(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 795 669**

(51) Int. CI.:

H04W 12/06 (2009.01)
G06F 21/32 (2013.01)
G06F 3/0488 (2013.01)
H04W 88/02 (2009.01)
H04L 29/06 (2006.01)
H04M 1/673 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.06.2015 PCT/KR2015/006590**

(87) Fecha y número de publicación internacional: **30.12.2015 WO15199501**

(96) Fecha de presentación y número de la solicitud europea: **26.06.2015 E 15811063 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3163926**

(54) Título: **Método y sistema de autenticación de usuario usando teclado numérico variable e identificación biométrica**

(30) Prioridad:

26.06.2014 KR 20140079247

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.11.2020

(73) Titular/es:

HAREXINFOTECH INC. (100.0%)
202 Toegye-ro Jung-gu
Seoul 100-272, KR

(72) Inventor/es:

PARK, KYUNG YANG

(74) Agente/Representante:

ISERN JARA, Jorge

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y sistema de autenticación de usuario usando teclado numérico variable e identificación biométrica

Campo técnico

La presente invención se refiere a un método y sistema para una autenticación de usuario y, más particularmente, a un método y sistema de autenticación de usuario que recibe información biométrica e información de posición de contraseña correspondiente a un orden de entrada de contraseña a través de un teclado numérico variable, transmite la información biométrica y la información de posición de contraseña a un servidor y realiza una autenticación de usuario en el servidor.

Antecedentes de la técnica

En una sociedad moderna, es necesario introducir una contraseña para un acuerdo electrónico basado en un teléfono inteligente. A diferencia de los teléfonos celulares, los teléfonos inteligentes son, como los ordenadores personales (PC) de propósito general, vulnerables a la piratería, debido a que las aplicaciones para teléfonos inteligentes pueden ser desarrolladas por cualquier persona.

En particular, cuando se introduce una contraseña a través de un teclado numérico fijo, se pueden revelar coordenadas de toque de contraseña de un usuario. En este caso, se puede filtrar la contraseña en sí, por lo que el usuario necesita prestar especial atención.

Con el fin de resolver un problema de este tipo, se desarrolló un método de autenticación usando un teclado numérico variable. En el método de teclado numérico variable, las posiciones de los botones de entrada de un teclado numérico se cambian cada vez que un usuario realiza una conexión. En consecuencia, la posibilidad de que se filtre una contraseña es pequeña, incluso si las posiciones de los botones de entrada del teclado numérico de un teléfono inteligente son robadas por un tercero.

Un usuario no puede realizar una autenticación cuando el usuario no conoce la contraseña en sí.

Sin embargo, en un método de autenticación basado en teclado numérico variable, la contraseña en sí se transmite desde un terminal a un servidor cuando se solicita una autenticación. En consecuencia, cuando un pirata informático piratea una contraseña mientras se está transmitiendo la contraseña en sí, el pirata informático puede averiguar la contraseña en sí, y esto causa una filtración de información personal y una vulnerabilidad en la seguridad.

Asimismo, cuando un tercero que conoce la contraseña de un usuario en sí finge ser el usuario y realiza una autenticación de usuario, no se puede evitar que la autenticación tenga éxito.

El documento de la técnica anterior US 2012/140993 A1 divulga una autenticación biométrica segura desde un dispositivo no seguro, al solicitar a un individuo que realice un desafío de acción.

El documento de la técnica anterior WO 2010/005960 A1 divulga un método para la transmisión de información que usa una disposición virtual para cifrar información de seguridad.

Descripción detallada de la invención

Problema técnico

Se pretende que la presente invención resuelva los problemas anteriores y está dirigida a proporcionar un método y sistema de autenticación de usuario que evite la filtración de contraseñas y mejore la seguridad al transmitir información de posición de contraseña desde un terminal móvil a un servidor de autenticación de usuario.

Además, la presente invención está dirigida a proporcionar un método y sistema de autenticación de usuario que aumente adicionalmente la seguridad al añadir información biométrica a un autenticador.

Solución técnica

La invención proporciona un servidor de autenticación de usuario de acuerdo con la reivindicación 1, un terminal móvil de acuerdo con la reivindicación 6 y un método para realizar una autenticación de usuario de acuerdo con la reivindicación 8. Se exponen realizaciones preferidas en las reivindicaciones dependientes.

Efectos ventajosos de la invención

De acuerdo con la presente invención, una contraseña en sí que se introduce a través de un teclado numérico variable no se transmite a un servidor de autenticación de usuario, sino que se transmite información de posición de

la contraseña correspondiente al orden en el que la contraseña es introducida por un usuario. En consecuencia, es posible mejorar la seguridad debido a que un pirata informático no se puede enterar de la contraseña incluso aunque el pirata informático intercepte información de posición de la información secreta que se está transmitiendo desde un terminal a un servidor.

Asimismo, en comparación con una técnica relacionada en la que meramente se introducen cuatro dígitos de una contraseña y, entonces, se cambia su posición, es posible mejorar adicionalmente la seguridad debido a que se realiza una autenticación de usuario a través de una contraseña e información biométrica.

Posteriormente, cuando la información biométrica es información de iris, es posible evitar el robo o la falsificación debido a que un iris tiene características individuales para cada persona y mejorar adicionalmente la seguridad en relación con una contraseña, debido a que el iris es más complejo y delicado que una huella dactilar.

Descripción de los dibujos

La figura 1 es un diagrama de bloques que muestra un sistema de autenticación de usuario que usa tanto una contraseña como información biométrica de acuerdo con una realización de la presente invención.
La figura 2 es un diagrama de secuencia que muestra un método de autenticación de usuario que usa tanto una contraseña como información biométrica de acuerdo con una realización de la presente invención.
La figura 3A es un diagrama que muestra un teclado numérico variable que se genera en primer lugar como un ejemplo de un teclado numérico variable que incluye teclas de cifrado y una tecla de autenticación biométrica que se genera de tal modo que las posiciones de las teclas de cifrado y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable de acuerdo con una realización de la presente invención.
La figura 3B es un diagrama que muestra un teclado numérico variable que se genera en segundo lugar como un ejemplo de un teclado numérico variable que incluye teclas de cifrado y una tecla de autenticación biométrica que se genera de tal modo que las posiciones de las teclas de cifrado y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable de acuerdo con una realización de la presente invención.
La figura 4A es un diagrama que muestra un teclado numérico variable en un plano x - y de acuerdo con una realización de la presente invención.
La figura 4A es un diagrama que muestra información de posición de un teclado numérico variable en un plano x - y de acuerdo con una realización de la presente invención.
La figura 5 es un diagrama que muestra un ejemplo de transmisión de información de posición de contraseña e información biométrica desde un terminal móvil a un servidor de autenticación de usuario de acuerdo con una realización de la presente invención.
La figura 6 es un diagrama de flujo que muestra un ejemplo de extraer una contraseña a partir de posiciones de teclas de cifrado y realizar una autenticación de usuario de acuerdo con una realización de la presente invención.
La figura 7 es un diagrama que muestra un ejemplo de obtención de imágenes de un iris de un usuario y transmisión de la imagen de iris a un servidor de autenticación de usuario de acuerdo con una realización de la presente invención.
La figura 8 es un diagrama que muestra un identificador correspondiente a un teclado numérico variable que está almacenado en un servidor de autenticación y un terminal de acuerdo con una realización de la presente invención.
La figura 9 es un diagrama de secuencia que muestra un ejemplo de cifrado y descifrado de una clave de simetría temporal, una clave pública de un usuario y una clave privada de un usuario de acuerdo con una realización de la presente invención.

Mejor modo

Estos y otros objetos, ventajas y características de la presente invención, y métodos de implementación de la misma, se aclararán a través de las siguientes realizaciones descritas con referencia a los dibujos adjuntos.

La presente invención se puede materializar, sin embargo, en diferentes formas y no se debería interpretar como limitada a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones se proporcionan de tal modo que esta divulgación transmita completamente los objetos, configuraciones y efectos de la presente invención a los expertos en la materia. El alcance de la presente invención es definido por las reivindicaciones adjuntas.

La terminología usada en el presente documento es solo para el fin de describir realizaciones y no se pretende que limite la presente invención. Como se usan en el presente documento, se pretende que las formas singulares "un", "una" y "el / la" incluyan asimismo las formas plurales, a menos que el contexto indique claramente lo contrario. Las expresiones "comprende" y / o "comprendiendo / que comprende", cuando se usan en esta memoria descriptiva, especifican la presencia de elementos, etapas, operaciones y/o componentes indicados, pero no excluyen la presencia o adición de otros uno o más elementos, etapas, operaciones y/o componentes.

