(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 417 479**

(51) Int. CI.:

G06F 15/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.02.2003 E 03705121 (6)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2013 EP 1475721**

(54) Título: **Procedimiento de autenticación de usuario y sistema de autenticación de usuario**

(30) Prioridad:

13.02.2002 JP 2002036056

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.08.2013

(73) Titular/es:

PASSLOGY CO., LTD. (100.0%)
Fukuroku Build. 4F, 2-7 Kanda-Tsukasamachi, Chiyoda-ku
Tokyo 101-0048 , JP

(72) Inventor/es:

OGAWA HIDEHARU

(74) Agente/Representante:

FÚSTER OLAGUIBEL, Gustavo Nicolás

DESCRIPCIÓN

Procedimiento de autenticación de usuario y sistema de autenticación de usuario.

ANTECEDENTES

La presente invención se refiere a un procedimiento de verificación de usuario y a un sistema de verificación de usuario para llevarlo a cabo.

En los últimos años, se han generalizado diversos aparatos informáticos, de los cuales los ordenadores son un ejemplo representativo. En particular, los teléfonos móviles provistos de funciones de correo electrónico y funciones de conexión a Internet se han extendido de forma extremadamente rápida y se han convertido en dispositivos informáticos necesarios para las personas.

A medida que avanza esta sociedad de la información, el acceso ilegítimo a los sistemas y otros problemas de seguridad se han vuelto extremadamente importantes. Tradicionalmente, para impedir el acceso ilegítimo a los sistemas, un procedimiento común es el de usar una identidad y contraseña de usuario registradas con anterioridad para llevar a cabo la verificación del usuario. Sin embargo, para responder a una necesidad de niveles de seguridad aún más altos, se han realizado propuestas de diversos procedimientos de verificación de usuario adaptados a distintos entornos de uso y objetivos.

Uno de ellos es el sistema de verificación de usuario que limita los dispositivos terminales que pueden acceder a un sistema. Este procedimiento se basa en la premisa de que la persona que posee el dispositivo terminal es la misma persona que lo usa. Por ejemplo, cuando se accede desde un teléfono móvil a un sistema determinado, se puede usar un número de identificación por unidad, que se asigna a dicho teléfono móvil para lograr una verificación de usuario más segura.

Además, también se conoce la verificación de usuario en la que se usa una tabla de números aleatorios. En esta verificación de usuario en la que se usa una tabla de números aleatorios, se adjudican previamente a cada usuario tarjetas de tablas de números aleatorios con tablas de números aleatorios escritas, y cada vez que se lleva a cabo la verificación de usuario, el sistema designa un carácter en una posición escogida libremente de la tabla de números aleatorios y solicita al usuario que lo introduzca. Por tanto, debido a que el carácter introducido cambia cada vez, este procedimiento resulta eficaz contra las «escuchas ocultas».

En la verificación de usuario llevada a cabo en el sistema, si se filtra («escuchas ocultas») la contraseña que se está usando allí, se originarán gravísimos problemas de seguridad. Por lo tanto, la gestión que haga el usuario de la contraseña resulta extremadamente importante y es fundamental que cada usuario se responsabilice de sus propias acciones cuando se consideran los problemas de seguridad del sistema.

En general, para cada sistema se requieren diferentes contraseñas usadas para la verificación de usuario y existen diversos formatos. Así, los usuarios que usan muchos sistemas deben gestionar muchas contraseñas y la gestión de las contraseñas se convierte en un engorro para el usuario. Debido a las características de las contraseñas, el usuario debería tratar de conservar la contraseña en la memoria, pero cuando se gestionan muchas contraseñas, no es raro que se anoten en un cuaderno o similar. Además, los usuarios a los que les resulta difícil gestionar sus contraseñas han escogido contraseñas con caracteres fáciles de recordar o han escogido los mismos caracteres para la contraseña de cada sistema para gestionarlas de manera integrada.

Sin embargo, dichas acciones del usuario en relación con la gestión de contraseñas conllevan que el sistema se vea expuesto a riesgos de seguridad. Mientras el usuario actúe de este modo, la verificación de usuario con contraseña prevista originalmente presentará problemas de seguridad fundamentales.

Además, aunque el usuario preste mucha atención a la hora de gestionar la contraseña, seguirá habiendo problemas de seguridad, como, por ejemplo, cuando la contraseña que se introduce en un terminal de una tienda es observado de manera ilegítima o cuando en el propio terminal se incorpora un mecanismo de «escucha oculta», de manera que la contraseña se filtre a un tercero.

Además, incluso en una verificación de usuario como la descrita, en la que los teléfonos móviles que pueden acceder al sistema están restringidos, cuando un usuario pierde un teléfono móvil, o se lo roban o pasa a manos de un tercero, solo se logra un nivel de seguridad equivalente al que se obtiene al llevar a cabo una verificación de usuario tradicional y, por tanto, este tipo de verificación de usuario presentaba dificultades a la hora de impedir de manera eficaz el acceso ilegítimo al sistema. Era similar incluso al de una verificación de usuario en la que se usan las tablas de números aleatorios.

Además de lo expuesto anteriormente, se observó que en los documentos WO 01/63545 A1 y US 5 742 035 se revelaban conceptos afines. Las respectivas memorias descriptivas se referían a la verificación de usuarios autorizados y dispositivos mnemotécnicos para números pin de tarjetas de crédito.

RESUMEN

Por lo tanto, para resolver los problemas mencionados anteriormente, la invención tiene por objeto proporcionar un nuevo procedimiento de verificación de usuario y un sistema para llevarlo a cabo que eviten de manera eficaz el acceso ilegítimo a un sistema por parte de un tercero.

Además, otro objeto de la presente invención consiste en proporcionar dicho procedimiento de verificación de usuario y dicho sistema para llevarlo a cabo, que utilicen al máximo la infraestructura existente del sistema, de manera que no suponga un coste excesivo.

Además, otro objeto de la presente invención consiste en proporcionar un procedimiento de verificación de usuario y un sistema para poder llevarlo a cabo que impidan de manera eficaz el acceso ilegítimo al sistema, al tiempo que se consiga que la gestión de contraseñas que realiza el usuario sea sencilla y su uso resulte práctico para todos los usuarios. Por extensión, la presente invención tiene por objeto eliminar los problemas de seguridad fundamentales ocasionados por las acciones de los usuarios.

Además, otro objeto de la presente invención consiste en proporcionar un procedimiento de registro y una interfaz de usuario para llevar a cabo dicho procedimiento de registro, para registrar una «contraseña» que se use en los procedimientos de verificación descritos anteriormente y en los sistemas para llevar a cabo los procedimientos de verificación de usuario.

Los problemas citados anteriormente se resuelven por medio de los conceptos definidos en las reivindicaciones independientes. Las formas de realización preferidas se definen en las reivindicaciones dependientes.

La presente invención es un procedimiento de verificación de usuario y un sistema de verificación de usuario, en los que se registra previamente un patrón de obtención de contraseña para cada usuario en un servidor de verificación, y después, cuando el usuario va a utilizar un sistema de destino usado, el servidor de verificación genera un patrón presentado y lo presenta al usuario. Después, el usuario introduce una cadena de caracteres correspondiente al propio patrón de obtención de contraseña del usuario para el patrón presentado. A continuación, el servidor de verificación efectúa una confirmación de la cadena de caracteres introducida basándose en el patrón presentado y el patrón de obtención de contraseña del propio usuario, y después se notifica el resultado de la confirmación al sistema de destino utilizado.

El «patrón de obtención de contraseña» se refiere a un elemento (grupo) específico que el usuario selecciona libremente entre un grupo de elementos que constituyen un patrón global. Más concretamente, el patrón de obtención de contraseña es un patrón matricial o regla matricial que muestra qué grupo de elementos se seleccionó a partir de una matriz que constituye el patrón global. Cabe señalar aquí que el patrón de obtención de contraseña no se refiere a los valores específicos de elementos específicos en el patrón global, sino que, en último término, se limita a indicar la información acerca de qué elemento fue seleccionado.

Más concretamente, de acuerdo con un primer aspecto, la presente invención es un procedimiento de verificación de usuario que comprende las siguientes etapas: una etapa de registro en la que se registra un patrón de obtención de contraseña basándose en un elemento específico seleccionado entre un grupo de elementos que constituyen un patrón predeterminado; una etapa de recepción en la que se recibe información de identificación del sistema asignada a un sistema de destino de uso, que se envía desde un terminal informático de un usuario; una etapa de generación en la que se genera un patrón presentado en el que se asigna un carácter predeterminado a cada elemento del grupo de elementos que constituye el patrón predeterminado cuando se recibe la información de identificación del sistema procedente del terminal informático; una etapa de introducción en la que se presenta en el terminal informático una pantalla predeterminada que contiene el patrón presentado generado, y se solicita al usuario que introduzca un carácter asignado a un elemento específico correspondiente al patrón de obtención de contraseña; una etapa de toma de decisión en la que se recibe el carácter introducido procedente del sistema de destino de uso, y se decide si el carácter recibido es legítimo o no en función del patrón presentado y el patrón de obtención de contraseña del usuario; y una etapa de notificación en la que se notifica al sistema de destino de uso el resultado de la toma de decisión.

Además, de acuerdo con un segundo aspecto, la presente invención consiste en un procedimiento de verificación de usuario que comprende las etapas de registro de un patrón de obtención de contraseña, basándose en un elemento específico seleccionado entre un grupo de elementos que forman un patrón predeterminado; recepción de información de identificación del sistema asignada a un sistema de destino de uso, que se envía desde un terminal informático del usuario; generación de un patrón presentado en el que se asigna un carácter predeterminado a cada elemento del grupo de elementos que forma el patrón predeterminado, cuando se recibe la información de identificación predeterminada procedente del terminal informático; presentación, en el terminal informático, de una pantalla predeterminada que contiene el patrón presentado generado, en la que se solicita al usuario que introduzca el carácter asignado a un elemento específico correspondiente al patrón de obtención de contraseña; recepción del carácter introducido desde el terminal informático, y toma de decisión acerca de si el carácter recibido es legítimo o no, basada en el patrón presentado y el patrón de obtención de contraseña del usuario; y notificación del resultado de la toma de decisión al sistema de destino de uso.

El procedimiento de la invención mencionado anteriormente se puede entender como una invención de un dispositivo. Además, estas invenciones se pueden llevar a la práctica en forma de programas y medios de almacenamiento en los que se almacenen dichos programas que, junto con un hardware predeterminado, logren llevar a cabo funciones predeterminadas al ser ejecutados en un ordenador.

Nótese que, en la presente memoria descriptiva, el término «medios» no se refiere a medios meramente físicos, sino que también se incluyen los casos en los que el software lleva a cabo una función de los medios. Además, una función de un medio la pueden llevar a cabo dos o más medios físicos, y funciones de dos o más medios las puede llevar a cabo un medio físico.

DESCRIPCIÓN DE LOS DIBUJOS

La fig. 1 es un diagrama resumen que explica un esquema global de un procedimiento de verificación de usuario de acuerdo con una forma de realización de la presente invención;

la fig. 2 es un diagrama que explica un patrón de obtención de contraseña de acuerdo con una forma de realización de la presente invención;

la fig. 3 es un diagrama que muestra un ejemplo de una pantalla de registro de un patrón de obtención de contraseña, mostrada en un ordenador personal, de acuerdo con una forma de realización de la presente invención;

la fig. 4 es un diagrama que muestra un ejemplo de una pantalla de confirmación de configuración mostrada en el ordenador personal de acuerdo con una forma de realización de la presente invención;

la fig. 5 es un diagrama que muestra un ejemplo de una estructura de datos de una base de datos de verificación, de acuerdo con una forma de realización de la presente invención;

la fig. 6 es un diagrama que muestra un ejemplo de una pantalla de recepción mostrada en un sistema de destino de uso, de acuerdo con una forma de realización de la presente invención;

la fig. 7 es un diagrama que muestra un ejemplo de una pantalla de menú mostrada en un teléfono móvil, de acuerdo con una forma de realización de la presente invención;

la fig. 8 es un diagrama que muestra un ejemplo de una pantalla de inicio del procedimiento de verificación mostrada en el teléfono móvil, de acuerdo con una forma de realización de la presente invención;

la fig. 9 es un diagrama de flujo que explica el flujo del proceso en un servidor de verificación, de acuerdo con una forma de realización de la presente invención;

la fig. 10 es un diagrama que explica un ejemplo de una tabla de espera de solicitud de verificación de usuario de acuerdo con una forma de realización de la presente invención;

la fig. 11 es un diagrama que muestra un ejemplo de una pantalla de visualización de la tabla de números aleatorios, que se muestra en el teléfono móvil, de acuerdo con una forma de realización de la presente invención;

la fig. 12 es un diagrama que muestra un ejemplo de una pantalla de recepción que se muestra en el sistema de destino de uso de acuerdo con una forma de realización de la presente invención;

la fig. 13 es un diagrama que muestra un ejemplo de una pantalla de introducción de contraseña que se muestra en el sistema de destino de uso de acuerdo con una forma de realización de la presente invención;

la fig. 14 es un diagrama de flujo que explica el flujo del proceso en un servidor de verificación de acuerdo con una forma de realización de la presente invención;

la fig. 15 es un diagrama resumen que explica un esquema global de un procedimiento de verificación de usuario de acuerdo con una forma de realización de la presente invención;

la fig. 16 es un diagrama que muestra un ejemplo de una pantalla de registro del patrón de obtención de contraseña, mostrada en un teléfono móvil, de acuerdo con una forma de realización de la presente invención;

la fig. 17 es un diagrama que muestra un ejemplo de una pantalla de confirmación de configuración mostrada en un teléfono móvil, de acuerdo con una forma de realización de la presente invención;

la fig. 18 es un diagrama de flujo que explica el flujo del proceso de un procedimiento de registro del patrón de obtención de contraseña de acuerdo con una forma de realización de la presente invención;

la fig. 19 es un ejemplo de una pantalla que explica el procedimiento de registro del patrón de obtención de contraseña de acuerdo con una forma de realización de la presente invención;

la fig. 20 es otro ejemplo de una pantalla que explica el procedimiento de registro del patrón de obtención de contraseña de acuerdo con una forma de realización de la presente invención;

la fig. 21 es un diagrama resumen que explica un esquema global de un procedimiento de verificación de usuario de acuerdo con una forma de realización de la presente invención;

la fig. 22 es un diagrama que muestra un ejemplo de una estructura de datos de una base de datos de verificación 14;

la fig. 23 es un diagrama que muestra un ejemplo de una tabla de espera de solicitud de verificación de usuario;

la fig. 24 es un diagrama de flujo que explica el flujo del proceso en un servidor de verificación 12, de acuerdo con la presente forma de realización;

la fig. 25 es un diagrama de flujo que explica el flujo del proceso en un servidor de verificación 12, de acuerdo con la presente forma de realización;

la fig. 26 es un diagrama de flujo que explica el flujo del proceso en un servidor de verificación 12, de acuerdo con la presente forma de realización;

la fig. 27 es un diagrama de flujo que muestra el proceso para generar la información de identificación por sistema;

la fig. 28 es un diagrama de flujo que muestra un procedimiento de verificación de contraseña;

la fig. 29 es un diagrama que muestra una base de datos de códigos de funciones que hace que el proceso para informar a un sistema de destino de uso 11 se corresponda con un código de función que consiste en un carácter asociado correspondiente a ese proceso; y

la fig. 30 es un diagrama resumen que explica un esquema global del procedimiento de verificación de usuario, de acuerdo con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA

A continuación se explican formas de realización de la presente invención haciendo referencia a los dibujos. Las siguientes formas de realización son ejemplos ilustrativos que explican la presente invención, y con ellos no se pretende limitar la presente invención a las formas de realización. La presente invención se puede llevar a la práctica en diversas formas de realización, siempre que se haga sin alejarse de la esencia de la presente invención.

