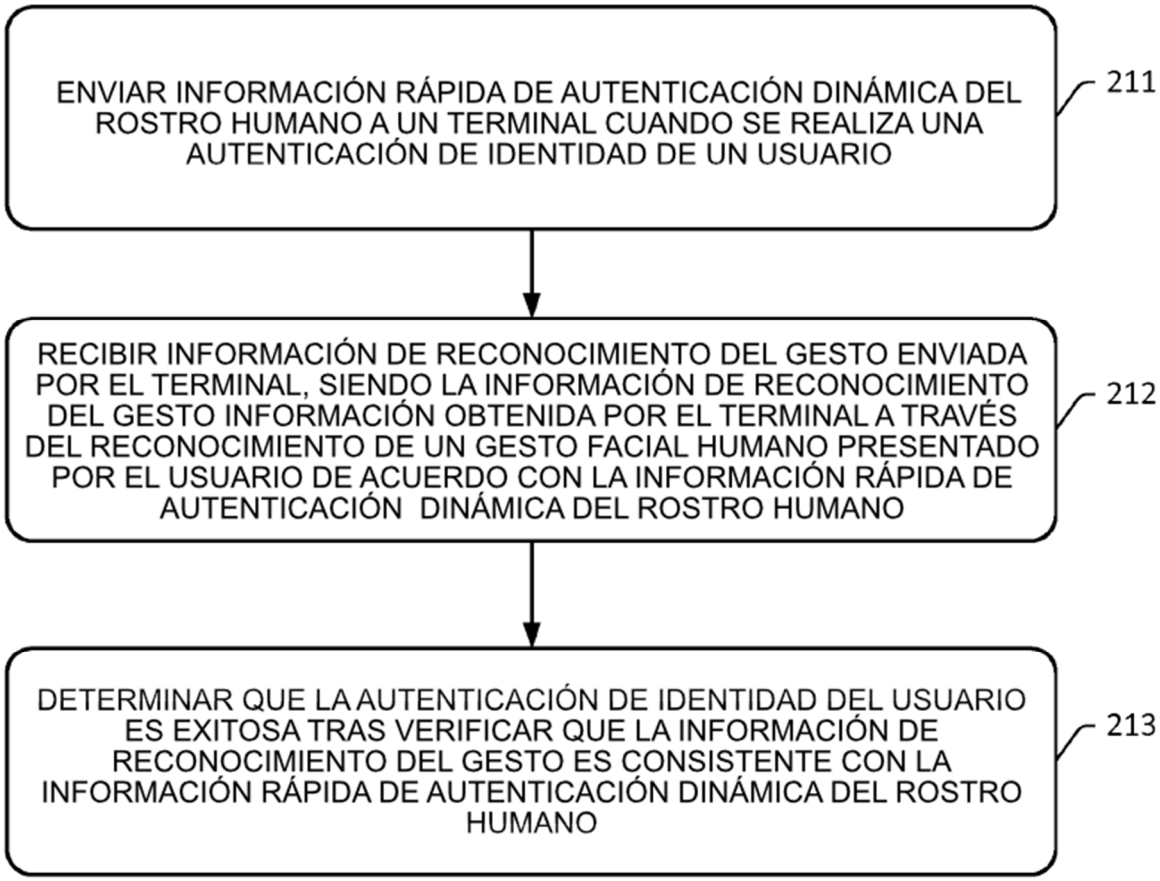
ENVIAR INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO A UN TERMINAL CUANDO SE REALIZA UNA AUTENTICACIÓN DE IDENTIDAD DE UN USUARIO
211
RECIBIR INFORMACIÓN DE RECONOCIMIENTO DEL GESTO ENVIADA POR EL TERMINAL, SIENDO LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO INFORMACIÓN OBTENIDA POR EL TERMINAL A TRAVÉS DEL RECONOCIMIENTO DE UN GESTO FACIAL HUMANO PRESENTADO POR EL USUARIO DE ACUERDO CON LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO
212
DETERMINAR QUE LA AUTENTICACIÓN DE IDENTIDAD DEL USUARIO ES EXITOSA TRAS VERIFICAR QUE LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO ES CONSISTENTE CON LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO HUMANO
213