En lo sucesivo, se describirán con detalle realizaciones de la presente invención con referencia a los dibujos adjuntos.

La figura 1 es un diagrama de bloques que muestra un sistema de autenticación de usuario que usa tanto una contraseña como información biométrica de acuerdo con una realización de la presente invención.

Como se muestra en la figura 1, un servidor de autenticación de usuario 200 que usa una contraseña e información biométrica incluye una unidad de generación de teclado numérico variable 210, una unidad de autenticación 220 y una unidad de almacenamiento de información de autenticación 230.

La unidad de generación de teclado numérico variable 210 genera un teclado numérico variable que incluye teclas de cifrado y una tecla de autenticación biométrica. En este caso, las posiciones de las teclas de cifrado y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable.

La unidad de autenticación 220 proporciona información con respecto al teclado numérico variable generado (es decir, información de disposición de botones de tecla) a un terminal móvil 100 que está ubicado en una posición remota.

Como otro ejemplo, se puede aplicar un método para generar una pluralidad de teclados numéricos variables de antemano, asignar un identificador a cada uno de los teclados numéricos variables, compartir el identificador con un terminal móvil y transmitir solo el identificador del teclado numérico variable como información de teclado numérico variable cada vez que tiene lugar una autenticación.

La unidad de autenticación 220 recibe información biométrica e información de posición de teclas de cifrado correspondiente al orden en el que las teclas de cifrado son introducidas por un usuario desde un terminal móvil 100 y realiza una autenticación de usuario basándose en la información biométrica y la información de posición recibidas.

Por ejemplo, la unidad de autenticación 220 recibe información biométrica e información de posición de teclas de cifrado correspondiente al orden en el que las teclas de cifrado son introducidas por un usuario (haciendo referencia a las figuras 4A, 4, 3, 1 y 2 en el teclado numérico correspondiente a (0,5, 2,5), (3,5, 3,5), (1,5, 3,5) y (2,5, 3,5)) desde un terminal móvil (por ejemplo, un teléfono inteligente) y realiza una autenticación de usuario basándose en la información biométrica y la información de posición recibidas.

La unidad de autenticación 220 almacena información de posición y orden de entrada de teclas de cifrado correspondiente a una contraseña cada vez que se genera un teclado numérico variable. Cuando la unidad de autenticación 220 recibe información biométrica e información de posición de teclas de cifrado correspondiente al orden en el que las teclas de cifrado son introducidas por un usuario desde el terminal móvil 100, la unidad de autenticación 220 realiza una autenticación de usuario al comparar la información biométrica, la información de posición y el orden de entrada recibidos con información de posición de teclas de cifrado, orden de entrada de teclas de cifrado e información biométrica de usuarios que están almacenados previamente.

Por ejemplo, haciendo referencia a la figura 4A, cuando una contraseña es 4312, la información de posición de la contraseña (es decir, las teclas de cifrado) corresponde a (0,5, 2,5), (3,5, 3,5), (1,5, 3,5) y (2,5, 3,5), y el orden de entrada de la contraseña es el mismo que el descrito anteriormente.

En este caso, como una realización adicional, la unidad de autenticación 220 puede recibir información biométrica (por ejemplo, información de huella dactilar) reconocida en un área (1,5, 2,5) de una tecla de autenticación biométrica además de su información de posición y puede realizar una autenticación de usuario en función de la información.

La unidad de autenticación 220 almacena la información descrita anteriormente para la autenticación en la unidad de almacenamiento de información de autenticación cada vez que se genera un teclado numérico variable y proporciona la información de autenticación al terminal móvil 100.

La información de posición de la contraseña correspondiente al orden en el que las teclas de cifrado son introducidas por el usuario, que es recibida por la unidad de autenticación 220 desde el terminal móvil 100, corresponde a (0,5, 2,5), (3,5, 3,5), (1,5, 3,5) y (2,5, 3,5). Asimismo, cuando se reciben información de posición de una contraseña, su orden de entrada e información de huella dactilar desde el terminal móvil 100, la unidad de autenticación 220 puede realizar una autenticación al comparar la información de posición, el orden de entrada y la información de huella dactilar recibidas con información de autenticación que incluye la información de posición (0,5, 2,5), (3,5, 3,5), (1,5, 3,5) y (2,5, 3,5), el orden de entrada y la información de huella dactilar del usuario que están almacenados en la unidad de almacenamiento de información de autenticación 230.

De acuerdo con una realización de la presente invención, una huella dactilar, un iris, voz, vasos sanguíneos (vena) o similares se pueden usar como información biométrica.

Cuando la información biométrica es una huella dactilar, la unidad de autenticación 220 compara puntos de puntos de característica de una huella dactilar recibida desde el terminal móvil 100 con posiciones de puntos de característica de una huella dactilar almacenada en la unidad de almacenamiento de información de autenticación 230, compila estadísticas a partir de la comparación, calcula una puntuación usando las estadísticas, y determina que las huellas dactilares son las mismas cuando la puntuación calculada es mayor que o igual a un valor umbral predeterminado (por ejemplo, un 80 %).

La tecnología de reconocimiento de huellas dactilares es una tecnología para emitir luz a una huella dactilar y reconocer y leer crestas de la huella dactilar usando la luz reflejada. Esta tecnología se utiliza ampliamente debido a que se realiza una exploración rápida cuando un usuario pone su dedo sobre una superficie de un escáner.

La tecnología de reconocimiento de huellas dactilares es una tecnología para identificar individuos al hallar un patrón de huellas dactilares único para cada persona, explorando bifurcaciones, longitudes de cresta y extremos de cresta para obtener características para cada huella dactilar en forma de coordenadas, y comparar las coordenadas con los datos almacenados previamente.

Un aparato de entrada para un reconocimiento de huellas dactilares se clasifica en uno de tipo óptico en el que se usa un prisma, holograma o similar y uno de tipo no óptico en el que se detectan calor o presión de un dedo o campo eléctrico u ondas ultrasónicas.

En comparación con otras tecnologías de reconocimiento biométrico, la tecnología de reconocimiento de huellas dactilares tiene ventajas en que un sensor y un semiconductor que se usan para almacenar e identificar huellas dactilares son económicos, el desarrollo de la tecnología es relativamente rápido y la tecnología es aplicable a diversas aplicaciones.

El reconocimiento de huellas dactilares tiene las ventajas de tener una tasa de reconocimiento relativamente alta (es decir, una tasa de error de un 0,5 % o menos) y una velocidad de verificación rápida de 1 segundo o menos. Asimismo, el reconocimiento de huellas dactilares tiene ventajas en términos de capacidad de adopción, conveniencia y fiabilidad.

Asimismo, cuando se usa un reconocimiento de huellas dactilares, los usuarios se sienten menos abrumados en comparación con cualquier otra tecnología de reconocimiento biométrico. Asimismo, un aparato para un reconocimiento de huellas dactilares ocupa un espacio muy pequeño.

Cuando la información biométrica es voz, la unidad de autenticación 220 extrae una característica a partir de la voz recibida desde el terminal móvil 100 para generar un patrón de referencia, compara el patrón de referencia generado con un patrón de referencia almacenado en la unidad de almacenamiento de información de autenticación 230 para medir la similitud entre los mismos, y determina que la voz recibida es la misma que la almacenada en la unidad de almacenamiento de información de autenticación 230 cuando la similitud medida es mayor que o igual a un valor umbral predeterminado (por ejemplo, un 80 %).

La tecnología de reconocimiento de voz reconoce información a través de un patrón de voz único de cada persona. La tecnología de reconocimiento de voz aparta el ruido, halla un rango vocal único de cada persona e identifica individuos en función del rango vocal único.

En consecuencia, con el fin de utilizar inicialmente la tecnología de reconocimiento de voz, necesariamente se ha de grabar la voz mientras casi no hay ruido ambiental.

Cuando la información biométrica se adquiere usando una tecnología de reconocimiento de venas, la unidad de autenticación 220 explora vasos sanguíneos en el dorso de una mano para obtener una posición de un vaso sanguíneo menos deformado como coordenadas específicas y realiza un reconocimiento. La tecnología de reconocimiento de venas es una tecnología que se desarrolló en Corea del Sur. La tecnología de reconocimiento de venas usa un principio en el que, cuando se emite luz infrarroja hacia un dedo, la luz infrarroja no puede pasar a través de los glóbulos rojos y, por lo tanto, solo de los vasos sanguíneos se obtienen imágenes como regiones oscuras mediante una cámara.