[Primera forma de realización]

La fig. 1 es un diagrama resumen que explica un esquema global de un procedimiento de verificación de usuario de acuerdo con la presente forma de realización. Como se muestra en la fig. 1, un sistema de destino de uso 11 está conectado a un servidor de verificación 12 a través de una línea de comunicación. Aquí se muestra un ejemplo en el que el sistema de destino de uso 11 está conectado al servidor de verificación 12 a través de Internet. El sistema de destino de uso 11 es un sistema que solicita la verificación de usuario para permitir el uso al usuario. El sistema de destino de uso 11, por medio del proceso de verificación de usuario que se describe más adelante, aprueba el uso por parte de un usuario que se decide que es legítimo. Como ejemplo típico de aplicación del sistema de destino de uso 11, se puede citar un sistema de apertura/cierre de llave de seguridad de una habitación o dispositivo terminal de pago por tarjeta de crédito, pero también puede tratarse de un sitio para miembros en Internet que se realice en forma de espacio virtual.

Este tipo de sistema de destino de uso 11 almacena una identificación única del sistema (información de identificación del sistema) en una memoria ROM interna. Además, el sistema de destino de uso 11 cuenta preferentemente con una interfaz de usuario para proporcionar un entorno operativo dialógico a un usuario. La interfaz de usuario, por ejemplo, está constituida por un teclado numérico y el correspondiente dispositivo de visualización. El sistema de destino de uso 11, a través de la interfaz de usuario, recibe una instrucción del usuario para «iniciar el uso» y muestra un identificador de sistema al usuario, y también recibe una entrada de contraseña introducida por el usuario y muestra un resultado de verificación de usuario.

Un dispositivo terminal inalámbrico 13 es un terminal informático portátil con funciones de comunicación inalámbrica, que corresponde típicamente a un teléfono móvil o PDA. Aquí se ofrece una explicación usando un teléfono móvil a modo de ejemplo. El teléfono móvil 13 se puede conectar desde una red de comunicaciones a través de un portal a diversos nodos (p. ej., el servidor de verificación 12) de Internet. Cuando se está utilizando el sistema de destino de uso 11, se usa el teléfono móvil 13 para proporcionar al usuario información de referencia para obtener una contraseña necesaria para la verificación del usuario.

El servidor de verificación 12 lleva a cabo la verificación de un usuario que intenta establecer el sistema de destino de uso 11 y notifica el resultado de la verificación al sistema de destino de uso 11. El servidor de verificación 12 cuenta con una base de datos de verificación 14 que gestiona los datos de registro necesarios para la verificación del usuario, proporcionados previamente por el usuario. La base de datos de verificación 14 gestiona, en forma de datos de registro, información sobre los usuarios que pueden utilizar el sistema de destino de uso 11 e información sobre el tipo de regla que ha registrado dicho usuario para la obtención de la contraseña. La información acerca de la regla de obtención de contraseña consiste en un patrón de obtención de contraseña y una regla de conversión que se describen más adelante. El servidor de verificación 12 posee una función de servidor web para recibir los datos de registro proporcionados en línea por el usuario.

El servidor de verificación 12 y la base de datos de verificación 14, típicamente, se pueden obtener usando un sistema informático de uso general. El servidor de verificación 12 está conectado de manera que se pueda comunicar con sistemas de destino de uso 11 individuales a través de líneas de comunicación. En ese caso, es preferible establecer comunicaciones seguras. Como en la presente forma de realización, cuando el sistema de destino de uso 11 y el servidor de verificación 12 se conectan a través de Internet, se pueden aplicar comunicaciones SSL u otras técnicas de seguridad semejantes en las comunicaciones para establecer comunicaciones seguras y prácticas. Obsérvese que también es posible conectarlos sin pasar por Internet, por medio de una línea dedicada.

Un ordenador personal 15 es un dispositivo terminal usado para que el usuario registre el patrón de obtención de contraseña en la base de datos de verificación 14. El ordenador personal 15 está construido de manera que se pueda conectar a Internet y posee una función de cliente web. Para registrar en la base de datos de verificación 14 los datos de registro necesarios para la confirmación del usuario, el usuario utiliza un navegador web para acceder al servidor de verificación 12.

Obsérvese que, para que el usuario registre el patrón de obtención de contraseña en la base de datos de verificación 14, también es posible usar el teléfono móvil 13 en lugar del ordenador personal 15. En la presente forma de realización, el motivo principal por el que se usa el ordenador personal 15 es que, por lo general, los ordenadores personales 15 son funcionalmente superiores a los teléfonos móviles 13 en lo que respecta a sus interfaces de usuario. En otra forma de realización, se ofrece una explicación referida a un ejemplo en el que se usa la interfaz de usuario del teléfono móvil 13 para registrar el patrón de obtención de contraseña.

El «patrón de obtención de contraseña» indica un grupo de elementos específico seleccionado libremente por el usuario, entre un grupo de elementos que forman un patrón global determinado. Para explicarlo de forma más concreta, se refiere a un patrón matricial o una regla matricial que muestra qué grupo de elementos de la matriz,

constituida por el patrón en su totalidad, fue seleccionado y cómo.

La fig. 2A y la fig. 2B son diagramas que explican el patrón de obtención de contraseña. La fig. 2A es un diagrama que muestra un ejemplo en el que una matriz de 4 filas y 12 columnas constituye el patrón global. En la fig. 2A y la fig. 2B, aparece un sombreado en los elementos seleccionados, y aparecen caracteres numéricos en los elementos de la secuencia de la selección. Por lo tanto, el patrón de obtención de contraseña en este caso se puede expresar, si se usa la expresión matricial, como: «(3, 2) - (0, 5) - (3, 7) - (0, 10)».

La fig. 2B es un diagrama que muestra un ejemplo en el que una matriz de 4 filas y 4 columnas constituye el patrón global. En este caso, el patrón de obtención de contraseña se puede expresar, si se usa la expresión matricial, como: «(0, 0) - (1, 2) - (2, 1) - (3, 2)».

El patrón de obtención de contraseña se usa para llevar a cabo la verificación de usuario con respecto al sistema de destino de uso 11 y, por tanto, el usuario debería recordarlo. Así, se puede decir que el patrón de obtención de contraseña es un tipo de contraseña. Se puede determinar libremente el número de elementos y el número de columnas que constituyen el patrón de obtención de contraseña, y se pueden establecer de manera apropiada según el nivel de seguridad de la verificación de usuario.

En un caso en el que la contraseña es una cadena de caracteres numéricos de J dígitos, el patrón global es preferentemente una matriz de K filas y L columnas, tal que satisface la siguiente condición:

$$10^J < (K*L) * (K*L-1) \cdot \cdot (K*L-J+1)$$

$$\cdot \cdot \text{Fórmula (1)}$$

En un procedimiento de verificación convencional, cuando la contraseña es una cadena de caracteres numéricos de J dígitos, existe un número de combinaciones de contraseñas de 10 veces J. Por otra parte, de acuerdo con el procedimiento de verificación de la presente forma de realización, cuando el patrón global es una matriz de K filas y L columnas, existen (K*L) * (K*L-1) · · (K*L-J+1) combinaciones de patrones de obtención de contraseña. Por lo tanto, al construir el patrón global de manera que satisfaga la fórmula (1) mencionada anteriormente, el número de combinaciones se puede aumentar más que en el procedimiento de verificación convencional, y se puede elevar el nivel de seguridad. Es decir, de acuerdo con la presente forma de realización, el número de dígitos de la contraseña que se debería introducir en el sistema de destino de uso 11 puede elevar fácilmente el nivel de seguridad por encima del procedimiento de verificación convencional, simplemente cambiando la estructura de la matriz, incluso en el mismo caso del procedimiento de verificación convencional.

Volviendo a la fig. 1, se ofrece una explicación en forma de resumen acerca del flujo del proceso en el procedimiento de verificación de usuario de acuerdo con la presente forma de realización.

En primer lugar, el usuario usa el ordenador personal 15 para registrar previamente su patrón de obtención de contraseña para el sistema de destino de uso 11 en la base de datos de verificación 14 ((1) en el diagrama). Cuando el usuario trata de usar el sistema de destino de uso 11, para obtener el identificador de sistema del mismo, el usuario utiliza la interfaz de usuario del sistema de destino de uso 11 para hacer que el sistema muestre en pantalla el identificador del sistema ((2) en el diagrama).

A continuación, el usuario introduce el identificador del sistema en el teléfono móvil 13, y lo envía al servidor de verificación 12 ((3) en el diagrama). El servidor de verificación 12 recibe el identificador del sistema, genera una tabla de números aleatorios y envía esta tabla al teléfono móvil 13 del usuario como un patrón presentado ((4) en el diagrama). El usuario consulta el patrón presentado en el teléfono móvil 13 e introduce la secuencia (cadena de caracteres numéricos) de valores de los elementos de su propio patrón de obtención de contraseña en el sistema de destino de uso 11 como contraseña. Así, el sistema de destino de uso 11 envía la contraseña al servidor de verificación 12 ((5) en el diagrama).

Cuando el servidor de verificación 12 recibe la contraseña procedente del sistema de destino de uso 11, el servidor de verificación 12 compara una cadena de caracteres numéricos obtenida a partir del patrón de obtención de contraseña que ya ha sido registrado y el patrón de obtención de contraseña generado, y la contraseña enviada desde el sistema de destino de uso 11, y decide si coinciden o no. El servidor de verificación 12 envía una notificación de verificación satisfactoria cuando coinciden, y una notificación de verificación fallida cuando no coinciden, al sistema de destino de uso 11 indicado por el identificador del sistema ((6) en el diagrama). Cuando el sistema de destino de uso 11 recibe la notificación de verificación satisfactoria procedente del servidor de verificación 12, el sistema de destino de uso 11 permite el uso por parte de dicho usuario.

De este modo, la contraseña que el usuario debería introducir es una contraseña temporal que se determina a partir de la tabla de números aleatorios generada cada vez que se lleva a cabo la verificación de usuario, de acuerdo con el patrón de obtención de contraseña registrado de antemano. Por lo tanto, aunque la contraseña introducida se filtrase a un tercero, la contraseña de por sí carecería por completo de sentido en la siguiente ocasión en que se llevase a cabo la confirmación de usuario, y de este modo se evitará de manera eficaz el acceso ilegítimo. Además, este tipo de patrón de obtención de contraseña que el usuario debe recordar no consiste en los «caracteres numéricos específicos» convencionales, sino en un patrón que es «conceptual y esquemático», y, por lo tanto, posee la cualidad de ser fácil de recordar y difícil de olvidar para el usuario, por lo cual resulta adecuado para la gestión de contraseñas.

A continuación, se ofrece una explicación al respecto de los datos de registro que se usan en la verificación de usuario. Para que el usuario utilice el sistema de destino de uso 11, antes del uso, el usuario debe obtener una cuenta de usuario (nombre de usuario) para el sistema de destino de uso 11, y también debe registrar un patrón de obtención

de contraseña para ese nombre de usuario. Por lo tanto, la base de datos de verificación 14 gestiona, a modo de datos de registro, qué sistema de destino de uso 11 ha otorgado derechos de uso a qué tipo de usuario, y qué tipo de patrones de obtención de contraseña han sido registrados por cada uno de los usuarios individuales a los que se han otorgado derechos de uso.

El registro de la cuenta de usuario para el sistema de destino de uso 11 se puede concebir, típicamente, en una forma en la que el gestor del sistema de destino de uso 11 recibe una solicitud por parte del usuario y la lleva a cabo, o en la que la lleva a cabo el propio usuario o usuaria. Se puede escoger adecuadamente el modo de registrar la cuenta de usuario de acuerdo con la política de funcionamiento del sistema de destino de uso 11. Para lograrlo, se pueden aplicar diversas técnicas existentes. Más adelante, en referencia a la cuenta de usuario para el sistema de destino de uso 11, se supone que el gestor registró la cuenta de usuario en la base de datos de verificación 14 y se ofrece una explicación al respecto de los procedimientos para que el usuario registre el patrón de obtención de contraseña.

La fig. 3 muestra un ejemplo de una pantalla de registro del patrón de obtención de contraseña que se muestra en el ordenador personal 15. Esta pantalla de registro está constituida por datos de página descritos mediante HTML u otro lenguaje equivalente de creación de páginas. El usuario maneja un navegador web para acceder al servidor de verificación 12, con el fin de que se muestre esta pantalla de registro en el ordenador personal 15. Por ejemplo, se puede usar un procedimiento en el que, en el momento en el que se registró la cuenta de usuario del sistema de destino de uso 11, el gestor enviaba por correo electrónico un texto que contenía una URL de datos de página que constituyen la pantalla de registro, a la dirección de correo de dicho usuario, y el usuario que los recibió selecciona la URL en el texto del correo, con lo cual se proporciona al usuario la pantalla de registro.

En el mismo diagrama, un campo de entrada de nombre de usuario 31 consiste en un campo para introducir el nombre usuario (cuenta de usuario) que utiliza el sistema de destino de uso 11. Como la cuenta de usuario ya está registrada con el gestor, se puede usar una construcción en la que el usuario no tenga que introducir de nuevo la cuenta de usuario, y la cuenta de usuario ya aparezca de antemano en el campo de entrada de nombre de usuario 31.

Un campo de entrada de nombre de grupo 32 es un campo para introducir un nombre de un grupo al que pertenece el usuario. No obstante, para simplificar las explicaciones, en la presente forma de realización no es necesario introducir el nombre del grupo.

Un campo de entrada de número de teléfono móvil 33 es un campo para introducir información de identificación individual para identificar el teléfono móvil 13 que se usará en la verificación de usuario cuando se utilice el sistema de destino de uso 11. De acuerdo con la presente forma de realización, se usa un número de teléfono móvil, que ha sido asignado al teléfono móvil 13 perteneciente al usuario. Obsérvese que es posible usar una construcción en la que el número de teléfono móvil 13 también esté previamente registrado con el gestor y ya aparezca de antemano en el campo de entrada de número de teléfono móvil 33.

Un patrón global 34 está formado por un objeto de botón, en el que un grupo de 48 elementos están alineados en forma de matriz de 4 filas y 12 columnas. Cada uno de los elementos recibe un número de serie del 1 al 48 como nombre de elemento, para distinguir los elementos individuales.

Un campo de entrada de designación de posición 35 es un campo para designar e introducir uno o más elementos específicos seleccionados entre la totalidad del patrón 34 usando sus nombres de elemento. En el presente ejemplo, se han introducido los elementos «1», «17», «33» y «48». En el caso en que se introduzcan una pluralidad de elementos, los elementos individuales se separan mediante un delimitador (p. ej., una coma). Además, se pueden introducir los mismos elementos. Aquí, la secuencia de elementos introducidos es el patrón de obtención de contraseña. La secuencia de elementos puede incluir un carácter ficticio «*». En el caso en que el usuario introduzca el carácter ficticio «*», se trata como una solicitud para establecer un carácter opcional. Aquí, junto con la regla de conversión que se muestra más adelante, este carácter ficticio impide que una tercera parte extrapole el patrón de obtención de contraseña. Es decir, debido a que el patrón de obtención de contraseña tiende a ser un patrón que resulta fácil de recordar para el usuario, se puede insertar un carácter sin sentido entre los caracteres que forman la contraseña propiamente dicha, a fin de evitar la extrapolación. Por ejemplo, en una secuencia de 8 elementos en la que los primeros 4 elementos son caracteres ficticios, el usuario puede introducir caracteres numéricos sin sentido para los primeros cuatro dígitos. Obsérvese que, cuando el usuario solo introduce «F» en el campo de entrada de designación de posición 35, se trata como una solicitud para establecer una contraseña fija, y en este caso se introducen un número predeterminado de dígitos de caracteres numéricos en un campo de entrada de contraseña fija 37.

Un campo de entrada de regla de conversión 36 es un campo en el que, cuando el usuario consulta el patrón presentado para proceder a introducir la contraseña, si se desea añadir otra regla de conversión más para los valores de elemento obtenidos a partir del patrón de obtención de contraseña, esta regla de conversión se introduce aquí. Es decir, los valores de elemento obtenidos a partir del patrón de obtención de contraseña se someten a otra regla de conversión añadida, y el resultado pasa a ser la auténtica contraseña que se debe introducir. En la regla de conversión, por ejemplo, se define una operación computacional de regla del 4 que se aplicará a los valores de elemento obtenidos a partir del patrón de obtención de contraseña. Más concretamente, cuando solo se introduce «+1» en el campo de entrada de regla de conversión 36, se suma «1» a cada uno de los valores de elemento obtenidos a partir del patrón de obtención de contraseña, y el resultado pasa a ser la auténtica contraseña que el usuario debería introducir. Además, cuando se usan comas, al igual que cuando se introduce «+1, +2, +3, +4» en el campo de entrada de regla de conversión 36, introduciéndose así la fórmula computacional de forma que corresponda a la secuencia de elementos introducidos en el campo de entrada de designación de posición 35, se aplica cada fórmula computacional a cada uno de los valores de elemento obtenidos a partir del patrón de obtención de contraseña, y su resultado pasa a ser la auténtica contraseña que el usuario debe introducir.