FIG. 2B

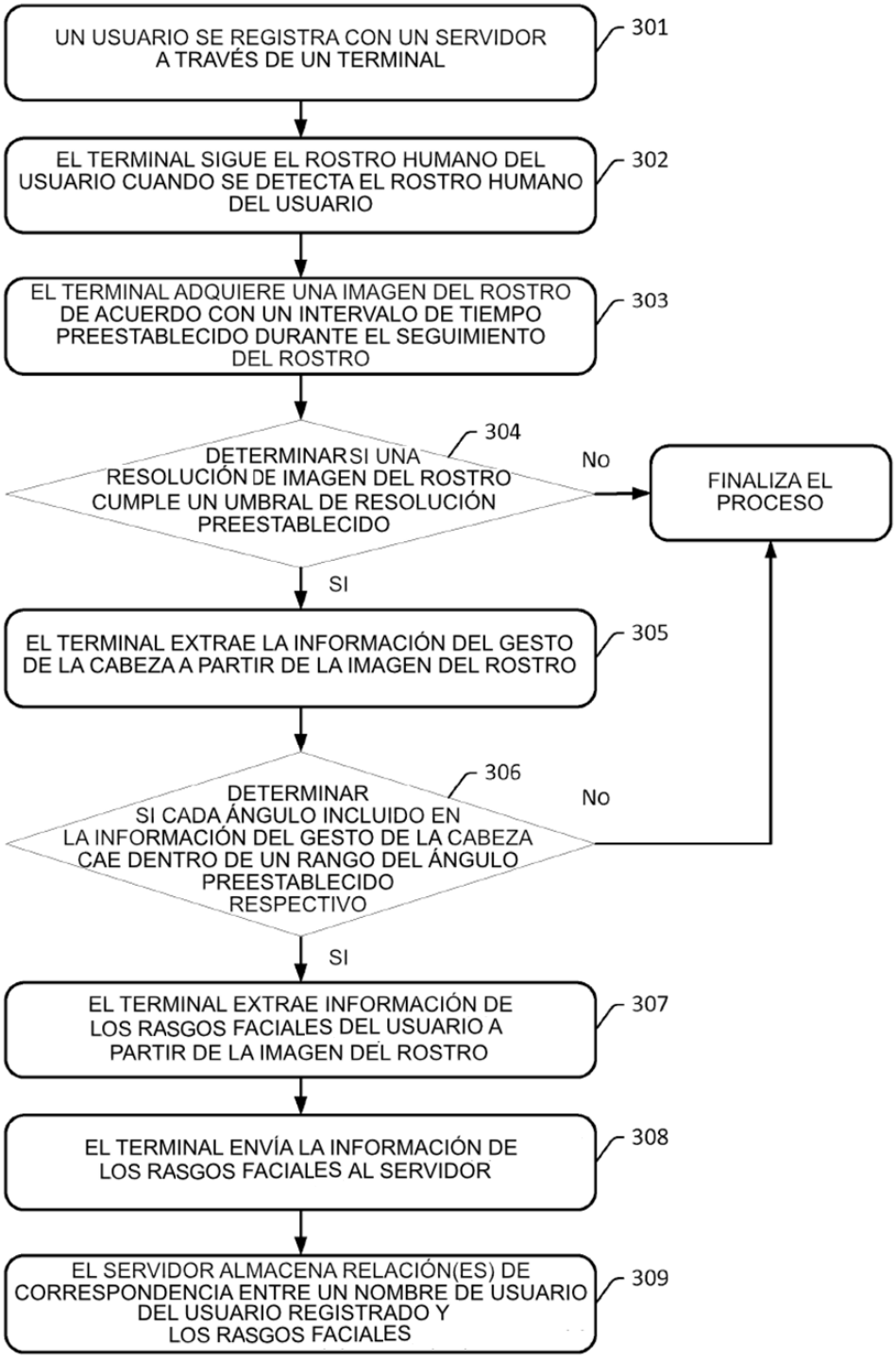
UN USUARIO SE REGISTRA CON UN SERVIDOR A TRAVÉS DE UN TERMINAL
301
EL TERMINAL SIGUE EL ROSTRO HUMANO DEL USUARIO CUANDO SE DETECTA EL ROSTRO HUMANO DEL USUARIO
302
EL TERMINAL ADQUIERE UNA IMAGEN DEL ROSTRO DE ACUERDO CON UN INTERVALO DE TIEMPO PREESTABLECIDO DURANTE EL SEGUIMIENTO DEL ROSTRO
303
DETERMINAR SI UNA RESOLUCIÓN DE IMAGEN DEL ROSTRO CUMPLE UN UMBRAL DE RESOLUCIÓN PREESTABLECIDO
304
No
FINALIZA EL PROCESO
SI
EL TERMINAL EXTRAE LA INFORMACIÓN DEL GESTO DE LA CABEZA A PARTIR DE LA IMAGEN DEL ROSTRO
305
DETERMINAR SI CADA ÁNGULO INCLUIDO EN LA INFORMACIÓN DEL GESTO DE LA CABEZA CAE DENTRO DE UN RANGO DEL ÁNGULO PREESTABLECIDO RESPECTIVO
306
No
SI
EL TERMINAL EXTRAE INFORMACIÓN DE LOS RASGOS FACIALES DEL USUARIO A PARTIR DE LA IMAGEN DEL ROSTRO
307
EL TERMINAL ENVÍA LA INFORMACIÓN DE LOS RASGOS FACIALES AL SERVIDOR
308
EL SERVIDOR ALMACENA RELACIÓN(ES) DE CORRESPONDENCIA ENTRE UN NOMBRE DE USUARIO DEL USUARIO REGISTRADO Y LOS RASGOS FACIALES
309