La tecnología de reconocimiento de venas tiene una gran ventaja en que la luz infrarroja utilizada en esta tecnología es inofensiva para los seres humanos. Es decir, la tecnología de reconocimiento de venas es una tecnología para hallar el número y los ángulos de las ramas venosas, que se entrelazan como carreteras, y leer rápidamente las ramas venosas.

Otra información biométrica incluye una cara, una huella de una palma, geometría de una mano, una imagen térmica, una firma, una vena, dinámica de pulsación de teclas de mecanografiado y retina.

La unidad de almacenamiento de información de autenticación 230 almacena contraseñas e información biométrica de usuarios de terminal móvil.

Asimismo, la unidad de almacenamiento de información de autenticación 230 almacena información de autenticación que incluye teclas de cifrado (contraseñas) de teclados numéricos variables generados por la unidad de generación de teclado numérico variable 210, información de posición de las teclas de cifrado e información biométrica.

El terminal móvil 100 incluye un teclado numérico variable 110, una unidad de visualización 120, una unidad de control 130 y una unidad de cámara 140.

En el presente caso, el terminal móvil 100 incluye un teléfono inteligente, un teléfono celular, un PC de tipo tableta, un ordenador ultraportátil, un terminal móvil de pago con tarjeta de crédito, un cajero automático (ATM) de un banco, un quiosco instalado en una farmacia, una oficina gubernamental, etc., o similares.

El teclado numérico variable 110 se genera de tal modo que las posiciones de las teclas de cifrado y una entrada de tecla de autenticación biométrica procedente de un usuario se cambian cada vez que se genera el teclado numérico variable 110. Es decir, la unidad de generación de teclado numérico variable 210 del servidor de autenticación de usuario 200 genera originalmente un teclado numérico variable, y el teclado numérico variable 110 del terminal móvil 100 sirve para mostrar el teclado numérico variable generado a un usuario en función de la información sobre el teclado numérico generado por el servidor de autenticación de usuario 200.

La unidad de visualización 120 visualiza información sobre el teclado numérico variable 110 que se genera de tal modo que las posiciones de teclas de cifrado y una tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable 110.

La unidad de control 130 recibe la información sobre el teclado numérico variable desde el servidor de autenticación de usuario 200 y transmite información de posición de teclas de cifrado, el orden en el que se introducen las teclas de cifrado e información biométrica, todo lo cual se adquiere, al servidor de autenticación de usuario 200.

La unidad de cámara 140 captura una imagen de la parte delantera de un usuario. En el presente caso, la unidad de cámara 140 se equipa con un sistema de reconocimiento de iris y puede incluir una función de transformar un patrón de iris complejo en una serie de códigos digitales mediante el uso de una técnica matemática denominada "transformación de ondícula".

La figura 2 es un diagrama de secuencia que muestra un método de autenticación de usuario que usa tanto una contraseña como información biométrica de acuerdo con una realización de la presente invención.

Como se muestra en la figura 2, en primer lugar, el método incluye generar un teclado numérico variable que incluye teclas de cifrado y una tecla de autenticación biométrica (S110). En este caso, las posiciones de las teclas de cifrado y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable.

A continuación, el método incluye transmitir el teclado numérico variable generado a un terminal móvil (S120).

Posteriormente, el método incluye recibir información biométrica e información de posición de las teclas de cifrado correspondiente al orden en el que las teclas de cifrado son introducidas por un usuario desde el terminal móvil 100 (S130).

Por último, el método incluye realizar una autenticación de usuario en función de la información biométrica y la información de posición correspondiente al orden de entrada recibidas (S140).

De acuerdo con una realización de la presente invención, la información de posición de algunas de las teclas de cifrado se puede usar cuando se realiza la autenticación de usuario.

Por ejemplo, cuando una contraseña es 4312, un usuario no necesita introducir la totalidad de los cuatro dígitos de la contraseña y puede introducir los primeros dos dígitos 4 y 3, los últimos dos dígitos 1 y 2, o el primer y el tercer dígitos.

Cuando se introducen los dos primeros dígitos 4 y 3, las posiciones de la contraseña son (0,5, 2,5) y (3,5, 3,5), como se muestra en la figura 4.

En consecuencia, la autenticación de usuario se realiza en función de las posiciones (0,5, 2,5) y (3,5, 3,5) de la contraseña, su orden de entrada e información biométrica (por ejemplo, información de huella dactilar, información de iris, etc.).

Cuando se realiza una autenticación de usuario en función de información de posición de algunas teclas de cifrado, es posible aumentar la velocidad de cálculo debido a que la cantidad de datos requeridos para realizar la autenticación es menor que la de la información de posición de todas las teclas de cifrado, y también es posible para mejorar la conveniencia para el usuario debido a que el número de teclas de cifrado que se debería introducir es

menor que el número total de teclas de cifrado.

Las figuras 3A y 3B son diagramas que muestran un teclado numérico variable que se genera en primer lugar y un teclado numérico variable que se genera en segundo lugar, respectivamente, como un ejemplo de un teclado numérico variable que incluye teclas de cifrado y una tecla de autenticación biométrica que se genera de tal modo que las posiciones de las teclas de cifrado y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable de acuerdo con una realización de la presente invención.

Como se muestra en las figuras 3A y 3B, las posiciones de las teclas de cifrado y la tecla de autenticación biométrica Bio en un teclado numérico variable se cambian cada vez que se genera el teclado numérico variable.

Las figuras 4A y 4B son diagramas que muestran un teclado numérico variable en un plano x - y de acuerdo con una realización de la presente invención, y la figura 4B es un diagrama que muestra información de posición de un teclado numérico variable en un plano x - y de acuerdo con una realización de la presente invención.

Como se muestra en la figura 4A, un usuario introduce una contraseña (por ejemplo, 4312) y presiona un botón de entrada de información biométrica Bio a través de un terminal móvil 100.

Por ejemplo, una información de posición de la contraseña se puede establecer como un valor de coordenadas en un plano x - y. Asimismo, la información de posición de la contraseña se puede establecer como un valor de coordenadas de un píxel. Esto es meramente un ejemplo, y la información de posición de la contraseña se puede transformar a otro formato.

La información de posición correspondiente a la contraseña de 4312 incluye (0,5, 2,5), (3,5, 3,5), (1,5, 3,5) y (2,5, 3,5), y el orden de la información de posición, tal como el orden de entrada de contraseña de 4 a 3 a 1 a 2, también tiene un significado significativo.

Cuando un usuario presiona el botón de entrada de información biométrica Bio, se activa un sensor de exploración de entrada de huella dactilar en una posición en la que se presiona el botón de entrada, y adquiere una imagen de huella dactilar del usuario.

De acuerdo con otra realización, cuando un usuario presiona el botón de entrada de información biométrica Bio, se muestra una ventana de entrada de huella dactilar en forma de una ventana emergente. La ventana de entrada de huella dactilar tiene un tamaño de 2,5 cm x 2,5 cm. El tamaño es suficiente para adquirir huellas dactilares de dedos que no sean el dedo índice.

La ventana de entrada de huella dactilar tiene la forma de una pantalla táctil. Cuando pasa un tiempo predeterminado después de que un usuario haya tocado con su dedo, se activa automáticamente el sensor de exploración de entrada de huella dactilar y, por lo tanto, la ventana de entrada de huella dactilar adquiere una imagen de huella dactilar del usuario.

La figura 5 es un diagrama que muestra un ejemplo de transmisión de información de posición de contraseña e información biométrica desde un terminal móvil a un servidor de autenticación de usuario.

Como se muestra en la figura 5, un terminal móvil 100 transmite información de posición de una contraseña, orden de entrada de la misma e información biométrica (por ejemplo, (0,5, 2,5), (3,5, 3,5), (1,5, 3,5), (2,5, 3,5), orden de entrada de la información de posición e información de huella dactilar) a un servidor de autenticación de usuario 200.

La figura 6 es un diagrama de flujo que muestra un ejemplo de extraer una contraseña a partir de posiciones de teclas de cifrado y realizar una autenticación de usuario de acuerdo con una realización de la presente invención.