Obsérvese que, dependiendo de la fórmula computacional introducida, el resultado producido por la aplicación del cálculo a los valores de los elementos puede aumentar (o disminuir). En esos casos, si se hace que una definición use la primera posición, entonces se puede hacer que el número de dígitos (el número de caracteres) de la contraseña

puede tenga una longitud fija y sin fluctuaciones. Además, también es posible establecer una definición tal que el resultado producido al aplicar los cálculos a los valores de los elementos se utilice tal como está, para permitir contraseñas de longitud variable.

En este tipo de pantalla de registro, el usuario puede utilizar un teclado para introducir directamente los elementos (nombres de elemento) en secuencia usando comas para separarlos, pero también se puede usar una interfaz de usuario gráfica de tipo convencional para introducir la información de manera similar. Cuando se usa la interfaz gráfica, el usuario sitúa el cursor sobre los elementos deseados y los selecciona (haciendo clic) y en ese momento se muestran en pantalla estos elementos en el campo de entrada de designación de posición 35 separados por delimitadores. Los elementos seleccionados, por ejemplo, se muestran preferentemente separados visualmente.

Obsérvese que hay un botón de candidato 38 para generar de manera automática la secuencia de elementos que se debe seleccionar. Es decir, cuando el usuario sitúa el cursor sobre el botón de candidato 38 y lo selecciona, por ejemplo, se introduce de forma aleatoria en el campo de entrada de designación de posición 35 una secuencia de elementos registrados previamente y se muestra en pantalla. Esto se debe a que, en el caso de que el usuario establezca el patrón de obtención de contraseña, el usuario tenderá a seleccionar botones contiguos y, al ser fáciles de extrapolar, se deben evitar situaciones de este tipo, y, por tanto, el botón de candidato 38 se proporciona a modo auxiliar.

Después de que el usuario introduzca la información necesaria en los campos de entrada predeterminados, el usuario selecciona un botón de confirmación de configuración 39 y, en ese momento, un navegador web envía al servidor de verificación 12 una solicitud de registro que contiene la información introducida. Basándose en la solicitud de registro recibida, el servidor de verificación 12 registra temporalmente el patrón de obtención de contraseña del usuario como datos de registro y muestra una pantalla de confirmación de configuración en el navegador web.

La pantalla de confirmación de configuración es una pantalla que sirve para que el usuario pueda introducir la contraseña de acuerdo con el patrón de obtención de contraseña establecido por el usuario, con el fin de confirmar el patrón de obtención de contraseña. En la fig. 4 se muestra un ejemplo de la pantalla de confirmación de configuración que se muestra en el ordenador personal 15. No obstante, en lugar de mostrarla en el ordenador personal 15, también es posible mostrar la pantalla de confirmación de configuración en el teléfono móvil 13 del usuario y que el usuario confirme la configuración desde el teléfono móvil 13. En este caso, cuando el usuario desea usar el sistema de destino de uso 11, también es posible confirmar el teléfono móvil 13 utilizado por el usuario.

Como se muestra en la fig. 4, en la pantalla de confirmación de configuración se presenta un patrón presentado 41, en el que se asocian caracteres numéricos aleatorios a cada grupo de elementos del patrón global 34 generado por el servidor de verificación 12. Como contraseña, el usuario introduce en un campo de entrada de contraseña 42 los caracteres numéricos (valores de elemento) del patrón global 34 que se han asociado a los elementos que corresponden al patrón de obtención de contraseña establecido previamente. Después de que el usuario introduzca la contraseña en el campo de entrada de contraseña 42, el usuario selecciona un botón de «Ir» 43, momento en el que el navegador web envía al servidor de verificación 12 la solicitud de verificación que contiene la contraseña introducida. A continuación, el servidor de verificación 12 decide si la contraseña contenida en la solicitud de confirmación recibida coincide con la cadena de caracteres numéricos obtenida a partir del patrón presentado que se ha generado y del patrón de obtención de contraseña que se registró poco antes de manera temporal, y cuando coinciden, registra formalmente el patrón de obtención de contraseña del usuario en la base de datos de verificación 14 como datos de registro.

Obsérvese que, cuando este procedimiento de registro de patrones de obtención de contraseña se lleva a cabo usando el ordenador personal 15, a fin de confirmar el teléfono móvil 13 perteneciente al usuario, el servidor de verificación 12 envía preferentemente un mensaje predeterminado al número de teléfono móvil recibido y se solicita la respuesta del usuario al mensaje.

La fig. 5 es un diagrama que muestra un ejemplo de estructuras de datos de la base de datos de verificación 14. Como se muestra en el diagrama, una entrada de la base de datos de verificación 14 está constituida por un campo de identificador de sistema 51, un campo de cuenta de usuario 52, un campo de identificador de usuario 53, un campo de patrón de obtención de contraseña 54 y un campo de regla de conversión 55. En el presente ejemplo, un usuario, «ogawa», se registra como un usuario que puede utilizar los sistemas de destino de uso 11 indicados por los identificadores de sistema «36578979» y «3657980». Además, al teléfono móvil 13 utilizado por el usuario «ogawa» para la verificación de usuario se le asigna el teléfono móvil 13 indicado por un identificador de usuario «090xxxx1234». Además, al patrón de obtención de contraseña para el usuario «ogawa» que se ha registrado con el sistema de destino de uso 11 indicado por el identificador de sistema «36578979» se le asigna la secuencia «1, 17, 33, 48» y, a la regla de conversión, se le asigna «+1».

A continuación, se ofrece una explicación detallada del flujo de proceso de un procedimiento de verificación de usuario para cuando el usuario intenta trata de utilizar el sistema de destino de uso 11. Cuando el usuario intenta utilizar el sistema de destino de uso 11, para obtener el identificador del sistema, el usuario emplea el sistema de destino de uso 11 para que se muestre en pantalla el identificador del sistema. Por ejemplo, cuando la interfaz de usuario del sistema de destino de uso 11 está provista de un botón de «inicio de uso», en el momento en el que el usuario pulsa el botón de «inicio de uso», el sistema de destino de uso 11 muestra en la interfaz del usuario una pantalla de recepción como la que aparece en la fig. 6 y muestra el identificador del sistema al usuario y solicita al usuario que introduzca el identificador de usuario.

El usuario acciona el teléfono móvil 13, designa una URL que ha sido registrada como un (así denominado) marcador, accede al servidor de verificación 12, se muestra una pantalla de menú como la de la fig. 7 y después selecciona el inicio del procedimiento de verificación, y se muestra una pantalla de inicio del procedimiento de verificación tal como la de la fig. 8. El usuario introduce un identificador de sistema en la pantalla de inicio del procedimiento de verificación y selecciona el botón de «OK». Obsérvese que se puede usar una construcción en la que,

cuando se use un identificador de sistema fijo, como en la presente forma de realización, el identificador de sistema introducido se puede registrar en el teléfono móvil 13.

Por consiguiente, el teléfono móvil 13 envía al servidor de verificación 12 un mensaje de inicio del procedimiento de verificación que contiene el identificador del sistema como parámetro. En ese momento, el teléfono móvil 13 envía al servidor de verificación 12 el identificador de usuario, que constituye un ejemplo de información de identificación para identificar al usuario. El identificador de usuario puede ser información que identifique, por ejemplo, el teléfono móvil o similar perteneciente al usuario o utilizado por él. En la presente forma de realización, el teléfono móvil 13 envía el número de teléfono móvil, que constituye un ejemplo de la información para identificar el teléfono móvil 13, al servidor de verificación 12 como identificador de usuario. El identificador de usuario se puede incluir en el mensaje de inicio del procedimiento de verificación como parámetro, o bien se puede enviar a nivel del sistema.

La fig. 9 y la fig. 14 son diagramas de flujo que explican el flujo del proceso en el servidor de verificación 12 de acuerdo con la presente forma de realización. En los siguientes diagramas de flujo, los flujos del proceso se explican secuencialmente, pero esto no es necesario. Por lo tanto, siempre que no se generen errores de coherencia en las operaciones o efectos de proceso, las secuencias del proceso se pueden dar la vuelta o realizarse en paralelo.

Como se muestra en la figura 9, el servidor de verificación 12 recibe el mensaje de inicio del procedimiento de verificación enviado por el teléfono móvil 13 y después extrae a partir del mismo el identificador del sistema y el identificador de usuario (etapa 901). A continuación, debido a que el servidor de verificación 12 está esperando a la solicitud de verificación de usuario procedente del sistema de destino de uso 11 indicado por el identificador de sistema extraído, el servidor de verificación 12 emite un identificador de evento, registra el identificador de sistema extraído y el identificador de usuario en una tabla de espera de solicitud de verificación de usuario como la que se muestra en la fig. 10 y carga un proceso para ejecutar el proceso que se muestra en la fig. 14 (etapa 902). La tabla de espera de solicitud de verificación de usuario se registra, por ejemplo, en la base de datos de verificación 14.

A continuación, el servidor de verificación 12 invoca una función generatriz de números aleatorios predeterminada, que emite caracteres numéricos aleatorios para generar el patrón presentado (etapa 903). Considerando los riesgos de seguridad, el patrón presentado es preferentemente una tabla de números aleatorios cuyos valores de elemento cambian cada vez que se lleva a cabo la verificación de usuario, pero también se puede usar un patrón presentado con valores de elemento fijos, y, por tanto, no debe ser excluido. Cuando el servidor de verificación 12 genera el patrón presentado, el patrón presentado se registra en la tabla de espera de solicitud de verificación de usuario mencionada anteriormente (etapa 904), y se envía junto con el identificador de usuario al teléfono móvil 13 (etapa 905). En consecuencia, el teléfono móvil 13 muestra una pantalla de visualización de tablas de números aleatorios como la que se muestra en la fig. 11.

Cuando se muestra la pantalla de visualización de tablas de números aleatorios en el teléfono móvil 13, el usuario introduce el identificador de usuario en la pantalla de recepción del sistema de destino de uso 11 que se muestra en la fig. 6. La fig. 12 muestra la pantalla de recepción en un estado en el que se ha introducido el identificador de usuario. Cuando el usuario pulse la tecla Intro, el sistema de destino de uso 11 muestra la pantalla de entrada de contraseña, tal como se observa en la fig. 13. Como respuesta, el usuario introduce la contraseña obtenida a partir del patrón de obtención de contraseña que ya ha sido registrado. Por ejemplo, el patrón de obtención de contraseña del usuario puede ser el patrón de obtención de contraseña que se registró en la pantalla de registro de patrón de obtención de contraseña que se muestra en la fig. 3. En dicho caso, de acuerdo con la pantalla de visualización de tablas de números aleatorios que se muestra en la fig. 11, se obtiene «5910», que después se somete a la aplicación de la regla de conversión «+1», mediante la cual se obtiene «6021». El usuario introduce entonces la contraseña así obtenida y pulsa la tecla Intro, momento en el cual el sistema de destino de uso 11 envía al servidor de verificación 12 como solicitud de verificación la contraseña que se introdujo (en lo sucesivo, «contraseña introducida») junto con su propio identificador de sistema.

La contraseña que se envía al sistema de destino de uso 11 la utiliza el servidor de verificación 12 en la verificación de usuario, de acuerdo con el diagrama de flujo que se muestra en la fig. 14. Es decir, cuando el servidor de verificación 12 que espera la solicitud de verificación de usuario recibe la solicitud de verificación de usuario procedente del sistema de destino de uso 11 (Sí en la etapa 1401), el servidor de verificación 12 consulta la tabla de espera de solicitud de verificación de usuario que se muestra en la fig. 10, y especifica el identificador de usuario (etapa 1402). Debido a que el registro en la tabla de espera de solicitud de verificación de usuario requiere el mensaje de inicio del procedimiento de verificación procedente del teléfono móvil 13, se puede excluir la solicitud de verificación de usuario procedente de un sistema de destino de uso 11 no registrado, por ser ilegítima. Cuando el servidor de verificación 12 identifica el identificador de usuario, el servidor de verificación 12 consulta la base de datos de verificación 14 e identifica el patrón de obtención de contraseña y la regla de conversión para ese identificador de usuario (etapa 1403). Posteriormente, el servidor de verificación 12, basándose en el patrón de obtención de contraseña y la regla de conversión identificados, obtiene la contraseña (en lo sucesivo «contraseña interna del sistema»), a partir del patrón presentado registrado en la tabla de espera de solicitud de verificación de usuario (etapa 1404). Específicamente, para el grupo de elementos que constituye el patrón presentado, el servidor de verificación 12 obtiene los valores de elemento correspondientes a la secuencia de elementos que constituye el patrón de obtención de contraseña, y además, si se ha definido la regla de conversión, aplica la regla de conversión a los valores de elemento y, de este modo, obtiene la contraseña interna del sistema. A continuación, el servidor de verificación 12 decide si la contraseña introducida que fue enviada y la contraseña interna del sistema coinciden o no (etapa 1405). Entonces, cuando se decide que coinciden entre sí, el servidor de verificación 12 notifica el resultado positivo de la verificación al sistema de destino de uso 11 indicado por el identificador del sistema (etapa 1406). Por otra parte, si no coinciden, el servidor de verificación 12 notifica el resultado negativo de la verificación (etapa 1407). El sistema de destino de uso 11 lleva a cabo el proceso basándose en el resultado notificado por el servidor de verificación 12.

Tal como se describe anteriormente, la presente forma de realización proporciona las siguientes ventajas. En concreto, la contraseña que se debe introducir cuando el usuario se dispone a utilizar el sistema de destino de uso 11 se determina temporalmente a partir del patrón presentado que se genera de forma aleatoria cada vez que se lleva a cabo

la verificación de usuario, de acuerdo con el patrón de obtención de contraseña que se ha registrado de antemano. Por lo tanto, aunque la contraseña introducida por el usuario se filtre a un tercero, la propia contraseña carecerá totalmente de sentido la próxima vez que se lleve a cabo la verificación de usuario y, de este modo, se puede evitar de manera eficaz el acceso ilegítimo. En este caso, ya que el usuario no recuerda los «caracteres numéricos específicos» como en la técnica convencional, sino el patrón de obtención de contraseña «conceptual y esquemático» como «contraseña», la contraseña resulta fácil de recordar y difícil de olvidar, con lo cual la gestión de las contraseñas resulta sencilla.

Además, ya que el usuario puede dar la regla de conversión para este patrón de obtención de contraseña, se puede optar a un mayor nivel de seguridad.

Además, el servidor de verificación 12 recibe el mensaje de inicio de procedimiento de verificación procedente del teléfono móvil 13 del usuario, y, de ese modo, recibe la solicitud de verificación de usuario procedente del sistema de destino de uso 11 designado en la misma, y, de ese modo, se puede impedir el acceso ilegítimo desde la unidad del sistema de destino de uso 11.

Obsérvese que la presente forma de realización se construye de tal manera que el sistema de destino de uso 11 muestra la pantalla de recepción (fig. 6) en la interfaz de usuario y pide al usuario que introduzca el identificador de usuario, pero esta construcción no es particularmente necesaria. Por ejemplo, también es posible una construcción en la que el sistema de destino de uso 11 obtenga información de una lista de usuarios capaces de utilizar el servidor de verificación 12 y después la muestre en pantalla al usuario en forma de menú desplegable y le solicite que introduzca la información.

Además, en la presente forma de realización, el identificador del sistema es un identificador de sistema que es exclusivo para el sistema de destino de uso 11 (un identificador de sistema único), pero el identificador de sistema también puede ser un identificador de sistema compartido que sea común a una pluralidad de sistemas de destino de uso 11. Es decir, una pluralidad de sistemas de destino de uso 11 pueden tener el mismo identificador de sistema. Por consiguiente, el sistema de destino de uso 11, en lugar de registrar en la base de datos de verificación 14 que se describe más adelante el identificador de sistema único de un sistema de destino de uso 11 dado, puede usar el identificador compartido para dirigir la solicitud de verificación al servidor de verificación 12, de manera que el sistema de verificación de usuario se pueda usar con facilidad.