FIG. 3A

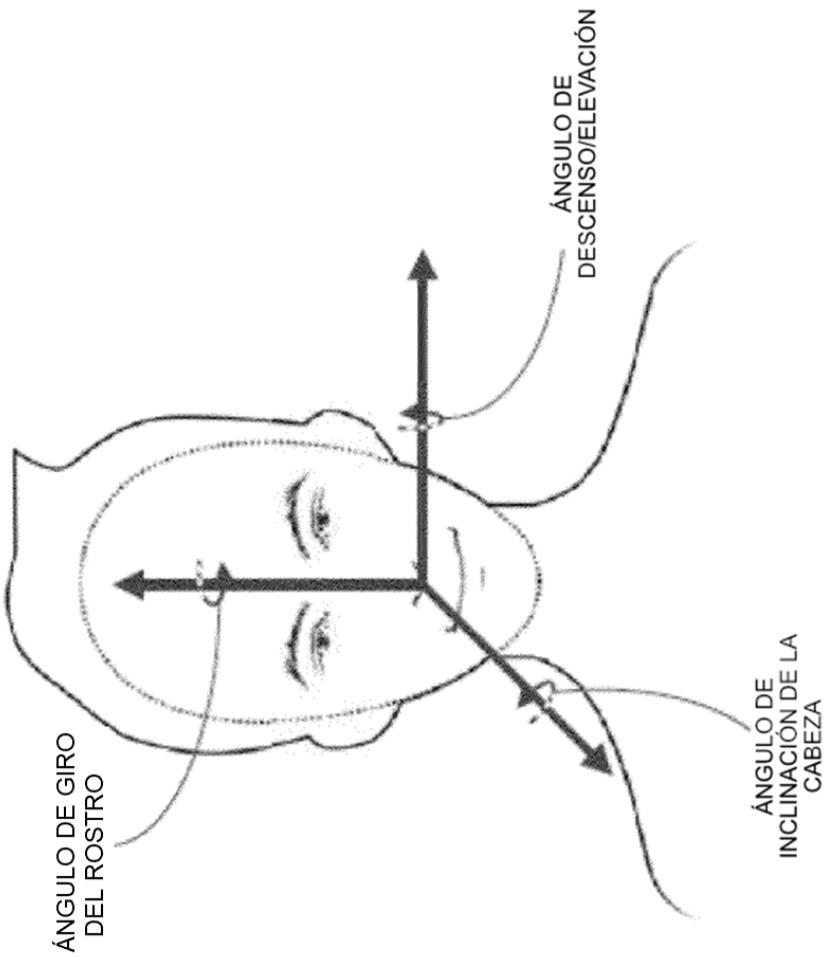
ÁNGULO DE DESCENSO/ELEVACIÓN
ÁNGULO DE GIRO DEL ROSTRO
ÁNGULO DE INCLINACIÓN DE LA CABEZA