Es decir, este caso supone que la contraseña está almacenada previamente en el servidor de autenticación de usuario 200. La autenticación de uso se realiza al recibir información de posición de una contraseña desde el terminal móvil 100, extraer la contraseña a partir de la información de posición recibida y el orden de entrada de la misma, y comparar la contraseña extraída con la contraseña almacenada en la unidad de almacenamiento de información de autenticación 230.

Como se muestra en la figura 6, la unidad de autenticación 220 recibe posiciones (por ejemplo, (0,5, 2,5), (3,5, 3,5), (1,5, 3,5), (2,5, 3,5) y orden de entrada de la información de posición) de las teclas de cifrado correspondientes al orden en el que las teclas de cifrado son introducidas por un miembro desde el terminal móvil 100 y extrae una contraseña (por ejemplo, 4312) introducida por el miembro (S142).

La unidad de autenticación 220 realiza una autenticación al comparar la contraseña extraída (por ejemplo, 412) y la información biométrica recibida (por ejemplo, información de huella dactilar, información de iris o similar) con una contraseña (por ejemplo, 4312) e información biométrica (por ejemplo, información de huella dactilar, información de iris o similar) que están almacenadas en la unidad de almacenamiento de información de autenticación 230 (S144).

La figura 7 es un diagrama que muestra un ejemplo de obtención de imágenes de un iris de un usuario y transmisión de la imagen de iris a un servidor de autenticación de usuario 200 de acuerdo con una realización de la presente invención.

Como se muestra en la figura 7, cuando la información biométrica es información de iris, un teclado numérico variable 110 adquiere de un usuario una entrada de un botón de indicación de entrada de iris.

Una unidad de control 130 controla una unidad de cámara 140 para obtener una imagen de un iris de un usuario delante.

La unidad de cámara 140 obtiene una imagen de un iris de un usuario de acuerdo con una instrucción de la unidad de control 130. La unidad de cámara 140 incluye un módulo de identificación biométrica. Cuando se obtiene una imagen de un iris, el módulo de identificación biométrica comprueba si una pupila se agranda o se reduce dependiendo de la luz incidente con el fin de determinar si el iris es un iris de una persona viva. En consecuencia, es posible mejorar adicionalmente la seguridad debido a que es fundamentalmente imposible realizar un reconocimiento de iris sobre un globo ocular de una persona muerta.

La unidad de control 130 transmite la imagen de iris al servidor de autenticación de usuario 200.

Posteriormente, se describirá un proceso en el que el servidor de autenticación de usuario 200 realiza una autenticación de usuario en función de la imagen de iris recibida desde el terminal móvil 100.

La unidad de autenticación 220 del servidor de autenticación de usuario 200 extrae una característica de identificación a partir de la imagen de iris recibida desde el terminal móvil 100.

El servidor de autenticación de usuario 200 mide la similitud al comparar la característica de identificación extraída con una característica de identificación almacenada en la unidad de almacenamiento de información de autenticación 230 y determina que el iris es el mismo que el almacenado en la unidad de almacenamiento de información de autenticación 230 cuando la similitud medida es mayor que o igual a un valor umbral predeterminado (por ejemplo, un 80 %).

Un iris humano se caracteriza por el hecho de que el mismo está completamente formado después de los 18 meses de edad y no cambia durante el curso de la vida. Asimismo, en el mundo viven diversos tipos de personas, pero no hay personas que tengan el mismo patrón de iris.

Debido a tales características únicas de los iris, la tecnología de reconocimiento biométrico tiene una seguridad más alta. La tecnología de reconocimiento de iris separa un área de un iris y un área de una esclerótica con respecto a una pupila negra y, entonces, explora un patrón del iris cuando se explora un ojo.

Un iris con aproximadamente 266 características de identificación medibles es más complejo y delicado que una huella dactilar con aproximadamente 40 características de identificación.

La figura 8 es un diagrama que muestra un ejemplo de realizar una autenticación primaria a través de un identificador correspondiente a un teclado numérico variable de acuerdo con una realización de la presente invención. Un identificador correspondiente a un teclado numérico variable que está almacenado en un servidor de autenticación en el lado izquierdo de la figura 8, y un identificador correspondiente a un teclado numérico variable que está almacenado en un terminal se muestra en el lado derecho de la figura 8.

Como se muestra en la figura 8, la unidad de autenticación 220 genera una pluralidad de teclados numéricos variables y genera identificadores (índices) correspondientes a los teclados numéricos variables. Es decir, cuando el servidor de autenticación de usuario 200 genera teclados numéricos variables, el servidor de autenticación de usuario 200 genera identificadores (índice 1, índice 2 e índice 3) correspondientes al teclado numérico variable 1, el teclado numérico variable 2 y el teclado numérico variable 3 y proporciona el teclado numérico variable 1, el teclado numérico variable 2 y el teclado numérico variable 3 y sus identificadores (el índice 1, el índice 2 y el índice 3) al terminal móvil 100 de antemano.

Con detalle, cada vez que se genera un teclado numérico variable, la unidad de autenticación 220 almacena un identificador correspondiente al teclado numérico variable generado en la unidad de almacenamiento de información de autenticación 230.

Por ejemplo, cuando el teclado numérico variable tiene el número 1, un identificador correspondiente al teclado numérico variable es el índice 1. La unidad de autenticación 220 almacena el identificador en la unidad de almacenamiento de información de autenticación 230 y comparte el identificador con un terminal móvil de antemano.

Cuando se recibe una solicitud de autenticación, la unidad de autenticación 220 selecciona uno de los identificadores

almacenados y proporciona el identificador seleccionado al terminal móvil 100. El terminal móvil 100 selecciona un teclado numérico variable que se va a usar para la autenticación de entre los teclados numéricos variables que se proporcionan de antemano en función del identificador recibido y visualiza el teclado numérico variable seleccionado en una pantalla del mismo.

La unidad de autenticación 220 realiza una autenticación secundaria al comparar una información de posición de teclas de cifrado, un orden de entrada de las mismas, una información de posición de una tecla de autenticación biométrica y una información biométrica de un miembro que se reciben desde el terminal móvil 100 con una información de posición de teclas de cifrado, un orden de entrada de las mismas, una información de posición de una tecla de autenticación biométrica y una información biométrica de un miembro que están almacenados en la unidad de almacenamiento de información de autenticación 230.

De acuerdo con esta realización, es posible mejorar adicionalmente la seguridad debido a que solo se transmite a un terminal móvil un identificador, en lugar de una estructura de disposición de un teclado numérico variable.

De acuerdo con la presente invención, una contraseña en sí que se introduce a través de un teclado numérico variable no se transmite a un servidor de autenticación de usuario, sino que se transmite información de posición de la contraseña correspondiente al orden en el que la contraseña es introducida por un usuario. En consecuencia, es posible mejorar la seguridad debido a que un pirata informático no se puede enterar de una contraseña incluso si el pirata informático intercepta información de posición de información secreta que se está transmitiendo desde un terminal a un servidor.

Asimismo, en comparación con la técnica relacionada en la que meramente se introducen cuatro dígitos de una contraseña y se cambia su posición, es posible mejorar adicionalmente la seguridad debido a que se realiza una autenticación de usuario a través de una contraseña e información biométrica.

Asimismo, es posible reducir la cantidad de datos que se transmiten y también aumentar la conveniencia para el usuario al transmitir solo una cierta información de seguridad desde un terminal móvil a un servidor de autenticación de usuario.

La figura 9 es un diagrama de secuencia que muestra un ejemplo de cifrado y descifrado de una clave de simetría temporal, una clave pública de un usuario y una clave privada de un usuario de acuerdo con una realización de la presente invención.

Como se muestra en la figura 9, la unidad de autenticación 220 genera una clave de simetría temporal (210) y transmite la clave de simetría temporal generada al terminal móvil 100 (S220).

El terminal móvil 100 cifra un mensaje con la clave de simetría temporal recibida desde la unidad de autenticación 220 y genera un texto cifrado (S230).

Posteriormente, el terminal móvil 100 cifra la clave de simetría temporal con una clave pública de un usuario A para generar una CLAVE-E (S240) y transmite el texto cifrado y la CLAVE-E a la unidad de autenticación 220 (S250).

La unidad de autenticación 220 descifra la CLAVE-E recibida desde el terminal móvil 100 con una clave privada del usuario A para restablecer la clave de simetría temporal (S260) y descifra el texto cifrado con la clave de simetría temporal para restablecer el mensaje (S270).