En el caso de que el sistema de destino de uso 11 utilice el identificador de sistema compartido para realizar la solicitud de verificación, el servidor de verificación 12 también puede proporcionar a ese sistema de destino de uso 11 un servicio diferente al servicio proporcionado al sistema de destino de uso 11 que posee el identificador de sistema único. De este modo, el servidor de verificación 12 puede enviar información personal del usuario al sistema de destino de uso 11 que utilizó el identificador de sistema único para realizar la solicitud de verificación, a la vez que deja de enviar información personal del usuario al sistema de destino de uso 11 que utilizó el identificador de sistema compartido para realizar la solicitud de verificación, o de otras formas similares puede establecer diferencias entre los servicios proporcionados al sistema de destino de uso 11 que utiliza el identificador de sistema único y al sistema de destino de uso 11 que utiliza el identificador de sistema compartido.

[Segunda forma de realización]

La presente forma de realización es una variación de la primera forma de realización. En lugar del sistema de destino de uso 11, la contraseña se introduce desde el teléfono móvil 13. Además, en la presente forma de realización, en lugar del identificador de sistema fijo, se ofrece una explicación acerca de un ejemplo que utiliza un identificador de uso nuevo que se genera cada vez que se utiliza el sistema de destino de uso 11.

La fig. 15 es un esquema resumen que explica un sistema global del procedimiento de verificación de usuario de acuerdo con la presente forma de realización.

En primer lugar, el usuario utiliza el ordenador personal 15 para registrar de antemano su propio patrón de obtención de contraseña o el sistema de destino de uso 11 en la base de datos de verificación 14 ((1) en el esquema). Cuando el usuario intenta utilizar el sistema de destino de uso 11, para obtener el identificador de usuario, el usuario acciona la interfaz de usuario del sistema de destino de uso 11 para que se muestre el identificador de uso ((2) en el esquema). El sistema de destino de uso 11, por ejemplo, obtiene información del momento en el que se llevaron a cabo las operaciones, para ello da una función de generación de números aleatorios, genera de manera aleatoria el identificador de uso y muestra el identificador en pantalla. En este momento, el sistema de destino de uso 11 envía el identificador de uso generado junto con su propio identificador de sistema al servidor de verificación 12 ((3) en el esquema).

A continuación, el usuario introduce el identificador de uso en el teléfono móvil 13 y lo envía al servidor de verificación 12 ((4) en el esquema). El servidor de verificación 12 recibe el identificador de uso, y después especifica el sistema de destino de uso 11 y también genera una tabla de números aleatorios, que se envía después al teléfono móvil 13 del usuario ((5) en el esquema) como patrón presentado. El usuario consulta el patrón presentado que se presenta en el teléfono móvil 13 e introduce la secuencia de valores de elemento (la cadena de caracteres numéricos) asignados al patrón de obtención de contraseña propio del usuario. De este modo, se envía la contraseña desde el teléfono móvil 13 al servidor de verificación 12 ((6) en el esquema).

El servidor de verificación 12 recibe esta transmisión y compara después la cadena de caracteres numéricos obtenida a partir del patrón de obtención de contraseña del usuario que se había registrado y el patrón presentado generado, y la cadena de caracteres numéricos que se envió desde el teléfono móvil 13, y decide si estas cadenas de caracteres numéricos coinciden entre sí o no. Después, el servidor de verificación 12 notifica el resultado positivo de la verificación si se decide que coinciden, o notifica el resultado negativo de la verificación en caso contrario, al sistema de destino de uso 11 que se especificó ((7) en el esquema). El sistema de destino de uso 11 da su aprobación al acceso por parte del usuario cuando se recibe la notificación del resultado positivo de la verificación procedente del servidor de

verificación 12.

Como se describe anteriormente, la presente forma de realización proporciona ventajas similares a las de la primera forma de realización, y además proporciona las siguientes ventajas. Es decir, ya que no es necesario introducir la contraseña desde el sistema de destino de uso 11, la interfaz de usuario del sistema de destino de uso 11 se puede realizar con una construcción simple. Además, ya que el nuevo identificador de uso se crea cada vez que se usa el sistema de destino de uso 11, aunque se filtre el identificador de uso, no supondrá problema alguno, lo cual permite optar a un mayor nivel de seguridad.

[Tercera forma de realización]

La presente forma de realización se refiere a un procedimiento de registro de patrón de obtención de contraseña mediante el uso del teléfono móvil 13, en el que el servidor de verificación 12 presenta un candidato a patrón de obtención de contraseña en el teléfono móvil 13, y el usuario selecciona entre los candidatos a patrón de obtención de contraseña presentados.

La fig. 16 muestra un ejemplo de pantalla de registro de patrón de obtención de contraseña que se muestra en el teléfono móvil 13. De forma similar a las formas de realización mencionadas anteriormente, por ejemplo en el momento en el que se registra la cuenta de usuario para el sistema de destino de uso 11, el servidor de verificación 12 usa un correo electrónico para enviar al teléfono móvil 13 del usuario un correo que contenga una URL de datos de página que constituyen esta pantalla de registro. Después de haber recibido esta transmisión, el usuario selecciona la URL contenida en el correo y mostrada en la pantalla del teléfono móvil 13, por lo que la pantalla de registro se proporciona al teléfono móvil 13 del usuario.

Es decir, cuando el servidor de verificación 12 recibe una solicitud de registro de patrón de obtención de contraseña desde el teléfono móvil 13 del usuario, el servidor de verificación 12 selecciona un patrón de obtención de contraseña como candidato de registro entre un grupo de patrones de obtención de contraseña que han sido registrados previamente, y después lo envía al teléfono móvil 13. Por consiguiente, la pantalla de registro que contiene el candidato a patrón de obtención de contraseña, como se muestra en la fig. 16A, se presenta en el teléfono móvil 13 del usuario. Cuando el usuario desee registrar el candidato a patrón de obtención de contraseña que se muestra en la pantalla de registro como su propio patrón de obtención de contraseña, el usuario selecciona un botón de «Registro» 161. Por otra parte, cuando el usuario desee ver otro candidato a patrón de obtención de contraseña, el usuario seleccionará un botón de «Siguiente» 162. Cuando el usuario selecciona el botón de «Siguiente» 162, el servidor de verificación 12 envía otro candidato al teléfono móvil 13 y se presenta en el teléfono móvil 13 otra pantalla de registro que contiene el otro patrón de obtención de contraseña, como se muestra en la fig. 16B. Si existe un candidato previo a patrón de obtención de contraseña, cuando el usuario desee visualizarlo, seleccionará un botón de «Atrás» 163.

Por ejemplo, en la pantalla de registro que se muestra en la fig. 16B, cuando el usuario selecciona el botón de «Registro» 161, el teléfono móvil 13 envía la solicitud de registro al servidor de verificación 12. El servidor de verificación 12, basándose en la solicitud de registro recibida, registra temporalmente el patrón de obtención de contraseña del usuario en la base de datos de verificación 14 a modo de datos de registro y envía la pantalla de confirmación de configuración al teléfono móvil 13. La fig. 17 es un esquema que muestra un ejemplo de la pantalla de confirmación de configuración en este momento. En un campo de entrada de contraseña 171 de la pantalla de confirmación de configuración, el usuario introduce los caracteres numéricos (valores de elemento) que han sido asignados a los elementos correspondientes al patrón de obtención de contraseña que se estableció, y después selecciona un botón de «OK» 172. Al hacerlo, el teléfono móvil 13 envía al servidor de verificación 12 una solicitud de confirmación que contiene la contraseña introducida. El servidor de verificación 12 decide entonces si la contraseña contenida en la solicitud de confirmación recibida coincide o no con la cadena de caracteres numéricos que se obtiene a partir del patrón presentado generado y el patrón de obtención de contraseña que se ha registrado temporalmente. Cuando la contraseña coincide, el patrón de obtención de contraseña del usuario se registra formalmente en la base de datos de verificación 14 a modo de datos de registro, y se envía al teléfono móvil 13 una indicación de que el registro ha concluido.

Como se describe anteriormente, de acuerdo con la presente forma de realización, debido a que el patrón de obtención de contraseña deseado se selecciona entre los candidatos a patrón de obtención de contraseña presentados por el servidor de verificación 12, aunque la interfaz de usuario resulte insuficiente, como cuando se usa el teléfono móvil 13, el patrón de obtención de contraseña se puede registrar con una enorme facilidad. Además, como el servidor de verificación 12 muestra en pantalla el patrón de obtención de contraseña, es posible evitar la situación en la que el usuario registra como su patrón de obtención de contraseña un patrón de obtención de contraseña que se puede extrapolar fácilmente, como cuando se seleccionan elementos contiguos.

[Cuarta forma de realización]

La presente forma de realización se refiere a un procedimiento de registro de patrón de obtención de contraseña usando el teléfono móvil 13, en el que se repiten las entradas de los valores de elemento correspondientes al patrón de obtención de contraseña previsto por el usuario, con lo cual se especifica el patrón de obtención de contraseña.

La fig. 18 es un diagrama de flujo que explica el flujo de proceso del procedimiento de registro del patrón de obtención de contraseña de acuerdo con la presente forma de realización. Este proceso se logra mediante unos programas correspondientes en un modelo cliente/servidor usando el teléfono móvil 13 y el servidor de verificación 12. En la presente forma de realización, se envían datos que contienen un programa específico para lograr este tipo de proceso desde el servidor de verificación 12 al teléfono móvil 13, y este programa se ejecuta en el teléfono móvil 13 para llevar a cabo la invención.

De forma similar a las formas de realización mencionadas anteriormente, por ejemplo en el momento en el que

se registra la cuenta de usuario para el sistema de destino de uso 11, el servidor de verificación 12 usa el correo electrónico para enviar al teléfono móvil 13 del usuario un correo que contiene una URL de datos de página que constituyen la pantalla de registro. Tras haber recibido esta transmisión, el usuario selecciona la URL entre el contenido del correo que se muestra en el teléfono móvil 13. En consecuencia, el servidor de verificación 12 envía al teléfono móvil 13 datos de página que contienen el programa predeterminado.

Tras haber recibido los datos de página, el teléfono móvil 13 interpreta los datos de página, ejecuta el proceso que se muestra en la fig. 18 de acuerdo con el programa predeterminado que contienen y muestra la pantalla de registro. Es decir, el teléfono móvil 13, en primer lugar, para el grupo de elementos de la totalidad del patrón 34, asigna números aleatorios generados usando la función de generación de números aleatorios para generar el patrón presentado, y lo muestra en pantalla como un patrón de obtención de contraseña combinado con otros elementos de pantalla, y pide al usuario que introduzca la información (etapa 1801). En la pantalla de registro, el usuario introduce caracteres numéricos asignados a los elementos del patrón de obtención de contraseña que el usuario está tratando de registrar. Cuando el teléfono móvil 13 recibe del usuario la secuencia de elementos (etapa 1802), los elementos que poseen los valores de elemento introducidos se extraen del patrón presentado, a modo de valores de elemento, y se mantiene su cantidad (etapa 1803). A continuación, el teléfono móvil 13 decide si el número de elementos extraídos y el número de elementos introducidos es el mismo o no (etapa 1804). Si se decide que no son el mismo, para reducir la lista de elementos, los números aleatorios se asignan únicamente a los elementos extraídos del patrón global 34 para generar el patrón presentado y, de forma similar, este patrón presentado se presenta como pantalla de registro y se pide al usuario que introduzca información (etapa 1805). Por otra parte, cuando se decide que el número de elementos extraídos y el número de elementos introducidos son iguales, se considera que se ha reducido la lista de elementos, de manera que el teléfono móvil muestra una pantalla de confirmación de registro y pide al usuario su confirmación (etapa 1806). Entonces, cuando el usuario pulsa un botón de «OK», por ejemplo (Sí en la etapa 1806), el teléfono móvil 13, para registrar la secuencia de elementos como patrón de obtención de contraseña, envía una solicitud de registro al servidor de verificación 12 (etapa 1806), con lo cual concluye el proceso.

De este modo, al repetir la introducción de valores de elemento correspondientes al patrón de obtención de contraseña que el usuario desea registrar, se reduce el número de elementos del patrón presentado y se concreta el patrón de obtención de contraseña previsto por el usuario.

La fig. 19 y la fig. 20 son ejemplos de pantallas que explican el procedimiento de registro del patrón de obtención de contraseña. En primer lugar, se supone que la pantalla que aparece en la fig. 19A se muestra en el teléfono móvil 13. Aquí, cuando el usuario introduce «9893» en la pantalla, el teléfono móvil 13 genera un nuevo patrón presentado basándose en la secuencia de elementos introducidos. Es decir, el teléfono móvil 13 extrae los elementos cuyos valores eran «9», «8» o «3» de los elementos del anterior patrón presentado, como elementos dados. No obstante, en este caso, el número de los elementos extraídos dados no se ha reducido hasta llegar al número de elementos introducidos, de forma que el teléfono móvil 13 genera el nuevo patrón presentado con los números aleatorios asignados a los elementos extraídos y muestra una pantalla de registro como la que aparece en la fig. 19B.

En esta pantalla, el usuario vuelve a introducir los caracteres numéricos aleatorios para los elementos del patrón de obtención de contraseña que el usuario esté intentando registrar, y de este modo lleva a cabo la tarea de reducir el número de elementos extraídos. En este caso, los caracteres numéricos que debe introducir el usuario son «6541». Si el número de elementos extraídos dados no se puede reducir, el teléfono móvil 13 generará un nuevo patrón de obtención de contraseña y después mostrará una pantalla de registro como la que aparece en la fig. 19C y solicitará al usuario que introduzca información. Aquí, en esta pantalla, el usuario introduce los caracteres numéricos «8501» que han sido asignados a los elementos del patrón de obtención de contraseña que el usuario está intentando registrar.

Debido a que estas entradas reducen el número de elementos extraídos, el teléfono móvil 13 muestra una pantalla de confirmación de registro como la que aparece en la fig. 20 y solicita al usuario su confirmación (etapa 1806). Cuando el usuario selecciona un botón de «OK» 201 en esta pantalla, el teléfono móvil 13 envía la secuencia de elementos al servidor de verificación 12 a modo de patrón de obtención de contraseña. Por otra parte, cuando el usuario selecciona un botón de «Rehacer» 202, el teléfono móvil 13 vuelve a efectuar el proceso de registro del patrón de obtención de contraseña desde el principio.

Como se describe anteriormente, de acuerdo con la presente forma de realización, la presentación del patrón presentado y la introducción de los valores de elemento correspondientes al patrón de obtención de contraseña que el usuario está intentando registrar se repiten para reducir el número de elementos del patrón presentado. Así, se puede concretar el patrón de obtención de contraseña previsto por el usuario. Por lo tanto, incluso en el caso de que la interfaz de usuario sea insuficiente, como en el caso del teléfono móvil 13, el patrón de obtención de contraseña se puede registrar de forma extremadamente sencilla.

Además, en la presente forma de realización, las operaciones para registrar el patrón de obtención de contraseña se llevan a cabo en la misma secuencia que las operaciones de entrada de la auténtica contraseña, de manera que el usuario también pueda practicar cómo introducir la información y pueda aprenderse rápidamente el patrón de obtención de contraseña sin fallos.

Obsérvese que, en la presente invención, el patrón presentado se genera de forma aleatoria para reducir el número de elementos previstos por el usuario. Así, dependiendo de la combinación de patrones presentados que se generan, existen casos en los que la tarea de reducción requiere tres aplicaciones o más. Para evitar esta situación, también es posible usar una combinación fija de patrones presentados mediante la cual la tarea de reducción quedará concluida con dos aplicaciones.

[Quinta forma de realización]

En la presente forma de realización, en lugar del identificador de usuario fijo para la verificación de usuario, se genera información de identificación temporal para identificar temporalmente al usuario.

La fig. 21 es un diagrama resumen que explica un esquema global de un procedimiento de verificación de usuario de acuerdo con la presente forma de realización. En primer lugar, el usuario utiliza el ordenador personal 15 para registrar de antemano su propio patrón de obtención de contraseña para el sistema de destino de uso 11 en la base de datos de verificación 14 ((1) en el diagrama). Cuando el usuario se dispone a usar el sistema de destino de uso 11, con el fin de obtener el identificador de sistema, el usuario emplea la interfaz de usuario del sistema de destino de uso 11 para mostrar en pantalla el identificador del sistema ((2) en el diagrama).