FIG. 3B

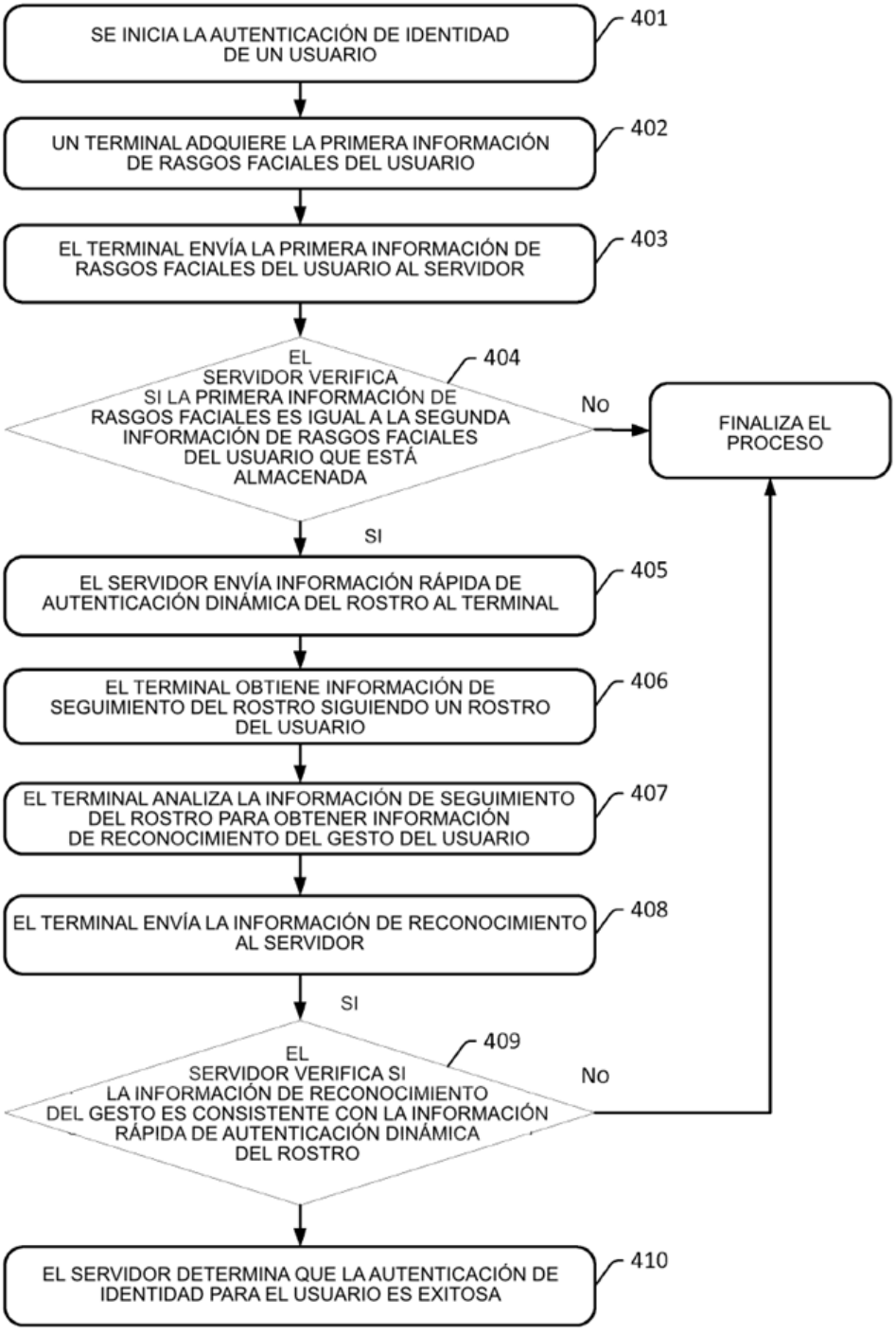
SE INICIA LA AUTENTICACIÓN DE IDENTIDAD DE UN USUARIO
401
UN TERMINAL ADQUIERE LA PRIMERA INFORMACIÓN DE RASGOS FACIALES DEL USUARIO
402
EL TERMINAL ENVÍA LA PRIMERA INFORMACIÓN DE RASGOS FACIALES DEL USUARIO AL SERVIDOR
403
EL SERVIDOR VERIFICA SI LA PRIMERA INFORMACIÓN DE RASGOS FACIALES ES IGUAL A LA SEGUNDA INFORMACIÓN DE RASGOS FACIALES DEL USUARIO QUE ESTÁ ALMACENADA
404
No
FINALIZA EL PROCESO
SI
EL SERVIDOR ENVÍA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO AL TERMINAL
405
EL TERMINAL OBTIENE INFORMACIÓN DE SEGUIMIENTO DEL ROSTRO SIGUIENDO UN ROSTRO DEL USUARIO
406
EL TERMINAL ANALIZA LA INFORMACIÓN DE SEGUIMIENTO DEL ROSTRO PARA OBTENER INFORMACIÓN DE RECONOCIMIENTO DEL GESTO DEL USUARIO
407
EL TERMINAL ENVÍA LA INFORMACIÓN DE RECONOCIMIENTO AL SERVIDOR
408
SI
EL SERVIDOR VERIFICA SI LA INFORMACIÓN DE RECONOCIMIENTO DEL GESTO ES CONSISTENTE CON LA INFORMACIÓN RÁPIDA DE AUTENTICACIÓN DINÁMICA DEL ROSTRO
409
No
EL SERVIDOR DETERMINA QUE LA AUTENTICACIÓN DE IDENTIDAD PARA EL USUARIO ES EXITOSA
410