Posteriormente, la unidad de autenticación 220 extrae posiciones de teclas de cifrado, orden de entrada de las teclas de cifrado e información biométrica a partir del mensaje restablecido y realiza una autenticación de usuario al comparar la información extraída con la información de autenticación almacenada previamente.

De acuerdo con otra realización de la presente invención, la autenticación de usuario se puede realizar solo con la información biométrica.

Mediante el uso de la información biométrica, es posible mejorar la conveniencia para el usuario debido a que un usuario no necesita recordar una contraseña, mejorar la seguridad debido a que no hay riesgo alguno de filtración de una contraseña y también, fundamentalmente, evitar la posibilidad de que una contraseña sea robada por un tercero en línea.

Asimismo, desde el punto de vista de un vendedor en el comercio electrónico, cuando se usa información biométrica, es difícil que un cliente cometa un fraude o engaño, y también es posible reducir el coste y mantener una cuenta secreta o similar.

Asimismo, desde un punto de vista público, es posible facilitar la detección de fraudes y reducir el riesgo de uso indebido o abuso de información con respecto a otras personas.

La materia objeto descrita anteriormente de la presente invención se ha de considerar ilustrativa y no restrictiva, y se debería entender que numerosas otras modificaciones y realizaciones pueden ser ideadas por los expertos en la materia sin apartarse del alcance de la invención como es definido por las reclamaciones. En consecuencia, las realizaciones de la presente invención se han de considerar descriptivas y no restrictivas de la presente invención.

REIVINDICACIONES

1. Un servidor de autenticación de usuario (200) que usa tanto una contraseña como información biométrica, comprendiendo el servidor de autenticación de usuario (200):

una unidad de generación de teclado numérico variable (210) configurada para generar un teclado numérico variable (110) que incluye teclas para posibilitar que un usuario de un terminal móvil (100) introduzca una contraseña, y una tecla de autenticación biométrica para posibilitar que el usuario del terminal móvil (100) genere información biométrica, en donde las posiciones de las teclas y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico (110);
una unidad de almacenamiento de información de autenticación (230) configurada para almacenar información de autenticación de usuarios de terminal móvil (100); y
una unidad de autenticación (220) configurada para realizar una autenticación de usuario al proporcionar información sobre el teclado numérico variable (110) generado al terminal móvil (100) ubicado en una posición remota y comparar información biométrica e información de posición de las teclas que forman la contraseña correspondiente al orden en el que se introducen las teclas que se reciben desde el terminal móvil (100) con la información de autenticación almacenada en la unidad de almacenamiento de información de autenticación (230).

2. El servidor de autenticación de usuario (200) de la reivindicación 1, en donde la unidad de autenticación (220) extrae la contraseña introducida por el usuario a partir de la información de posición de las teclas correspondiente al orden en el que las teclas son introducidas por el usuario y realiza una autenticación de usuario al comparar la contraseña extraída y la información biométrica recibida con la información de autenticación almacenada en la unidad de almacenamiento de información de autenticación (230).

3. El servidor de autenticación de usuario (200) de la reivindicación 1, en donde la unidad de autenticación (220) almacena la información de posición y el orden de entrada de las teclas correspondientes a la contraseña cada vez que se genera el teclado numérico variable (110) y, cuando la unidad de autenticación (220) recibe la información biométrica y la información de posición de las teclas correspondiente al orden en el que las teclas son introducidas por el usuario desde el terminal móvil (100), la unidad de autenticación (220) realiza una autenticación de usuario al comparar la información biométrica, la información de posición y el orden de entrada recibidos con la información de posición de las teclas, el orden de entrada de las teclas y la información biométrica que están almacenados.

4. El servidor de autenticación de usuario (200) de la reivindicación 1, en donde la unidad de autenticación (220) almacena un identificador correspondiente al teclado numérico variable cada vez que se genera el teclado numérico variable, proporciona el identificador almacenado al terminal móvil (100), cuando se recibe un identificador desde el terminal móvil (100), realiza una autenticación primaria al comparar el identificador recibido con el identificador almacenado, y realiza una autenticación secundaria cuando la primera autenticación se realiza con éxito al comparar la información de posición de las teclas, el orden de entrada de las mismas y la información biométrica del usuario que se reciben desde el terminal móvil (100) con la información de posición de las teclas, el orden de entrada de las mismas y la información biométrica del usuario que están almacenados en la unidad de almacenamiento de información de autenticación (230).

5. El servidor de autenticación de usuario (200) de la reivindicación 1, en donde la unidad de autenticación (220) genera una clave de simetría temporal cada vez que se genera el teclado numérico variable, proporciona la clave de simetría temporal generada al terminal móvil (100), cuando el terminal móvil cifra un mensaje que incluye la información de posición de las teclas, el orden de entrada de las teclas y la información biométrica con la clave de simetría temporal y cifra la clave de simetría temporal con una clave pública del usuario, recibe el mensaje cifrado y la clave de simetría temporal cifrada desde el terminal móvil (100), descifra la clave de simetría temporal cifrada con una clave privada del usuario, descifra el mensaje con la clave de simetría temporal descifrada, extrae la información de posición de las teclas, el orden de entrada de las teclas y la información biométrica a partir del mensaje, y realiza una autenticación de usuario al comparar la información de posición extraída, el orden de entrada y la información biométrica con la información de posición de las teclas, el orden de entrada de las teclas y la información biométrica que están almacenados previamente.

6. Un terminal móvil (100) capaz de una autenticación de usuario, comprendiendo el terminal móvil (100):

una unidad de visualización (120) configurada para visualizar información sobre un teclado numérico variable (110) que incluye teclas, para posibilitar que un usuario de un terminal móvil (100) introduzca una contraseña, y que incluye adicionalmente una tecla de autenticación biométrica usada por el usuario del terminal móvil (100) para generar información biométrica, en donde las posiciones de las teclas y de la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable (110); y
una unidad de control (130) configurada para recibir la información sobre el teclado numérico variable (110) desde un servidor de autenticación de usuario (200) y entregar información de posición de las teclas, que forman la contraseña, correspondiente al orden en el que se introducen las teclas, y la información biométrica al servidor de autenticación de usuario (200) a través del teclado numérico variable (110).

7. El terminal móvil (100) de la reivindicación 6, que comprende adicionalmente una unidad de cámara (140) configurada para capturar una imagen delante, en donde,
cuando la información biométrica es información de iris y el teclado numérico variable (110) adquiere del usuario una entrada de un botón de indicación de entrada de iris, la unidad de control (130) controla la unidad de cámara (140) para capturar una imagen de un iris del usuario delante y transmitir la imagen de iris capturada al servidor de autenticación de usuario (200).

8. Un método para realizar una autenticación de usuario usando tanto una contraseña como información biométrica por un servidor de autenticación de usuario (200), comprendiendo el método:

generar (S110) un teclado numérico variable (110) que incluye teclas para posibilitar que un usuario de un terminal móvil (100) introduzca una contraseña, y una tecla de autenticación biométrica usada por el usuario del terminal móvil (100) para generar información biométrica, en donde las posiciones de las teclas y la tecla de autenticación biométrica se cambian cada vez que se genera el teclado numérico variable (110);
transmitir (S120) el teclado numérico variable (110) generado a un terminal móvil (100); recibir (S130) información biométrica e información de posición de las teclas, que forman la contraseña, correspondiente al orden en el que las teclas son introducidas por un usuario desde el terminal móvil (100); y
realizar (S140) una autenticación de usuario basándose en la información biométrica y la información de posición de las teclas recibidas.

9. El método de la reivindicación 8, en el que realizar una autenticación de usuario comprende realizar una autenticación de usuario basándose en información de posición de algunas de las teclas.

10. El método de la reivindicación 8, en donde realizar una autenticación de usuario comprende extraer una contraseña introducida por el usuario a partir de la información de posición de las teclas correspondiente al orden en el que las teclas son introducidas por el usuario y realizar una autenticación de usuario al comparar la contraseña extraída y la información biométrica recibida con una contraseña e información biométrica almacenadas en la unidad de almacenamiento de información de autenticación.