A continuación, el usuario introduce el identificador de sistema en el teléfono móvil 13 y lo envía al servidor de verificación 12 ((3) en el diagrama). El servidor de verificación 12 recibe la transmisión, genera la tabla de números aleatorios (que, en la presente forma de realización, es una información numérica aleatoria en forma de matriz de 4 filas por 4 columnas o de 4 filas por 12 columnas) y envía esta tabla al teléfono móvil 13 del usuario a modo de patrón presentado, y también genera información temporal que sirve para identificar temporalmente al usuario y está asociada al identificador de usuario, y envía esta información al teléfono móvil 13 ((4) en el diagrama) del usuario. El usuario consulta la información temporal y el patrón presentado que se presentan en el teléfono móvil 13 e introduce en el sistema de destino de uso 11 la información temporal y, como contraseña, la secuencia de elementos (cadena de caracteres numéricos) que ha sido asignada al patrón de obtención de contraseña del propio usuario. En consecuencia, el sistema de destino de uso 11 envía la información temporal y la contraseña al servidor de verificación 12 ((5) en el diagrama.

El servidor de verificación 12 recibe la información temporal y la contraseña enviada por el sistema de destino de uso 11 y después identifica al usuario a partir de la información temporal y compara la cadena de caracteres numéricos obtenida a partir del patrón de obtención de contraseña de usuario que ya ha sido registrado y el patrón presentado generado, y la contraseña enviada por el sistema de destino de uso 11 para decidir si coinciden. Entonces, el servidor de verificación 12 notifica el resultado positivo de la verificación y la información de identificación de usuario por cada sistema, que se describe más adelante, cuando se decide que coinciden, y notifica el resultado negativo de la verificación cuando se decide que no coinciden, al sistema de destino de uso 11 indicado por el identificador de sistema ((6) en el diagrama). El sistema de destino de uso 11 da su aprobación para el uso de ese sistema de destino de uso 11 a dicho usuario cuando se recibe la notificación del resultado positivo de la verificación procedente del servidor de verificación 12.

La fig. 22 es un diagrama que muestra un ejemplo de estructuras de datos de la base de datos de verificación 14. Como se muestra en la fig. 22, una entrada de la base de datos de verificación 14 incluye un campo de identificador de sistema 51, un campo de cuenta de usuario 52, un campo de identificador de usuario 53, un campo de patrón de obtención de contraseña 54, un campo de información de identificación temporal 56 y un campo de información de identificación de usuario por cada sistema 57. En el presente ejemplo, un usuario «ogawa» se registra como un usuario que puede utilizar los sistemas de destino de uso 11 indicados por los identificadores de sistema «36578979», «3657980» y «36578981». Además, se establece que el teléfono móvil 13 que utiliza el usuario «ogawa» para la verificación de usuario corresponda al teléfono móvil 13 indicado por un identificador de usuario «090xxxx1234». Además, se establece que el patrón de obtención de contraseña para el usuario «ogawa» que se ha registrado con el sistema de destino de uso 11 indicado por el identificador de sistema «36578979» corresponda a «1, 17, 33, 48».

La fig. 23 es un diagrama que muestra un ejemplo de una tabla de espera de solicitud de verificación de usuario (compárese con la primera forma de realización). En la presente forma de realización, la tabla de espera de solicitud de verificación de usuario incluye un campo de identificador de evento 100, un campo de identificador de sistema 101, un campo de identificador de usuario 102, un campo de patrón presentado 103 y un campo de información de identificación temporal 104.

Las figs. 24 a 26 son diagramas de flujo que explican el flujo del proceso en el servidor de verificación 12 de acuerdo con la presente forma de realización. En los siguientes diagramas de flujo, los flujos de proceso se explican secuencialmente, pero no se establecen restricciones en este flujo de proceso. Por lo tanto, el flujo de proceso se puede construir con las secuencias de proceso cambiadas de orden o realizadas en paralelo.

Como se muestra en la fig. 24, el servidor de verificación 12 recibe el mensaje de inicio del procedimiento de verificación enviado por el teléfono móvil 13 y después extrae de ahí el identificador de sistema y el identificador de usuario (etapa 2000). A continuación, ya que el servidor de verificación 12 está esperando a la solicitud de verificación de usuario procedente del sistema de destino de uso 11 indicado por el identificador de sistema extraído, el servidor de verificación 12 emite un identificador de evento y registra el identificador de sistema extraído y el identificador de usuario en una tabla de espera de solicitud de verificación de usuario como la que se muestra en la fig. 23.

A continuación, el servidor de verificación 12 decide si la información de identificación temporal es necesaria o no para que el usuario utilice el sistema de destino de uso 11 (etapa 2002). El servidor de verificación 12 decide preferentemente si genera o no la información de identificación temporal basándose en una solicitud del usuario. Por ejemplo, el servidor de verificación 12 puede notificar el teléfono móvil 13 del usuario a fin de solicitar información acerca de si el usuario utilizará o no la información de identificación temporal en el sistema de destino de uso 11. Después, el servidor de verificación 12 decide si genera o no la información de identificación temporal basándose en la información recibida a través del teléfono móvil 13 procedente del usuario.

Además, el servidor de verificación 12 puede registrar de antemano información que muestre si la información de identificación temporal será utilizada o no para el sistema de destino de uso 11 que utilizará el usuario. En dicho caso, el servidor de verificación 12 decide si genera o no la información de identificación temporal basándose en la información registrada de antemano, el identificador de sistema y el identificador de usuario. La información que muestra si la información de identificación temporal será utilizada o no se puede registrar previamente, por ejemplo, cuando se registra el usuario o en cualquier momento posterior al registro del usuario.

En el caso de que el servidor de verificación 12 decida que la información de identificación temporal no es necesaria para el sistema de destino de uso 11 («No» en la etapa 2002), el servidor de verificación 12 invocará una

función de generación de números aleatorios predeterminada, y genera números aleatorios para generar el patrón presentado (etapa 2012). Cuando el servidor de verificación 12 genera el patrón presentado, el patrón presentado se registra en la tabla de espera de solicitud de verificación de usuario que se describe anteriormente (etapa 2014). A continuación, el servidor de verificación 12 envía el patrón presentado al teléfono móvil 13 del usuario (etapa 2018).

Cuando el servidor de verificación 12 decide que la información temporal es necesaria para el sistema de destino de uso 11 («Sí» en la etapa 2002), el servidor de verificación 12 decide entonces si la información de identificación temporal está ya registrada o no para el sistema de destino de uso 11 (etapa 2004). Entonces, cuando el servidor de verificación 12 decide que la información de identificación temporal no ha sido registrada («No» en la etapa 2004), se genera una nueva información de identificación temporal (etapa 2010). La información de identificación temporal es preferentemente información generada, por ejemplo, mediante una función de números aleatorios, que no tiene relación alguna con el identificador de usuario.

Cuando el servidor de verificación 12 decide que la información de identificación temporal ya ha sido registrada («Sí» en la etapa 2004), basándose en factores como la cantidad de tiempo transcurrido desde que se generó la información de identificación temporal y el número de veces que se ha recibido la información de identificación temporal en el servidor 12, el servidor de verificación 12 decide si la información de identificación temporal es válida o no (etapa 2006). Entonces, cuando el servidor de verificación 12 decide que la información de identificación temporal no es válida («No» en la etapa 2006), se elimina la información de identificación temporal (etapa 2008) y se genera una nueva información de identificación temporal (etapa 2010). Entonces, el servidor de verificación 12 registra en la base de datos de verificación 14 y en la tabla de espera de solicitud de verificación la nueva información de identificación temporal generada (etapa 2011). En la presente forma de realización, el servidor de verificación 12 genera «6584» como información de identificación temporal correspondiente al identificador de usuario «090xxxx1234» y la registra en la base de datos de verificación 14 y la tabla de espera de solicitud de verificación (véanse las figs. 22 y 23).

A continuación, el servidor de verificación 12 invoca la función predeterminada de generación de números aleatorios y genera caracteres numéricos aleatorios para generar el patrón presentado (etapa 2012). Cuando el servidor de verificación 12 genera el patrón presentado, el servidor de verificación 12 registra el patrón presentado en la tabla de espera de solicitud de verificación de usuario (etapa 2014). Entonces, el servidor de verificación 12 envía la información de identificación temporal y el patrón presentado al teléfono móvil 13 del usuario (etapa 2016). Cuando la información de identificación temporal y el patrón presentado se envían al teléfono móvil 13, el servidor de verificación 12 espera la solicitud de verificación de usuario procedente del sistema de destino de uso 11.

En la presente forma de realización, el servidor de verificación 12 responde al mensaje de inicio de verificación procedente del usuario determinando la validez de de la información de identificación temporal que ya se ha registrado, basándose en factores tales como la duración del periodo transcurrido desde que se generó la información de identificación temporal y el número de veces que la información de identificación temporal ha sido recibida en el servidor 12, pero el servidor de verificación 12 también puede determinar la validez de la información de identificación temporal independientemente del flujo de proceso que se explica en los presentes diagramas.

Como se muestra en la fig. 25, cuando el servidor de verificación 12 que está esperando la solicitud de verificación de usuario recibe la solicitud de verificación de usuario procedente del sistema de destino de uso 11 («Sí» en la etapa 2100), el servidor de verificación 12 usa la información de identificación temporal y el identificador del sistema para consultar la tabla de espera de solicitud de verificación de usuario que se muestra en la fig. 23 e identifica el identificador de usuario (etapa 2102). Tras haber identificado el identificador de usuario, el servidor de verificación 12 consulta la base de datos de verificación 14 y, basándose en el patrón de obtención de contraseña para ese identificador de usuario, obtiene la contraseña interna del sistema a partir del patrón presentado (etapa 2104). En este caso, el servidor de verificación 12 puede utilizar una regla de conversión predeterminada, al igual que en la primera forma de realización, para obtener la contraseña interna del sistema a partir del patrón presentado.

A continuación, el servidor de verificación 12 decide si la contraseña introducida que se envió y la contraseña interna del sistema coinciden entre sí o no (etapa 2106). Entonces, en el caso de que el servidor de verificación 12 decida que las dos contraseñas coinciden, el servidor de verificación 12 notifica el resultado positivo de la verificación al sistema de destino de uso 11 indicado por el identificador de sistema (etapa 2108), pero si las dos contraseñas no coinciden entre sí, se notifica el resultado negativo de la verificación (etapa 2110). El sistema de destino de uso 11 lleva a cabo entonces un proceso que depende del resultado de la verificación notificado desde el servidor de verificación 12.

En la presente forma de realización, debido a que se utiliza la información de identificación temporal en lugar del identificador de usuario, aunque el identificador incluya, por ejemplo, el número de teléfono móvil u otra información similar que pudiera identificar al usuario, se puede establecer el proceso de la verificación de usuario sin que esta información se filtre al sistema de destino de uso 11. Por consiguiente, aunque se utilice el sistema de destino de uso 11 para un cuestionario o similar en el que no sea necesario identificar al usuario, o cuando no se desea revelar información personal, se puede garantizar el anonimato y se puede usar el sistema con total tranquilidad.

La fig. 26 es un diagrama de flujo que muestra el proceso en el que el servidor de verificación 12 envía la información de identificación de usuario para cada sistema al sistema de destino de uso 11. Cuando el usuario introduce la información de identificación temporal en el sistema de destino de uso 11 y el sistema de destino de uso 11 aprueba el uso por parte de dicho usuario, el servidor de verificación 12 envía al sistema de destino de uso 11 la información de identificación de usuario para cada sistema que corresponde al identificador de usuario y el sistema de destino de uso 11 (identificador de sistema). En este caso, la información de identificación de usuario para cada sistema es preferentemente información fija que distingue a cada uno de los usuarios para cada sistema de destino 11.

El servidor de verificación 12 recibe la solicitud de información de identificación de usuario por cada sistema procedente del sistema de destino de uso 11 (etapa 2200). Entonces, cuando la solicitud de información de identificación de usuario por sistema ha sido recibida procedente del sistema de destino de uso 11 («Sí» en la etapa 2200), el servidor de verificación 12 confirma si la información de identificación de usuario por sistema para el sistema

de destino de uso 11 se ha registrado en la base de datos de verificación 14 (etapa 2202). Entonces, en el caso de que la información de identificación de usuario por sistema no haya sido registrada aún en la base de datos de verificación 14, el servidor de verificación 12 genera la información de identificación de usuario por sistema para el sistema de destino de uso 11 (etapa 2204) y la registra en la base de datos de verificación 14 (etapa 2206). En la presente forma de realización, el servidor de verificación 12 genera «125897» como información de identificación de usuario por sistema para el sistema de destino de uso 11 (identificador de sistema «36578980») del usuario (identificador de usuario «090xxx12345»), y registra esta información en la base de datos de verificación 14. Obsérvese que, para los identificadores de sistema «36578979» y «36578981», se ha registrado la información de identificación de usuario por sistema «125896» y «125898» en la base de datos de verificación 14.

A continuación, el servidor de verificación 12 envía la información de identificación de usuario por sistema al sistema de destino de uso 11 (etapa 2208). En este caso, cuando el servidor de verificación 12 posee la frecuencia de uso del sistema de destino de uso 11 del usuario, que constituye información del usuario para el sistema de destino de uso 11, el servidor de verificación 12 también puede enviar esta información. Además, en la presente forma de realización, el servidor de verificación 12 envía la información de identificación de usuario por sistema al sistema de destino de uso 11, pero, en lugar de ello, también es posible enviar la información de identificación temporal a modo de información de identificación de usuario por sistema al sistema de destino de uso 11.

En la presente forma de realización, el servidor de verificación 12 proporciona la información de identificación de usuario por sistema al sistema de destino de uso 11, con lo cual el sistema de destino de uso 11 puede especificar el usuario que utilice el sistema de destino de uso 11. Es decir, incluso en el caso de que el usuario utilice la información de identificación temporal, el sistema de destino de uso 11 puede determinar la identidad del usuario. Por consiguiente, el sistema de destino de uso 11 puede disponer de información tal como la referida a si ese usuario es un usuario que había utilizado previamente el sistema de destino de uso 11, o similar. Es decir, el sistema de destino de uso 11 puede utilizar la información de identificación de usuario por sistema para construir los datos para la información de usuario en el sistema de destino de uso 11, para prestar un servicio adaptado a cada usuario.

La fig. 27 es un diagrama de flujo que muestra el proceso (S2204 en la fig. 26) para generar la información de identificación de usuario por sistema. En primer lugar, el servidor de verificación 12 genera la tabla de conversión de números aleatorios (etapa 2300). La tabla de conversión de números aleatorios se genera preferentemente de acuerdo con las letras, números u otros caracteres numéricos incluidos en la información de identificación de usuario por sistema que se generó. Por ejemplo, en un caso en el que la información de identificación de usuario por sistema está constituida por una cadena de caracteres numéricos de M dígitos (siendo M un número natural), la tabla de conversión de números aleatorios puede ser una tabla de conversión de números aleatorios para realizar una conversión 1 a 1 de la cadena de caracteres numéricos de M dígitos en una cadena de caracteres numéricos (de números aleatorios) de M dígitos que sea diferente. En otras palabras, se trata de una tabla de números aleatorios para convertir cada cadena de caracteres numéricos de M dígitos (cuyo número es M-plex) en una cadena de caracteres numéricos de M dígitos diferente (cuyo número es M-plex). En la presente forma de realización, la información de identificación de usuario por sistema que se genera está constituida por una cadena de caracteres numéricos de 6 dígitos, y por tanto, se genera una tabla de números aleatorios que posee 1 000 000 de patrones de conversión 1 a 1. El servidor 12 utiliza preferentemente la misma tabla de números aleatorios para cada usuario. Es decir, en el caso de que ya se haya generado la tabla de números aleatorios, se puede omitir la presente etapa.

La información de identificación de usuario por sistema también puede estar constituida por una cadena de caracteres numéricos que tenga el mismo número de dígitos que el identificador de usuario, o puede estar constituida por un número diferente de dígitos. Además, la tabla de conversión de números aleatorios se registra preferentemente en la base de datos de verificación 14.