FIG. 4A

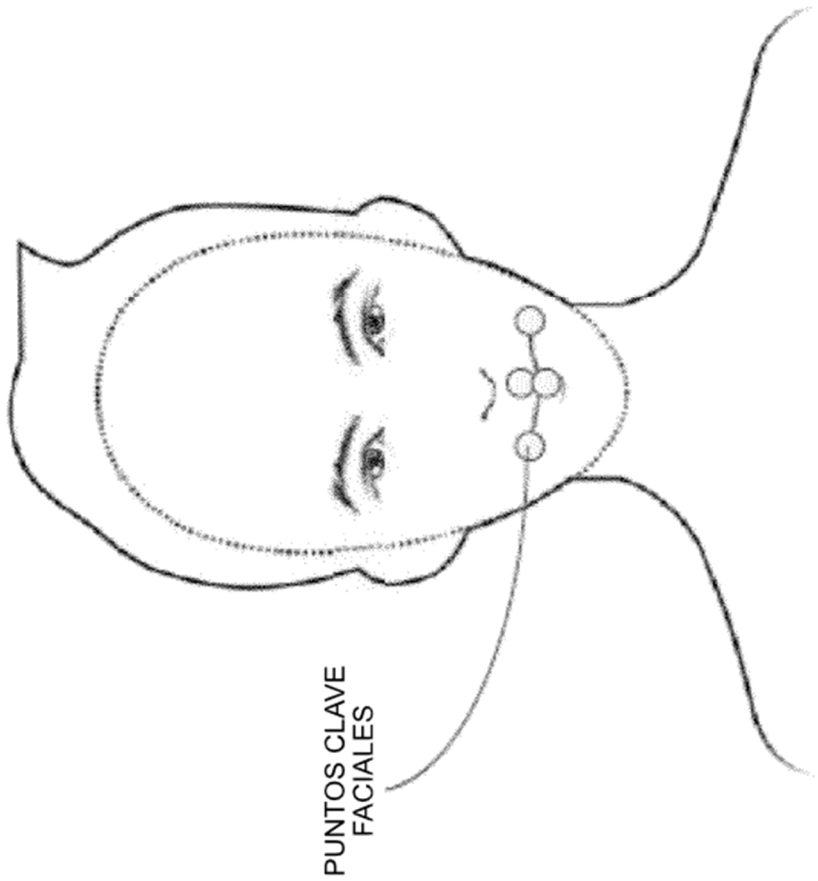

FIG. 4B

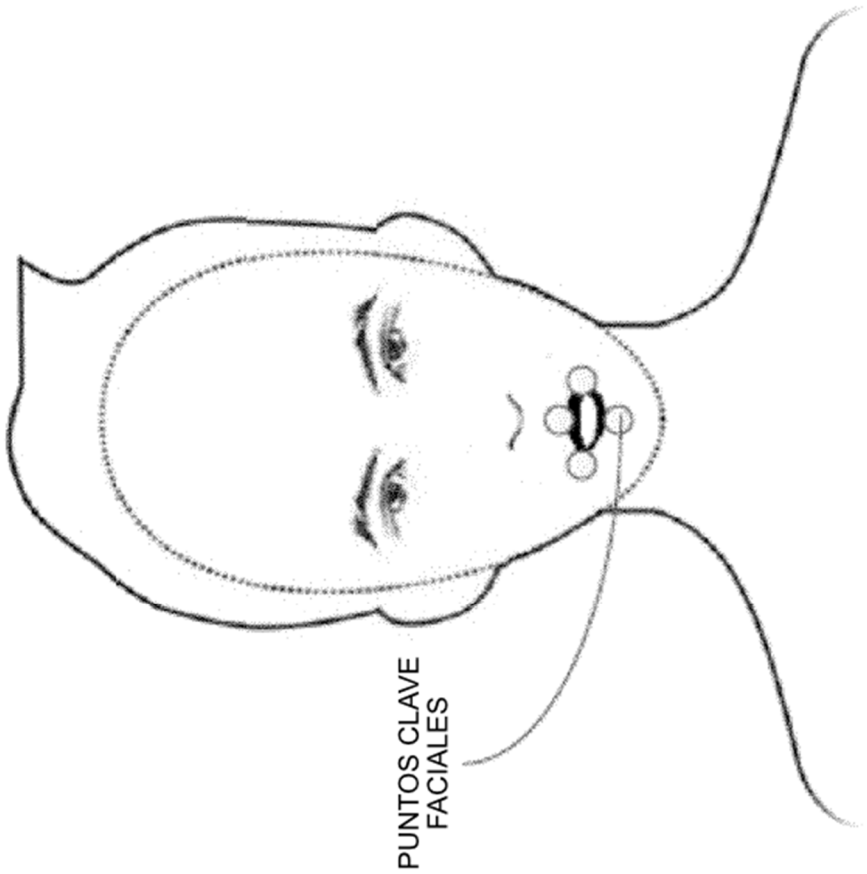

FIG. 4C