FIG. 1

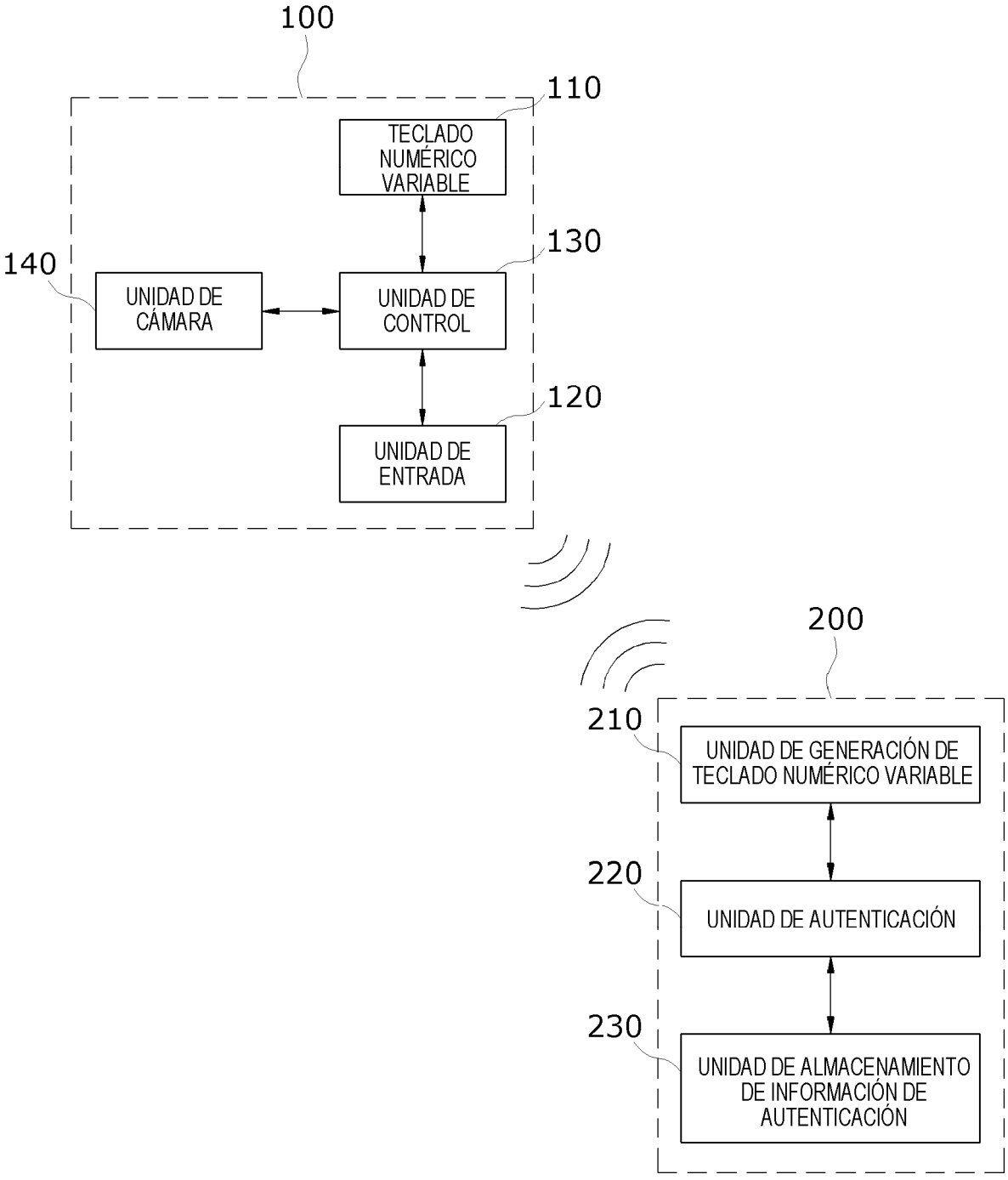

100
110
TECLADO NUMÉRICO VARIABLE
130
140
UNIDAD DE CÁMARA
UNIDAD DE CONTROL
120
UNIDAD DE ENTRADA
200
210
UNIDAD DE GENERACIÓN DE TECLADO NUMÉRICO VARIABLE
220
UNIDAD DE AUTENTICACIÓN
230
UNIDAD DE ALMACENAMIENTO DE INFORMACIÓN DE AUTENTICACIÓN

FIG. 2

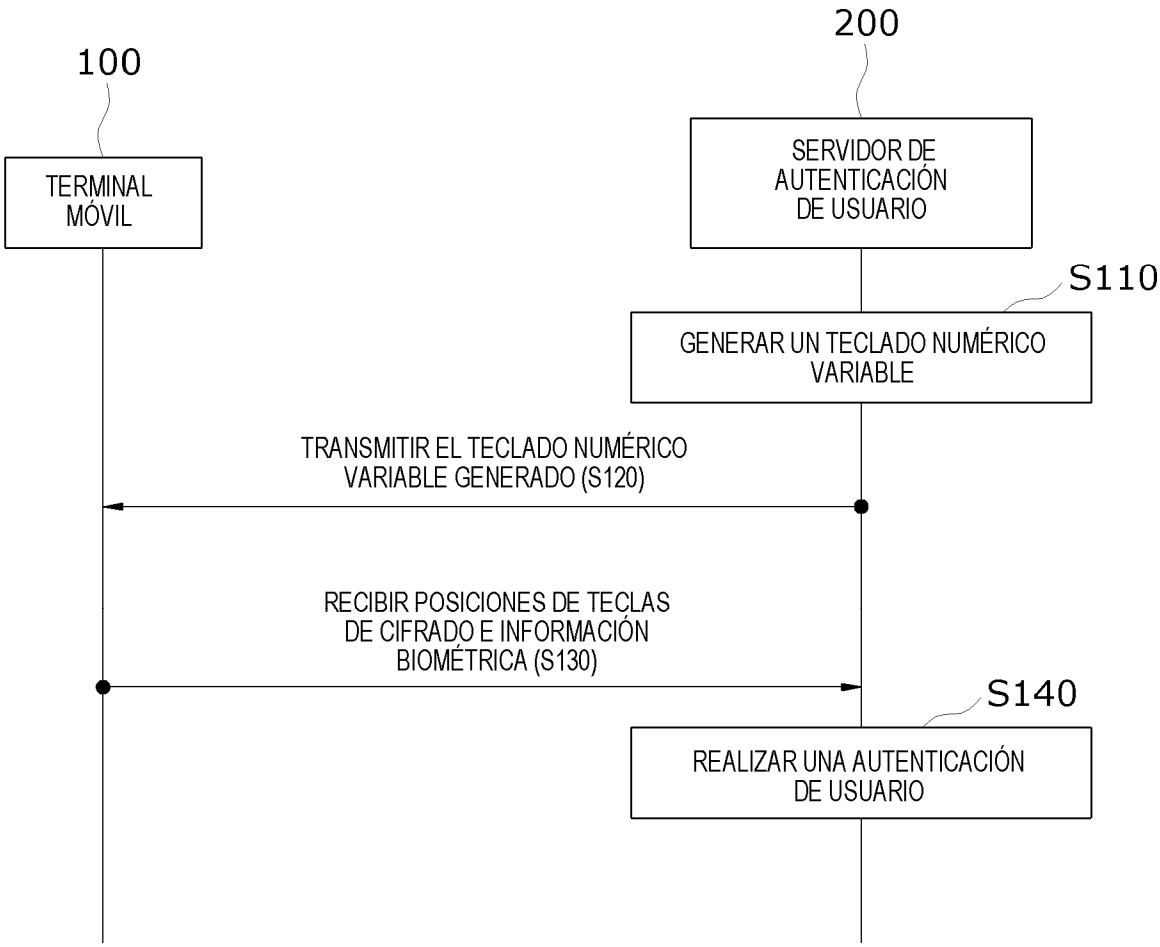

100
TERMINAL MÓVIL
200
SERVIDOR DE AUTENTICACIÓN DE USUARIO
S110
GENERAR UN TECLADO NUMÉRICO VARIABLE
TRANSMITIR EL TECLADO NUMÉRICO VARIABLE GENERADO (S120)
RECIBIR POSICIONES DE TECLAS DE CIFRADO E INFORMACIÓN BIOMÉTRICA (S130)
S140
REALIZAR UNA AUTENTICACIÓN DE USUARIO