A continuación, el servidor de verificación 12 genera el identificador de identificación interna por usuario para identificar al usuario dentro del servidor de verificación 12. El identificador de identificación interna por usuario, preferentemente, no se notifica al usuario y el sistema de destino de uso 11. En la presente forma de realización, el identificador de identificación interna por usuario es una cadena de caracteres numéricos que posee el mismo número de dígitos que el identificador de usuario, pero también puede ser una cadena de caracteres numéricos que tenga un número de dígitos diferente al del identificador de usuario. El identificador de identificación interna por usuario se registra preferentemente en la base de datos de verificación 14.

A continuación, el servidor de verificación 12 genera una tabla de conversión por sistema para cada sistema de destino de uso 11 (etapa 2304). Las tablas de conversión por sistema, preferentemente, no se notifican a los sistemas de destino de uso 11. La tabla de conversión por sistema puede ser una tabla de conversión numérica que convierte números predeterminados incluidos en una cadena de caracteres numéricos predeterminada en otros números, o puede ser una tabla de conversión de la posición de los dígitos que cambie un número predeterminado de dígitos de los números por otro número predeterminado de dígitos de los números en una cadena de caracteres numéricos que tenga un número predeterminado de dígitos, o puede ser una tabla de conversión de número de dígitos que cambie el número de dígitos de la cadena de caracteres numéricos borrando un número de dígitos predeterminado de los números o insertando un número predeterminado de números en una cadena de caracteres numéricos que tenga un número de dígitos predeterminado. En este caso, la conversión se lleva a cabo, preferentemente, de tal modo que, al menos dentro del mismo sistema de destino de uso 11, no exista superposición en los resultados producidos al convertir el número de dígitos. La tabla de conversión por sistema se registra preferentemente en la tabla de conversión.

A continuación, el servidor de verificación 12 genera, para cada sistema de destino de uso 11, un identificador de identificación interna por sistema para identificar el sistema de destino de uso 11 dentro del servidor de verificación 12 (etapa 2306). El identificador de identificación interna por sistema, preferentemente, no se notifica al usuario y al sistema de destino de uso 11. En la presente forma de realización, el identificador de identificación interna por sistema es una cadena de caracteres numéricos que posee el mismo número de dígitos que el identificador de usuario, pero también puede ser una cadena de caracteres numéricos que posea un número de dígitos diferente al del identificador de usuario. El identificador de identificación interna por sistema se registra preferentemente en la base de datos de

verificación 14.

A continuación, el servidor de verificación 12 suma el identificador de identificación interna por sistema al identificador de identificación interna por usuario (etapa 2308). Al sumar el identificador de identificación interna generado para cada usuario al identificador de identificación interna generado para cada sistema de destino de uso 11, se puede elevar el nivel de seguridad. En el caso de que al sumar la cifra en un dígito predeterminado al identificador de identificación interna por sistema aumente el número de caracteres en los dígitos predeterminados, el servidor de verificación 12 puede llevar a cabo el proceso para borrar los caracteres en los dígitos que se han incrementado, de manera que el número de dígitos o caracteres después de la suma supere el número de dígitos en el identificador de identificación interna por usuario y el identificador de identificación interna por sistema. Además, el servidor de verificación 12 puede sumar el identificador de identificación interna por usuario y el identificador de identificación interna por sistema, con el fin de calcular una cadena de caracteres numéricos que tenga un número diferente de dígitos que el identificador de identificación interna por usuario y/o el identificador de identificación interna por sistema. El servidor de verificación 12 también puede realizar cálculos del identificador de identificación interna por usuario y el identificador de identificación interna por sistema mediante restas, multiplicaciones, divisiones u otros procedimientos tradicionales.

A continuación, el servidor de verificación 12 utiliza la tabla de conversión por sistema mencionada anteriormente para convertir el resultado del cálculo obtenido en la etapa 2308 (etapa 2310). En la presente forma de realización, el servidor de verificación 12 convierte el resultado de la suma obtenido en la etapa 2308, mediante el uso de la tabla de conversión de posición de dígitos. Entonces, el servidor de verificación 12 utiliza la tabla de conversión de número de dígitos para convertir el resultado de la suma producido por la conversión de las posiciones de los dígitos, en la cadena de caracteres numéricos de 6 dígitos, que es el número de dígitos contenidos en la tabla de conversión de números aleatorios.

A continuación, el servidor de verificación 12 utiliza la tabla de conversión de números aleatorios mencionada anteriormente para convertir el resultado de la conversión producida en la etapa 2310 (etapa 2312). En la presente forma de realización, el servidor de verificación 12 convierte el resultado de la conversión obtenido en la etapa 2310 en una cadena de caracteres numéricos de 6 dígitos (de números aleatorios), que es el mismo número de dígitos que el del resultado de la conversión. Mediante la utilización de la tabla de conversión de números aleatorios para llevar a cabo la conversión, resulta difícil analizar el resultado de la conversión, lo cual permite elevar el nivel de seguridad.

A continuación, el servidor de verificación 12 utiliza la tabla de conversión por sistema mencionada anteriormente para volver a convertir el resultado de la conversión producida en la etapa 2312 (etapa 2314). En la presente forma de realización, el servidor de verificación 12 convierte el resultado de la conversión obtenido en la etapa 2312 por medio de la tabla de conversión numérica, y de este modo obtiene la información de identificación de usuario por sistema. Por consiguiente, el nivel de seguridad se puede aumentar aún más.

En la presente forma de realización, para cada usuario, y para cada sistema de destino de uso 11, se prepara un identificador de identificación interna y una tabla de conversión diferentes, y debido a que las conversiones se realizan basándose en ellos, el nivel de seguridad se puede aumentar aún más. En particular, en la presente forma de realización, las conversiones se llevan a cabo basándose en la tabla de conversión de números aleatorios, de manera que resulta extremadamente difícil usar el resultado de la conversión para obtener la información de lo que había antes de la conversión. Es decir, a partir del resultado de la conversión es extremadamente difícil identificar la información personal del usuario, y por tanto, el nivel de seguridad se puede aumentar más todavía. Además, debido a esto, para cada sistema de destino de uso 11, se puede generar diferente información de identificación de usuario por sistema. Además, para usuarios predeterminados, la información de identificación (la información de identificación de usuario por sistema) se genera para cada sistema de destino de uso 11, por lo que, en una pluralidad de sistemas de destino de uso 11, es posible evitar que se use información enviada desde el servidor de verificación 12, comparar la información del usuario o similar, con lo que evita el compartir información entre sistemas de destino de uso 11.

[Sexta forma de realización]

La presente forma de realización se refiere a un procedimiento para verificar la contraseña introducida desde el sistema de destino de uso 11. A continuación, se ofrece una explicación referente al procedimiento de verificación de contraseñas de acuerdo con la presente forma de realización, usando un ejemplo en el que la contraseña introducida en el sistema de destino de uso 11 coincide con una cadena de caracteres numéricos que contiene un carácter numérico predeterminado, en un dígito predeterminado de la contraseña interna del sistema.

La fig. 28 es un diagrama de flujo que muestra un procedimiento de verificación de contraseña. En primer lugar, el servidor de verificación 12 recibe la contraseña introducida desde el sistema de destino de uso 11 («Sí» en la etapa 2400), y después compara la contraseña introducida y la contraseña interna del sistema (etapa 2402). Cuando la contraseña introducida y la contraseña interna del sistema coinciden («Sí» en la etapa 2404), el servidor de verificación 12 notifica al sistema de destino de uso 11 que la verificación ha sido satisfactoria (etapa 2406).

Cuando la contraseña introducida y la contraseña interna del sistema no coinciden («No» en la etapa 2404), el servidor de verificación 12 compara la contraseña introducida y la contraseña interna del sistema (etapa 2408). En la presente forma de realización, el servidor de verificación 12 compara el número de dígitos de la contraseña introducida y el número de dígitos de la contraseña interna del sistema (etapa 2410). Entonces, cuando el número de dígitos de la contraseña introducida y el número de dígitos de la contraseña interna del sistema no coinciden («No» en la etapa 2410), el servidor de verificación 12 notifica al sistema de destino de uso 11 que la verificación ha arrojado un resultado negativo (etapa 2412).

La contraseña dada como ejemplo en la presente forma de realización es «45871», y la contraseña interna del sistema es «4587». Es decir, el servidor de verificación 12 determina que la contraseña introducida y la contraseña interna del sistema no coinciden, y también determina que poseen un número de dígitos diferente, respectivamente.

Cuando el número de dígitos de la contraseña introducida y el número de dígitos de la contraseña interna del sistema son diferentes («Sí» en la etapa 2410), el servidor de verificación 12 borra el carácter numérico incluido en una posición designada, que es una posición predeterminada, en la contraseña introducida (etapa 2414). En la presente forma de realización, la posición predeterminada es el dígito «1», que es el dígito situado más a la derecha, y el servidor de verificación 12 borra el carácter numérico «1» del dígito «1» de la contraseña introducida «45871», con lo que se obtiene «4587». Es decir, a partir de la contraseña introducida que posee cinco dígitos, se borra el número predeterminado de caracteres numéricos, con lo que se obtiene la contraseña de 4 dígitos.

La posición designada en la contraseña se registra preferentemente en la base de datos de verificación 14. La posición designada se puede determinar en correspondencia con cada sistema de destino de uso 11. En la presente forma de realización, la posición designada en la contraseña se registra de antemano en el servidor de verificación 12, y el servidor de verificación 12 lee el dígito «1» como la posición designada a partir de la base de datos de verificación 14, y se borra el carácter numérico en el dígito «1» de la contraseña introducida.

A continuación, el servidor de verificación 12 decide si la contraseña introducida después de que se haya borrado el carácter numérico predeterminado coincide o no con la contraseña interna del sistema (etapa 2416). Entonces, cuando se decide que no hay coincidencia («No» en la etapa 2416), el servidor de verificación 12 notifica al sistema de destino de uso 11 que la verificación ha resultado negativa (etapa 2412).

Cuando el servidor de verificación 12 ha decidido que la contraseña introducida con el carácter numérico predeterminado borrado coincide con la contraseña interna del sistema («Sí» en la etapa 2416), el servidor de verificación 12 notifica al sistema de destino de uso 11 que la verificación ha resultado positiva y que se debe llevar a cabo el proceso predeterminado (etapa 2418). A continuación, se ofrece una explicación referente a un procedimiento mediante el cual el servidor de verificación 12 decide el proceso que se debe notificar al sistema de destino de uso 11.

La fig. 29 es un diagrama que muestra una base de datos de códigos de función en la que el proceso notificado al sistema de destino utilizado (11) se asocia con un código de función que corresponde a ese proceso y está constituida por caracteres predeterminados. De este modo, el servidor de verificación 12 vincula, y registra de antemano, con la base de datos de verificación 14 un código de función que se debe incluir en la posición designada de la contraseña introducida y el proceso que se debe notificar al sistema de destino utilizado 11. Entonces, el servidor de verificación 12, basándose en los caracteres borrados incluidos en la posición designada de la contraseña introducida, extrae el proceso que se debe notificar al sistema de destino utilizado 11 a partir de la base de datos de códigos de función y lo notifica al sistema de destino utilizado 11. Se puede designar una pluralidad de posiciones para una contraseña. Además, el código de función puede consistir en caracteres numéricos de varios dígitos o un texto o texto gráfico u otros caracteres similares.

Por ejemplo, en el caso de que el carácter borrado sea «0», el servidor de verificación 12 notifica al sistema de destino utilizado 11 que solo se trata de una prueba para practicar. Así, el sistema de destino utilizado 11 proporciona al usuario un servicio de práctica. Además, cuando el carácter borrado es «2», el servidor de verificación 12 notifica al sistema de destino utilizado 11 que se ha producido una situación de emergencia. Entonces, el sistema de destino utilizado 11, por ejemplo, informa a la policía o similar, o bloquea el identificador de usuario, la información de identificación temporal y la información de identificación de usuario por sistema, o lleva a cabo otro proceso de este tipo. Además, en el caso de que el sistema de destino utilizado 11 sea un sistema de gestión bancaria y ya se haya realizado la verificación de usuario, de manera que el usuario pueda realizar un depósito en una cuenta predeterminada, se puede establecer una cantidad de cero yenes como depósito en cuenta, o llevar a cabo una acción similar para crear la apariencia de que se ha depositado una suma de dinero designada por el usuario, mostrando una pantalla ficticia en la pantalla del sistema de destino de uso 11. Por consiguiente, aun en el caso de que, por ejemplo, un usuario sea amenazado para usar el sistema de destino utilizado 11, el usuario puede informar al servidor de verificación 12 y al sistema de destino utilizado 11 de que se ha producido una situación de emergencia, sin que la otra persona se dé cuenta.

Además, en el caso de que el carácter borrado sea el 9, el servidor de verificación 12 consulta la base de datos de códigos de función, decide que el carácter borrado es ficticio y notifica al sistema de destino utilizado 11 que la verificación de usuario ha resultado positiva. En este caso, el servidor de verificación 12 también puede notificar al sistema de destino utilizado 11 que el elemento ficticio se incluyó como código de función.

En la presente forma de realización, la contraseña introducida es «45871» y la contraseña interna del sistema es «4587». Por lo tanto, el servidor de verificación 12 extrae el número «1» como carácter designado. Entonces, el servidor de verificación 12 consulta la base de datos de códigos de función incluida en la base de datos de verificación 14 y notifica al sistema de destino utilizado 11 que la confirmación ha resultado positiva y que es de solo lectura. Así, el sistema de destino utilizado 11 proporciona servicios de solo lectura al usuario. Los servicios de solo lectura consisten, por ejemplo, en mostrar el saldo de una cuenta bancaria, visualizar foros y otros servicios de este tipo. Por consiguiente, el usuario puede obtener una contraseña de solo lectura que permita al usuario ver el saldo bancario, por ejemplo, y que se genera cada vez que se lleva a cabo la verificación de usuario, y permite que el usuario solicite a otra persona que use la contraseña para dejar que la otra persona vea el saldo bancario, sin que la otra persona sepa que esa contraseña es de solo lectura.

De acuerdo con la presente forma de realización, al incluir los caracteres predeterminados en la contraseña, el usuario puede solicitar al servidor de verificación 12 y/o al sistema de destino utilizado 11 un proceso predeterminado, sin que lo sepa otra persona. Además, al incluir el carácter predeterminado en la contraseña, se puede solicitar, simplemente introduciendo la contraseña, al servidor de verificación 12 y/o el sistema de destino utilizado 11 que lleven a cabo múltiple procesos. Además, de acuerdo con la presente forma de realización, al incluir los caracteres predeterminados en la contraseña, el número de dígitos de la contraseña introducida aumenta y, de este modo, se puede elevar aún más el nivel de seguridad de la contraseña.

[Séptima forma de realización]

La presente forma de realización se refiere a un procedimiento de verificación en el que una persona distinta al usuario introduce la contraseña desde el sistema de destino utilizado 11 para llevar a cabo la verificación de usuario.

La fig. 30 es un diagrama conceptual que explica un esquema global del procedimiento de verificación de usuario de acuerdo con la presente forma de realización. En primer lugar, el usuario utiliza el ordenador personal 15 y registra previamente su patrón de obtención de contraseña para el sistema de destino utilizado 11, junto con la información personal que sea necesaria para usar el sistema de destino utilizado 11, en la base de datos de verificación 14 ((1) en el diagrama). El usuario obtiene entonces el identificador de sistema del sistema de destino utilizado 11 a partir de un confirmante que intentará usar el sistema de destino utilizado 11 para confirmar la identidad del propio usuario o usuaria ((2) en el diagrama). Por ejemplo, el usuario obtiene el identificador del confirmante para el sistema de destino utilizado 11, a través de la televisión, radio, revistas u otro medio de información.

A continuación, el usuario introduce ese identificador de sistema en el teléfono móvil 13 y lo envía al servidor de verificación 12 ((3) en el diagrama). El servidor de verificación 12 recibe esta transmisión, genera la tabla de números aleatorios y la envía al teléfono móvil 13 del usuario como patrón presentado ((4) en el diagrama). En este momento, el servidor de verificación 12 puede enviar la información temporal al teléfono móvil 13 del usuario. El usuario consulta el patrón presentado que se muestra en el teléfono móvil 13 y después obtiene la secuencia de valores del elemento (contraseña) asignada al propio patrón de obtención de contraseña del usuario y lo notifica al confirmante ((5) en el diagrama). Por ejemplo, el usuario puede utilizar un teléfono, correo electrónico u otros medios de transmisión de información para notificar la contraseña al confirmante. En este momento, el usuario también puede informar al confirmante acerca de la información de identificación temporal. El confirmante introduce la contraseña y/o información de identificación temporal que se notificó al usuario. Por consiguiente, el sistema de destino utilizado 11 envía la contraseña introducida y/o la información de identificación temporal al servidor de verificación 12 ((6) en el diagrama).