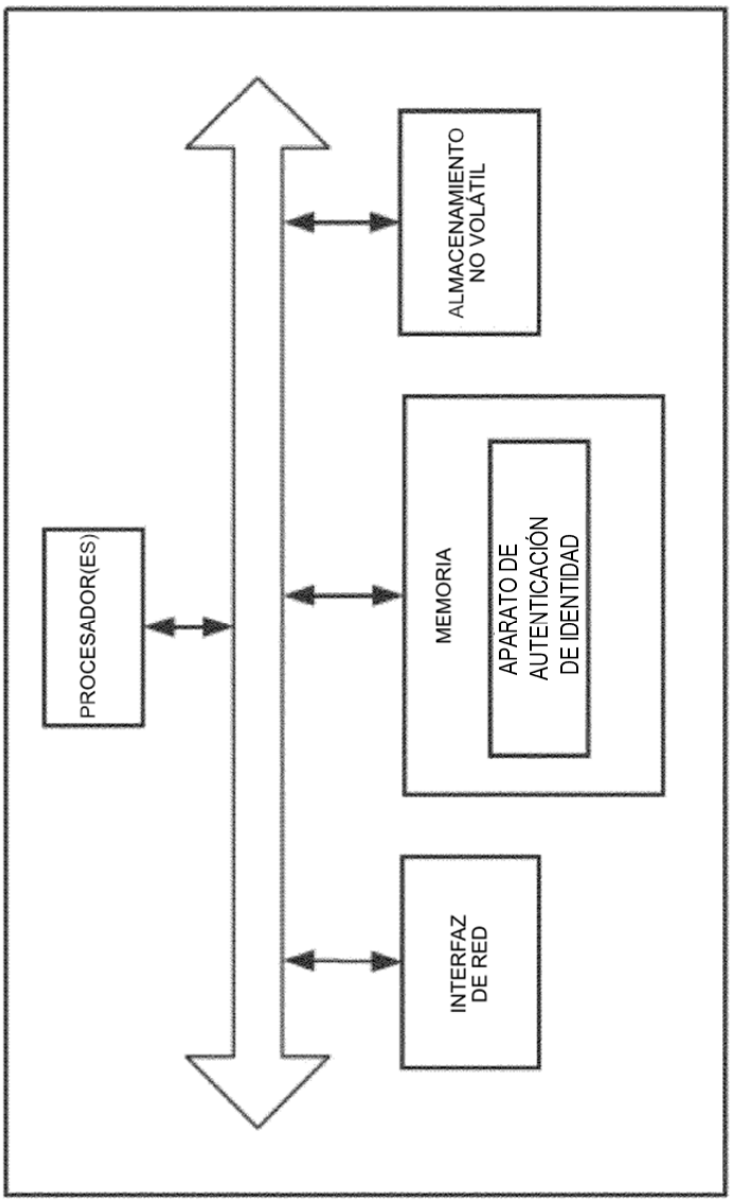
PROCESADOR(ES)
ALMACENAMIENTO NO VOLÁTIL
MEMORIA
APARATO DE AUTENTICACIÓN DE IDENTIDAD
INTERFAZ DE RED