FIG. 3A

PRIMERA VEZ

	1	2	3
4	Bio	5	6
*	7	8	#
9	CANCELAR	CORREGIR	0

FIG. 3B

SEGUNDA VEZ

*	6	7	8
9		0	#
CORREGIR	1	Bio	2
3	CANCELAR	4	5

FIG. 4A

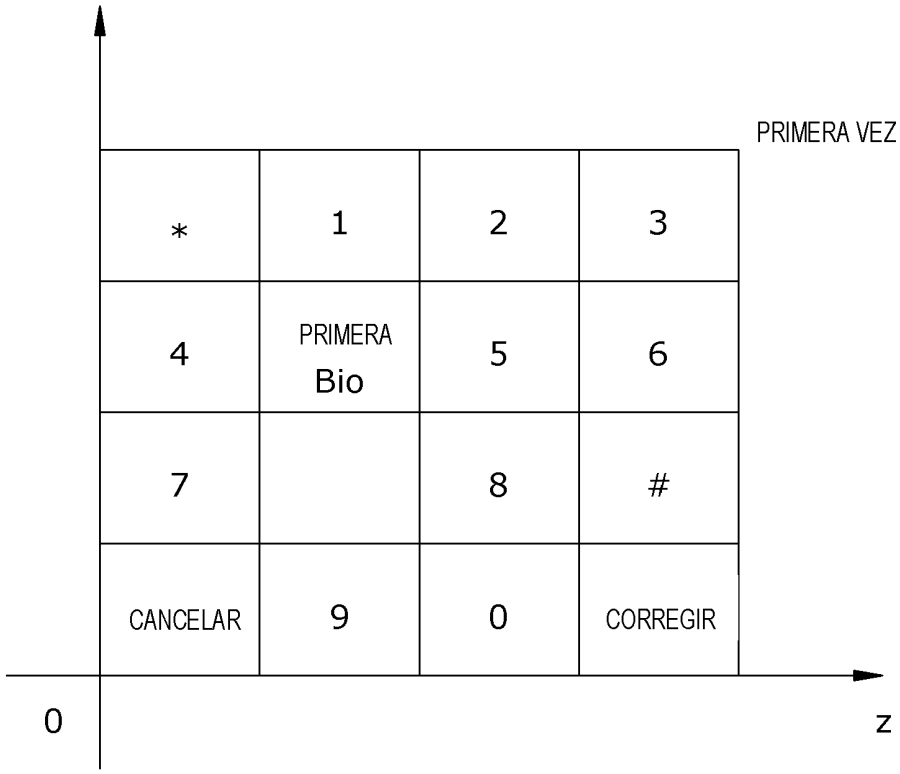


FIG. 4B

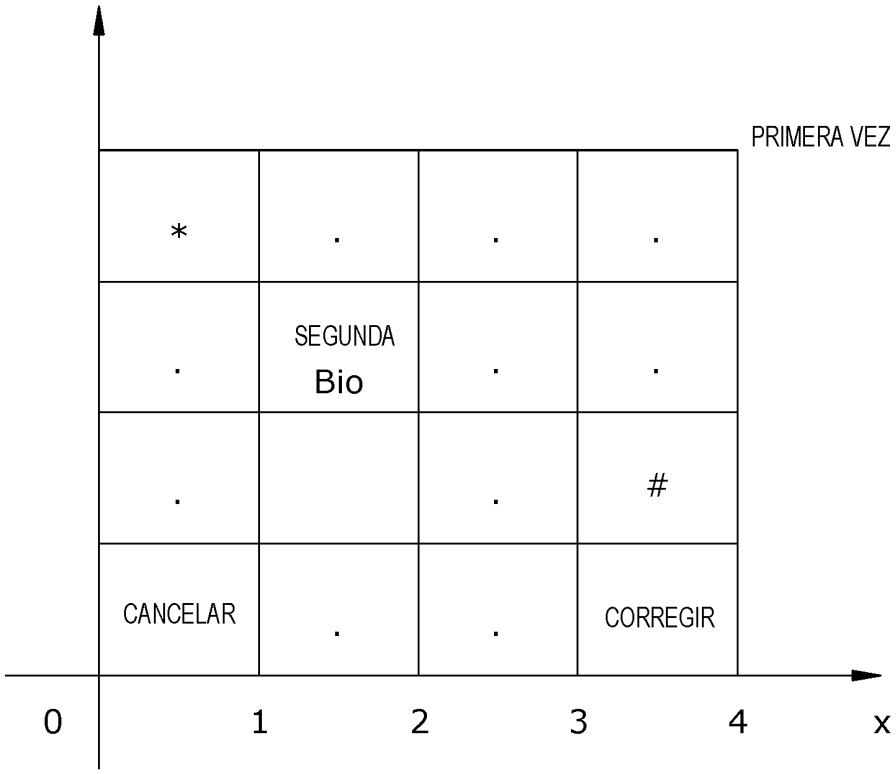


FIG. 5

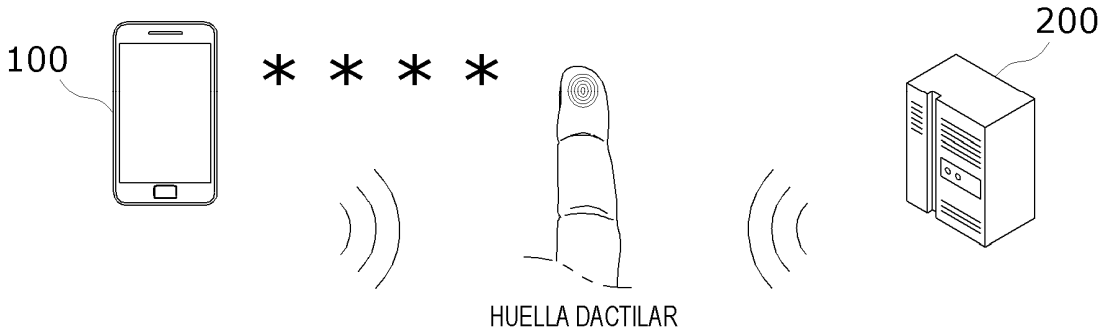


FIG. 6

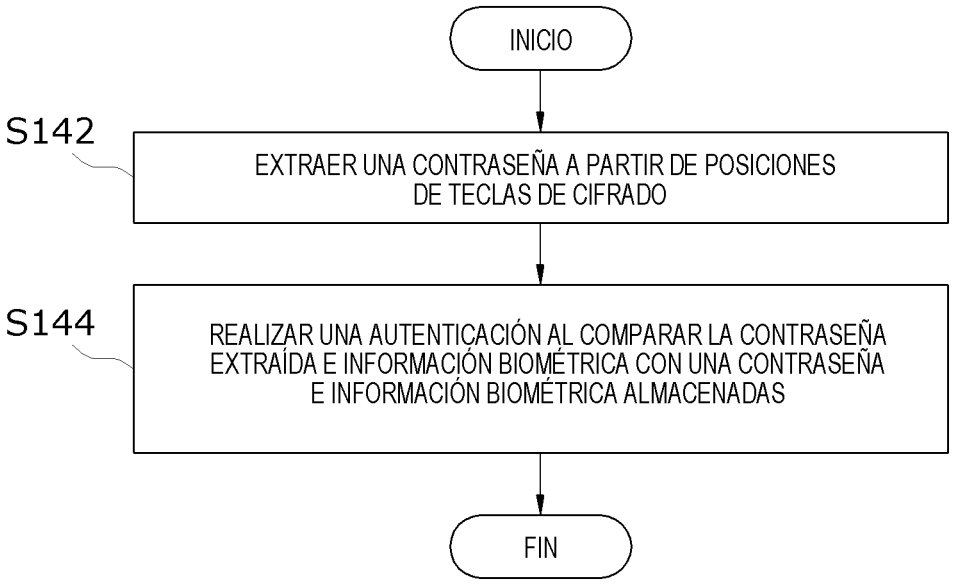

INICIO
S142
EXTRAER UNA CONTRASEÑA A PARTIR DE POSICIONES DE TECLAS DE CIFRADO
S144
REALIZAR UNA AUTENTICACIÓN AL COMPARAR LA CONTRASEÑA EXTRAÍDA E INFORMACIÓN BIOMÉTRICA CON UNA CONTRASEÑA E INFORMACIÓN BIOMÉTRICA ALMACENADAS
FIN