El servidor de verificación 12 recibe la contraseña procedente del sistema de destino utilizado 11 y después compara la cadena de caracteres numéricos obtenida a partir del patrón de obtención de contraseña del usuario que ya se ha registrado y el patrón presentado que se generó, con la contraseña que se envió desde el sistema de destino utilizado 11, para decidir si coinciden. Después, el servidor de verificación 12 notifica el resultado positivo de la verificación cuando coinciden y el resultado negativo en caso contrario, al sistema de destino utilizado 11 indicado por el identificador de sistema ((7) en el diagrama). Entonces, en el caso de la confirmación positiva del usuario, el confirmante utiliza el sistema de destino utilizado 11 para obtener a partir del servidor de verificación 12 la información personal necesaria para ese usuario.

En la presente forma de realización, el «confirmante» es, por ejemplo, una compañía de compras por teléfono, un profesional hotelero que haya recibido una reserva de alojamiento, un profesional inmobiliario que haya recibido una solicitud de alquiler, emisores de diversos tipos de documentación de identificación personal, una compañía de tarjetas de crédito que ofrezca crédito o una forma de pagar una cuenta, un médico que realice una consulta, o similares. Además, la «información personal necesaria» consiste en, por ejemplo, la dirección del usuario, número de teléfono, número de tarjeta de crédito, cuenta de ahorros, historial médico, documentos médicos, currículum vítae, lugar de trabajo u otra información similar relativa al usuario. El usuario puede restringir la información personal que se pone a disposición del confirmante usando el sistema de destino utilizado 11. Por ejemplo, cuando el usuario envía el identificador de sistema desde el teléfono móvil 13 al servidor de verificación 12, el usuario puede introducir un código para restringir la revelación de la información personal y enviarlo al servidor de verificación 12.

La presente invención proporciona el nuevo procedimiento de verificación de usuario y sistema para llevarlo a cabo, que impide de manera eficaz el acceso ilegítimo a un sistema por parte de un tercero.

Además, la presente invención puede proporcionar el procedimiento de verificación de usuario y el sistema para llevarlo a cabo, que utiliza al máximo la infraestructura del sistema existente, sin incurrir en gastos extra.

REIVINDICACIONES

1. Un procedimiento de verificación de usuario realizado en un servidor de verificación (12), con un sistema de destino de uso (11) conectado al servidor de verificación (12) y un terminal informático (13) que se puede conectar con el servidor de verificación (12), y dicho sistema de destino de uso (11) se comunica con el servidor de verificación (12) a través de un primer canal de comunicación, y el procedimiento comprende las etapas de:

registro de un patrón de obtención de contraseña basado en un elemento específico seleccionado entre un grupo de elementos que forman un patrón predeterminado;

recepción de un mensaje de inicio del procedimiento de verificación que incluye información de identificación del sistema asignada al sistema de destino de uso (11), en la que dicho mensaje de inicio del procedimiento de verificación se envía desde el dispositivo terminal informático (13) de un usuario a través de un segundo canal de comunicación;

en el que el sistema de destino de uso (11) incluye un interfaz de usuario para llevar a cabo un procedimiento de cálculo per una instrucción facilitada a través del interfaz de usuario y, como respuesta a una operación del usuario, muestra en pantalla la información de identificación del sistema, para permitir que el usuario introduzca la información de identificación del sistema en el terminal informático (13),

en el que el terminal informático (13) es un dispositivo de comunicación portátil que el usuario lleva consigo, de tal manera que el usuario del terminal informático (13) se comunica con otro dispositivo de comunicación portátil,

generación de un patrón presentado en el que se asigna un carácter predeterminado a cada elemento del grupo de elementos que forma el patrón predeterminado, cuando se recibe la información de identificación del sistema procedente del terminal informático (13);

envío, a través del segundo canal de comunicación, del patrón presentado generado, desde el servidor de verificación (12) al terminal informático (13), e indicación al usuario de que introduzca un carácter asignado a un elemento específico correspondiente al patrón de obtención de contraseña;

recepción del carácter introducido desde el sistema de destino de uso (11) por el servidor de verificación (12) a través del primer canal de comunicación, y

exclusión de una solicitud de verificación de usuario procedente de un sistema de destino de uso no registrado por ser ilegítima, basada en mensajes de inicio del procedimiento de verificación recibidos, y toma de decisión acerca de si el carácter recibido es legítimo o no, basada en el patrón presentado y el patrón de obtención de contraseña del usuario; y

notificación del resultado de la decisión al sistema de destino de uso (11) a través del primer canal de comunicación.

2. Procedimiento de verificación de usuario de acuerdo con la reivindicación 1, en el que, en la etapa de registro, se registra el patrón de obtención de contraseña asociado con información de identificación del usuario que se asigna a cada usuario.

3. Procedimiento de verificación de usuario de acuerdo con la reivindicación 2, en el que, en la etapa de toma de decisión, se recibe la información de identificación del usuario desde el terminal informático (13), y se especifica el patrón de obtención de contraseña del usuario de entre los patrones de obtención de contraseña registrados, basándose en la información de identificación de usuario recibida.

4. Procedimiento de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que, en la etapa de toma de decisión, se especifica el carácter asignado a un elemento específico del patrón presentado, basándose en el patrón de obtención de contraseña del usuario, y se compara el carácter recibido y el carácter especificado.

5. Procedimiento de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que la etapa registro comprende las etapas de:

presentación al usuario de una pantalla que contiene un patrón de registro en el que se asigna un nombre de elemento a cada grupo de elementos, e invitación al usuario para que introduzca su selección de un elemento específico; y

registro del patrón de obtención de contraseña basándose en el elemento específico introducido selectivamente por el usuario.

6. Procedimiento de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que el patrón de obtención de contraseña es una secuencia de nombres de elementos asignados a los elementos específicos del patrón predeterminado.

7. Procedimiento de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en el que la etapa de registro comprende las etapas de:

invitación al usuario para que introduzca una regla de conversión predeterminada para el carácter predeterminado asignado al elemento específico introducido selectivamente; y

registro del patrón de obtención de contraseña, basándose en la regla de conversión predeterminada.

8. Procedimiento de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 1 a 7, en el que, en la etapa de generación, se genera el patrón presentado basándose en un valor numérico aleatorio obtenido con una función numérica aleatoria predeterminada.

9. Sistema de verificación de usuario para llevar a cabo la verificación de usuario en un servidor de verificación (12), con un sistema de destino de uso (11) conectado al servidor de verificación (12) y un terminal informático (13) que se puede conectar con el servidor de verificación (12), y dicho sistema de destino de uso (11) se comunica con el servidor de verificación (12) a través de un primer canal de comunicación, que comprende:

medios de registro adaptados para registrar un patrón de obtención de contraseña basándose en un elemento específico seleccionado entre un grupo de elementos que forman un patrón predeterminado;

medios de recepción adaptados para recibir un mensaje de inicio del procedimiento de verificación que incluye información de identificación del sistema asignada al sistema de destino de uso (11), y dicho mensaje de inicio del procedimiento de verificación se envía desde el dispositivo terminal informático (13) de un usuario a través de un segundo canal de comunicación;

en el que el sistema de destino de uso (11) incluye un interfaz de usuario para llevar a cabo un procedimiento de cálculo per una instrucción facilitada a través del interfaz de usuario y, como respuesta a una operación del usuario, mostrar en pantalla la información de identificación del sistema, para permitir que el usuario introduzca la información de identificación del sistema en el terminal informático (13),

en el que el terminal informático (13) es un dispositivo de comunicación portátil que el usuario lleva consigo, de tal manera que el usuario del terminal informático (13) se comunica con otro dispositivo de comunicación portátil,

medios de generación adaptados para generar un patrón presentado en el que se asigna un carácter predeterminado a cada elemento del grupo de elementos que forma el patrón predeterminado, cuando se recibe la información de identificación del sistema procedente del terminal informático (13);

medios de envío adaptados para enviar, a través del segundo canal de comunicación, el patrón presentado generado, desde el servidor de verificación (12) al terminal informático (13), y solicitar al usuario que introduzca un carácter asignado a un elemento específico correspondiente al patrón de obtención de contraseña;

otros medios de recepción adaptados para recibir el carácter introducido desde el sistema de destino de uso (11) por el servidor de verificación (12) a través del primer canal de comunicación, y

medios de toma de decisiones adaptados para excluir una solicitud de verificación de usuario por ser ilegítima, procedente de un sistema de destino de uso no registrado, basándose en mensajes de inicio del procedimiento de verificación recibidos, y para decidir si el carácter recibido es legítimo o no, basándose en el patrón presentado y el patrón de obtención de contraseña del usuario; y

medios de notificación adaptados para notificar el resultado de la decisión al sistema de destino de uso (11) a través del primer canal de comunicación.

10. Sistema de verificación de usuario de acuerdo con la reivindicación 9, en el que los medios de registro están también adaptados para registrar el patrón de obtención de contraseña asociado con información de identificación del usuario que se asigna a cada usuario.

11. Sistema de verificación de usuario de acuerdo con la reivindicación 10, en el que los medios de toma de decisión están también adaptados para recibir la información de identificación del usuario desde el terminal informático (13), y para especificar el patrón de obtención de contraseña del usuario de entre los patrones de obtención de contraseña registrados, basándose en la información de identificación de usuario recibida.

12. Sistema de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 9 a 11, en el que los medios de toma de decisión están también adaptados para especificar el carácter asignado a un elemento específico del patrón presentado, basándose en el patrón de obtención de contraseña del usuario, y comparar el carácter recibido y el carácter especificado.

13. Sistema de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 9 a 12, en el que los medios de registro están también adaptados para:

presentar al usuario una pantalla que contiene un patrón de registro en el que se asigna un nombre de elemento a cada grupo de elementos, y para solicitar al usuario que introduzca su selección de un elemento específico; y

registrar el patrón de obtención de contraseña basándose en el elemento específico introducido selectivamente por el usuario.

14. Sistema de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 9 a 13, en el que el patrón de obtención de contraseña es una secuencia de nombres de elementos asignados a los elementos específicos del patrón predeterminado.

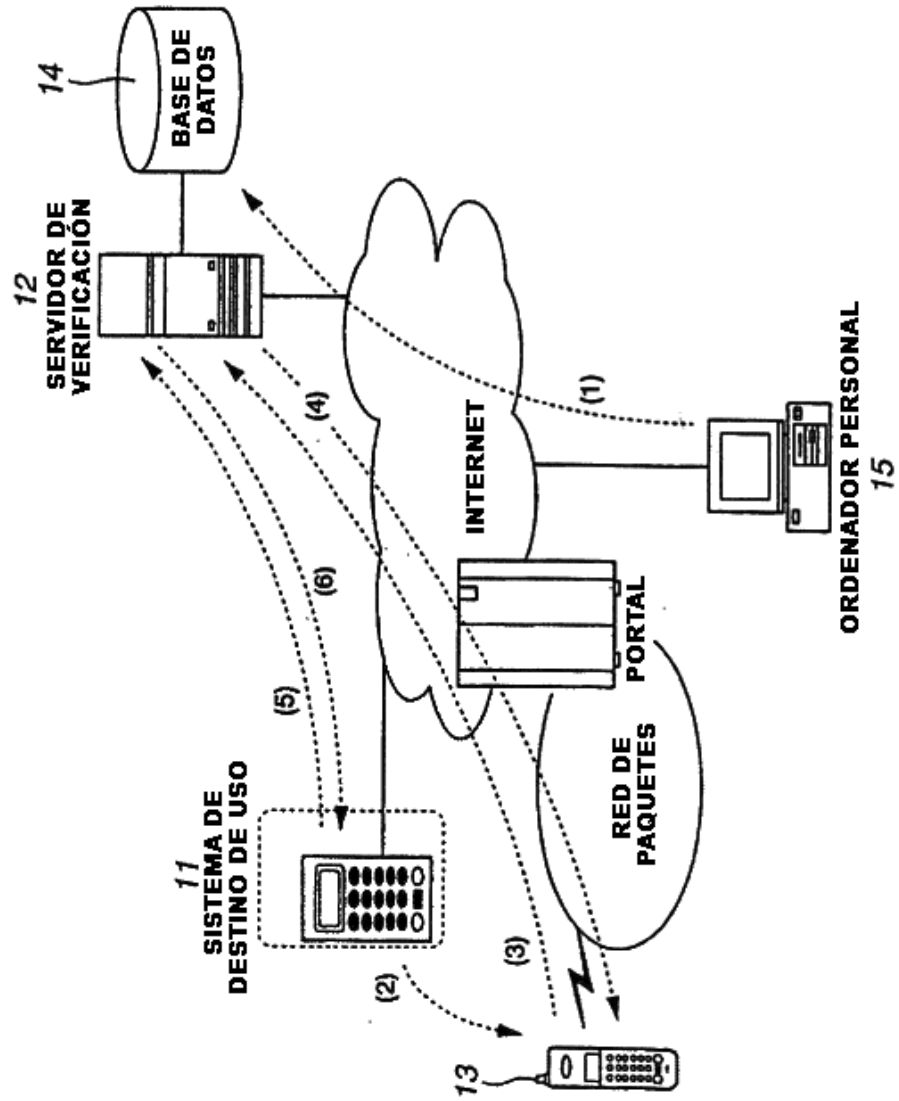
15. Sistema de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 9 a 14, en el que los medios de registro están también adaptados para:

solicitar al usuario que introduzca una regla de conversión predeterminada para el carácter predeterminado asignado al elemento específico introducido selectivamente; y

registrar el patrón de obtención de contraseña, basándose en la regla de conversión predeterminada.

16. Sistema de verificación de usuario de acuerdo con una cualquiera de las reivindicaciones 9 a 15, en el que los medios de generación están también adaptados para generar el patrón presentado, basándose en un valor numérico aleatorio obtenido con una función numérica aleatoria predeterminada.