FIG. 5

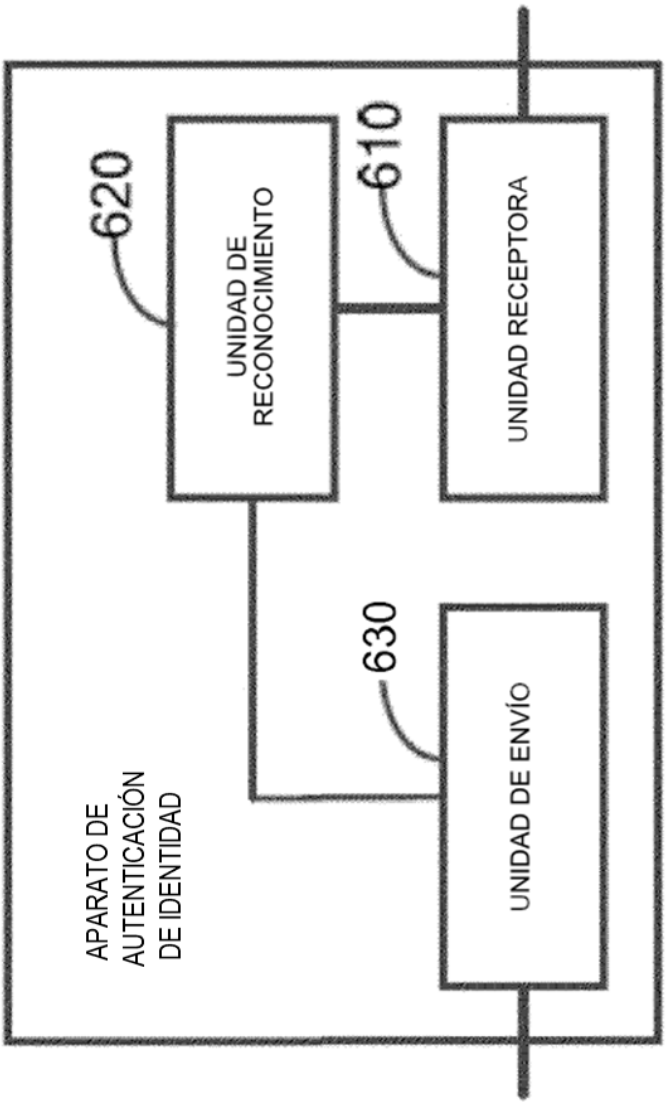
APARATO DE AUTENTICACIÓN DE IDENTIDAD
620
UNIDAD DE RECONOCIMIENTO
610
UNIDAD RECEPTORA
630
UNIDAD DE ENVÍO

FIG. 6

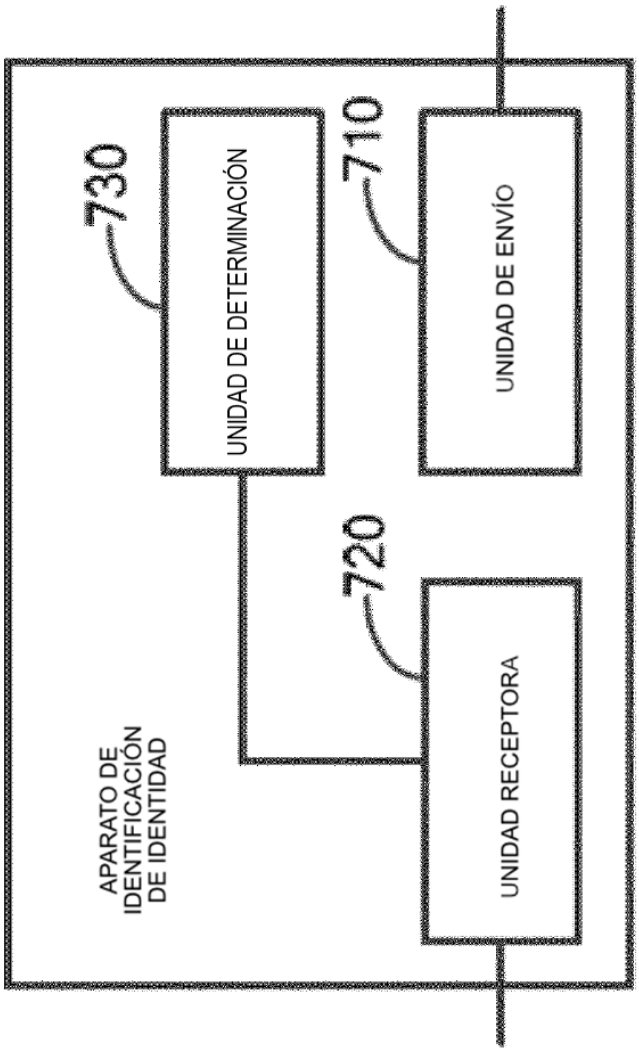
APARATO DE IDENTIFICACIÓN DE IDENTIDAD
730
UNIDAD DE DETERMINACIÓN
710
UNIDAD DE ENVÍO
720
UNIDAD RECEPTORA

FIG. 7