FIG. 7

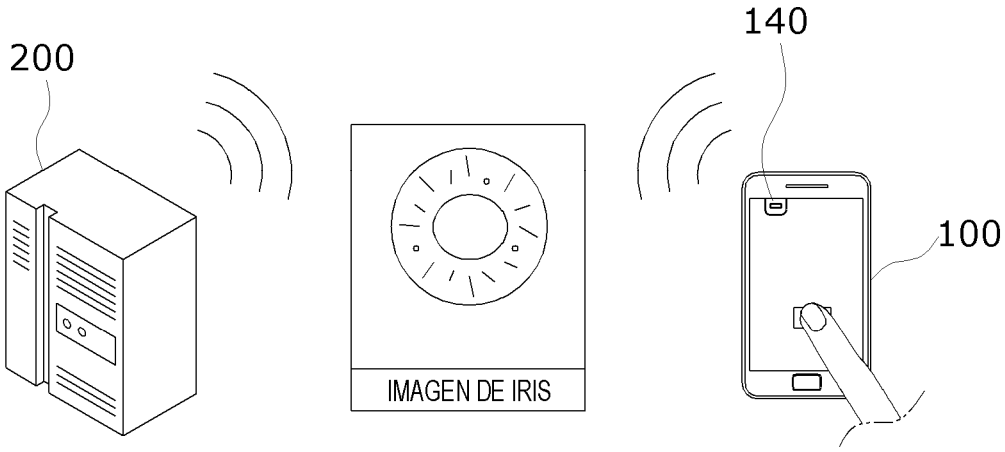


FIG. 8

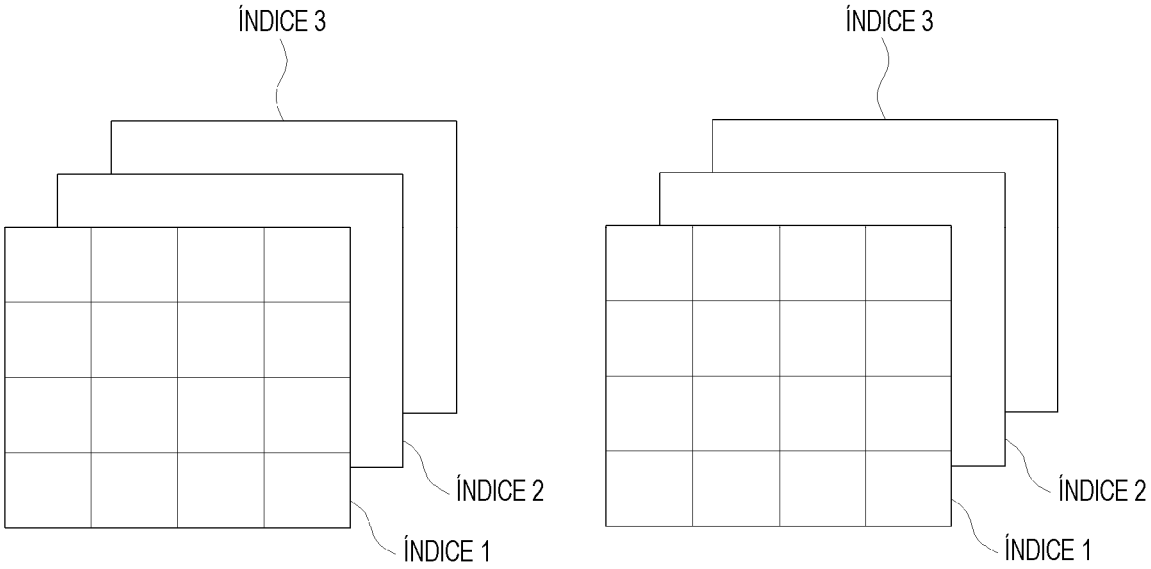
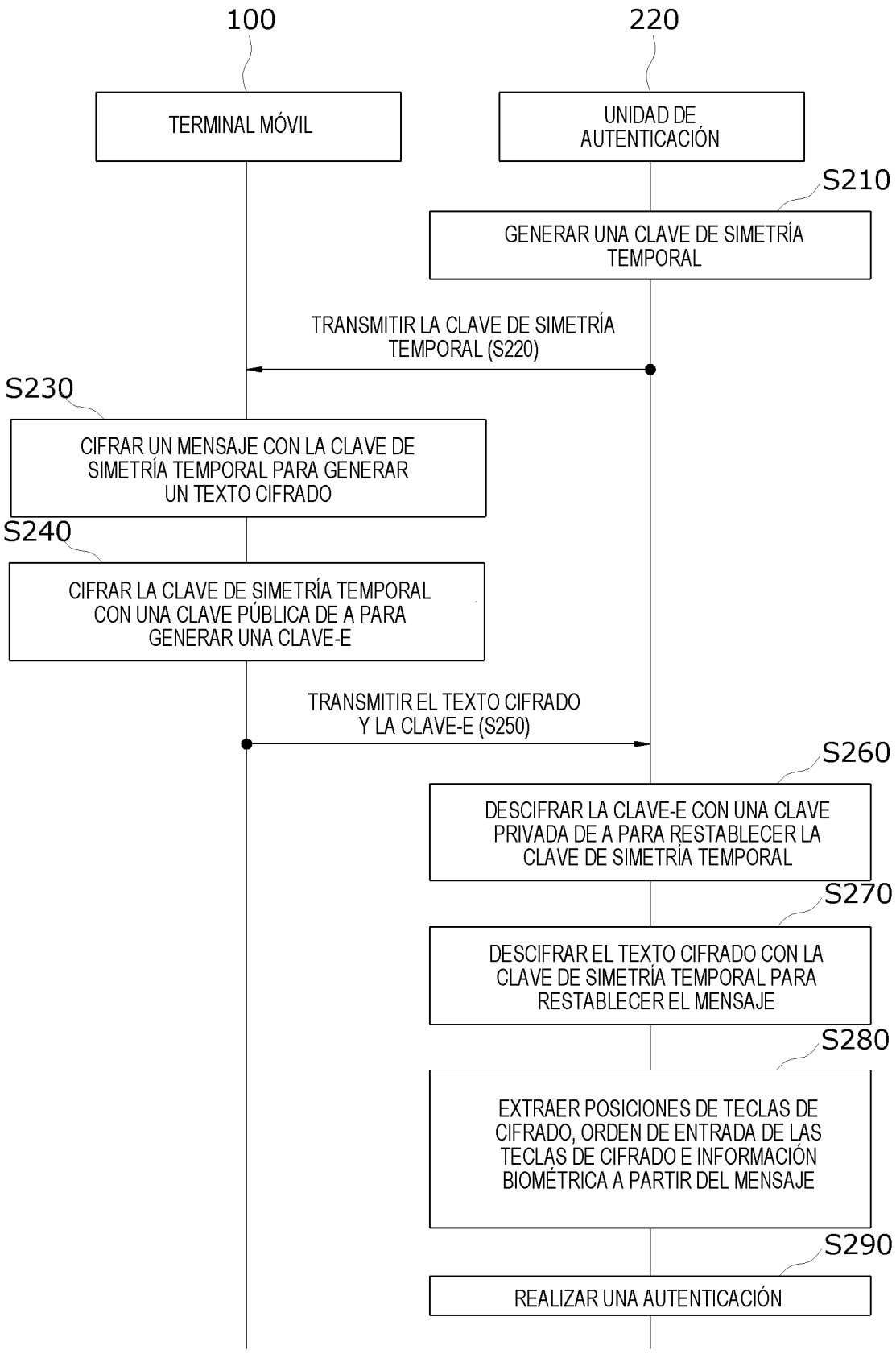


FIG. 9


100
220
TERMINAL MÓVIL
UNIDAD DE AUTENTICACIÓN
S210
GENERAR UNA CLAVE DE SIMETRÍA TEMPORAL
TRANSMITIR LA CLAVE DE SIMETRÍA TEMPORAL (S220)
S230
CIFRAR UN MENSAJE CON LA CLAVE DE SIMETRÍA TEMPORAL PARA GENERAR UN TEXTO CIFRADO
S240
CIFRAR LA CLAVE DE SIMETRÍA TEMPORAL CON UNA CLAVE PÚBLICA DE A PARA GENERAR UNA CLAVE-E
TRANSMITIR EL TEXTO CIFRADO Y LA CLAVE-E (S250)
S260
DESCIFRAR LA CLAVE-E CON UNA CLAVE PRIVADA DE A PARA RESTABLECER LA CLAVE DE SIMETRÍA TEMPORAL
S270
DESCIFRAR EL TEXTO CIFRADO CON LA CLAVE DE SIMETRÍA TEMPORAL PARA RESTABLECER EL MENSAJE
S280
EXTRAER POSICIONES DE TECLAS DE CIFRADO, ORDEN DE ENTRADA DE LAS TECLAS DE CIFRADO E INFORMACIÓN BIOMÉTRICA A PARTIR DEL MENSAJE
S290
REALIZAR UNA AUTENTICACIÓN