FIG.1


14
BASE DE DATOS
12
SERVIDOR DE VERIFICACIÓN
INTERNET
(1)
ORDENADOR PERSONAL
15
(4)
(6)
(5)
PORTAL
RED DE PAQUETES
11
SISTEMA DE DESTINO DE USO
(3)
(2)
13

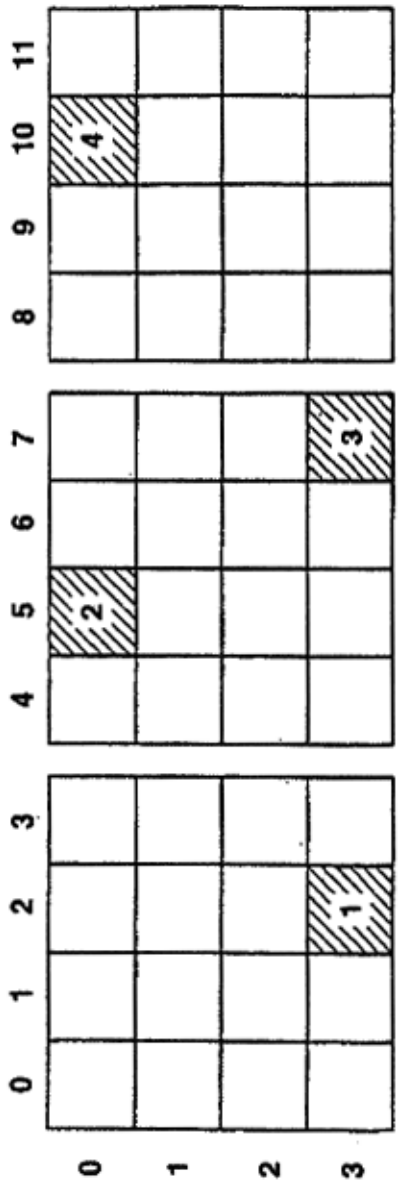


FIG.2A

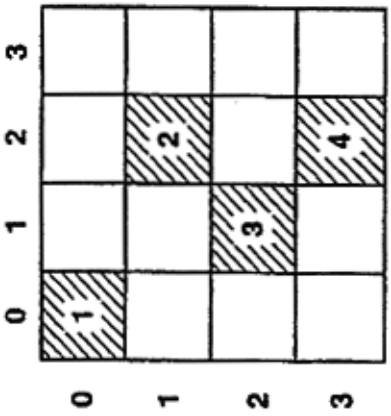


FIG.2B

FIG.3

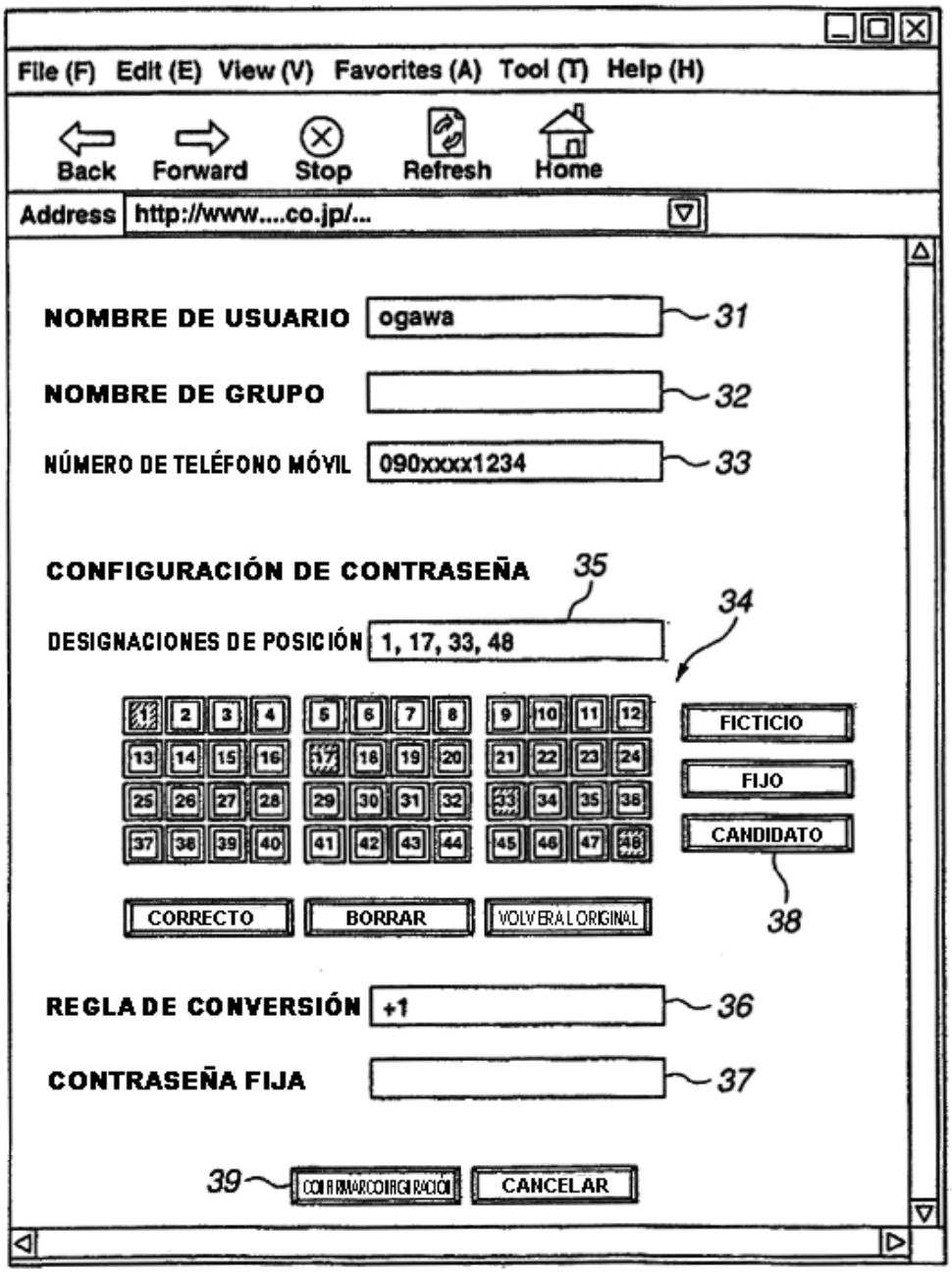

File (F) Edit (E) View (V) Favorites (A) Tool (T) Help (H)
Back
Forward
Stop
Refresh
Home
Address
http://www....co.jp/...
NOMBRE DE USUARIO
ogawa
31
NOMBRE DE GRUPO
32
NÚMERO DE TELÉFONO MÓVIL
090xxxx1234
33
CONFIGURACIÓN DE CONTRASEÑA
35
34
DESIGNACIONES DE POSICIÓN
1, 17, 33, 48
FICTICIO
FIJO
CANDIDATO
38
CORRECTO
BORRAR
VOLVER A L ORIGINAL
REGLA DE CONVERSIÓN
+1
36
CONTRASEÑA FIJA
37
39
CANCELAR

FIG.4

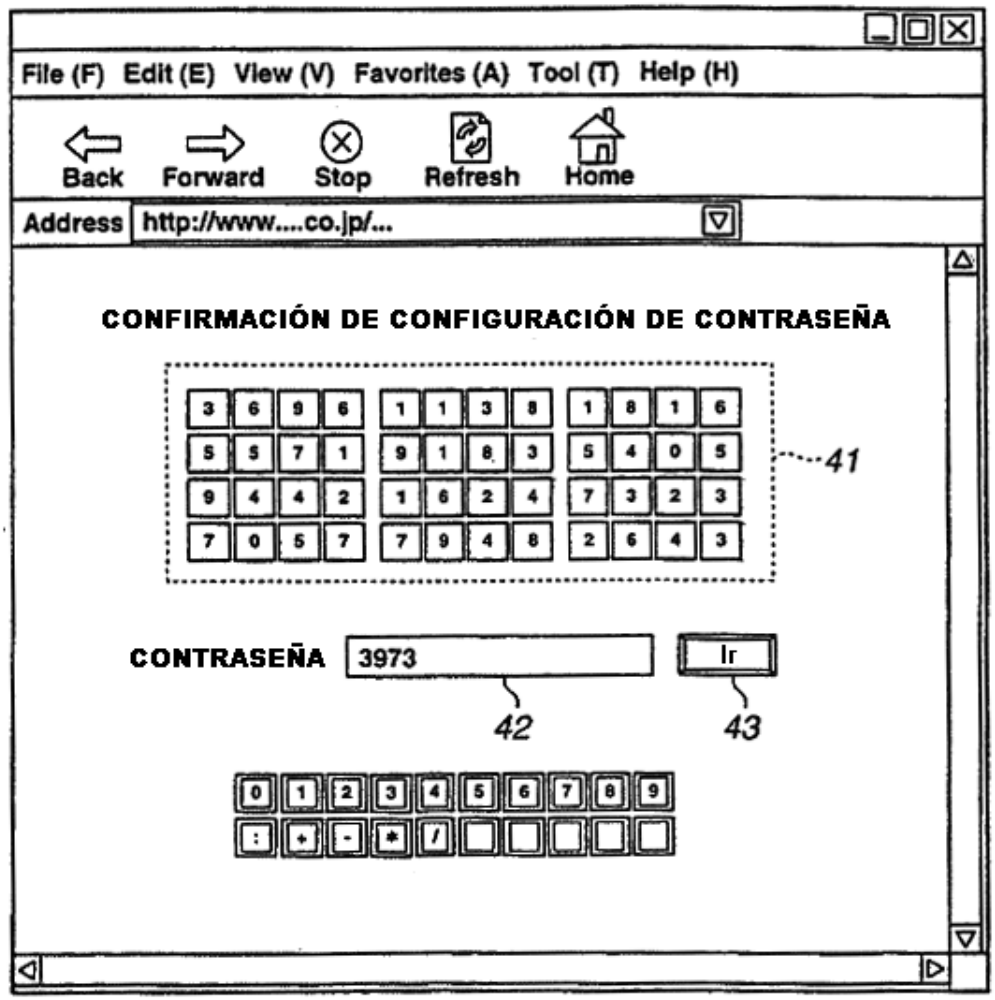
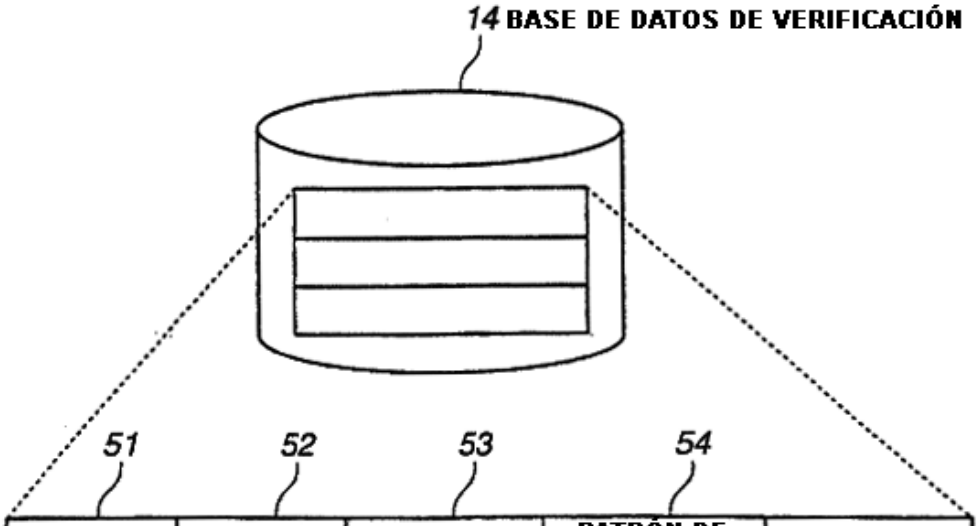

File (F) Edit (E) View (V) Favorites (A) Tool (T) Help (H)
Back
Forward
Stop
Refresh
Home
Address
http://www....co.jp/...
CONFIRMACIÓN DE CONFIGURACIÓN DE CONTRASEÑA
3 6 9 6 1 1 3 8 1 8 1 6
5 5 7 1 9 1 8 3 5 4 0 5
9 4 4 2 1 6 2 4 7 3 2 3
7 0 5 7 7 9 4 8 2 6 4 3
41
CONTRASEÑA
3973
Ir
42
43
0 1 2 3 4 5 6 7 8 9
: + - * /

FIG.5



ID DE SISTEMA	CUENTA DE USUARIO	ID DE USUARIO	PATRÓN DE OBTENCIÓN DE CONTRASEÑA	REGLA DE CONVERSIÓN
36578979	ogawa	090xxxx1234	1, 17, 33, 48	+1
36578979	taro	030xxxx5678	F4762	
36578980	ogawa	090xxxx1234	16, 30, 23, 55	0

FIG.6

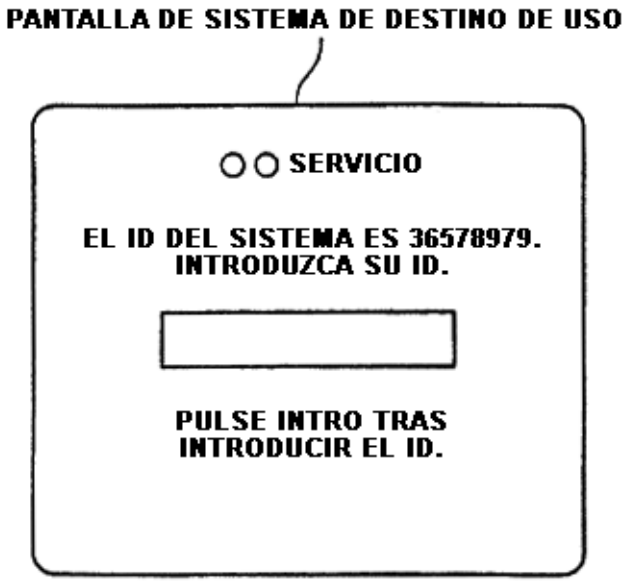

PANTALLA DE SISTEMA DE DESTINO DE USO
SERVICIO
EL ID DEL SISTEMA ES 36578979.
INTRODUZCA SU ID.
PULSE INTRO TRAS
INTRODUCIR EL ID.

FIG.7

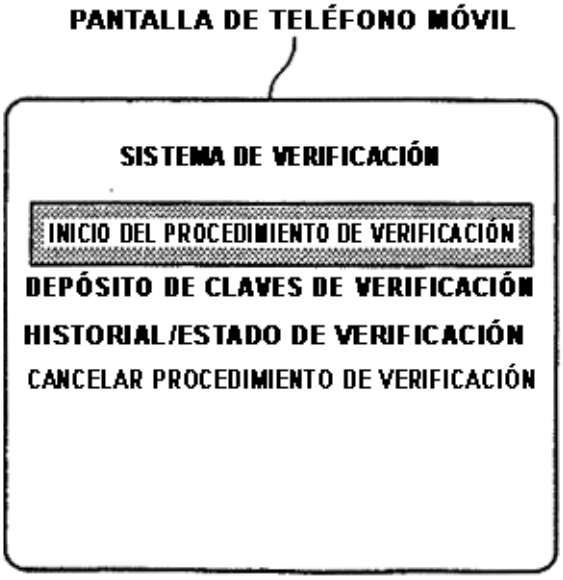

PANTALLA DE TELÉFONO MÓVIL
SISTEMA DE VERIFICACIÓN
INICIO DEL PROCEDIMIENTO DE VERIFICACIÓN
DEPÓSITO DE CLAVES DE VERIFICACIÓN
HISTORIAL/ESTADO DE VERIFICACIÓN
CANCELAR PROCEDIMIENTO DE VERIFICACIÓN

FIG.8


PANTALLA DE TELÉFONO MÓVIL
INICIAR PROCEDIMIENTO DE VERIFICACIÓN
INTRODUCIR ID DEL SISTEMA:
36578979
OK

FIG.9


INICIO
RECIBIR MENSAJE DE INICIO DEL PROCEDIMIENTO DE VERIFICACIÓN Y EXTRACCIÓN DE ID DE SISTEMA E ID DE USUARIO
ETAPA 901
PROCESO PARA ESPERAR LA SOLICITUD DE VERIFICACIÓN DE USUARIO PROCEDENTE DEL SISTEMA DE DESTINO DE USO
ETAPA 902
GENERAR EL PATRÓN PRESENTADO
ETAPA 903
REGISTRAR EL PATRÓN PRESENTADO EN LA TABLA DE ESPERA DE SOLICITUD DE VERIFICACIÓN DE USUARIO
ETAPA 904
ENVIAR PATRÓN PRESENTADO
ETAPA 905
FIN

FIG.10

101 ID DE EVENTO	102 ID DE SISTEMA	103 ID DE USUARIO	PATRÓN PRESENTADO
:	:	:	:
99	36578979	090xxxx1234	587981012938...
:	:	:	:
:	:	:	:

FIG.11

FIG.12

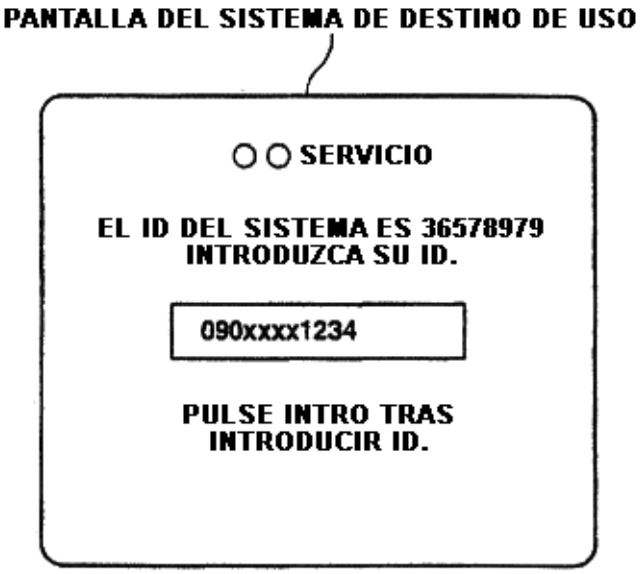

PANTALLA DEL SISTEMA DE DESTINO DE USO
SERVICIO
EL ID DEL SISTEMA ES 36578979
INTRODUZCA SU ID.
090xxxx1234
PULSE INTRO TRAS
INTRODUCIR ID.

FIG.13

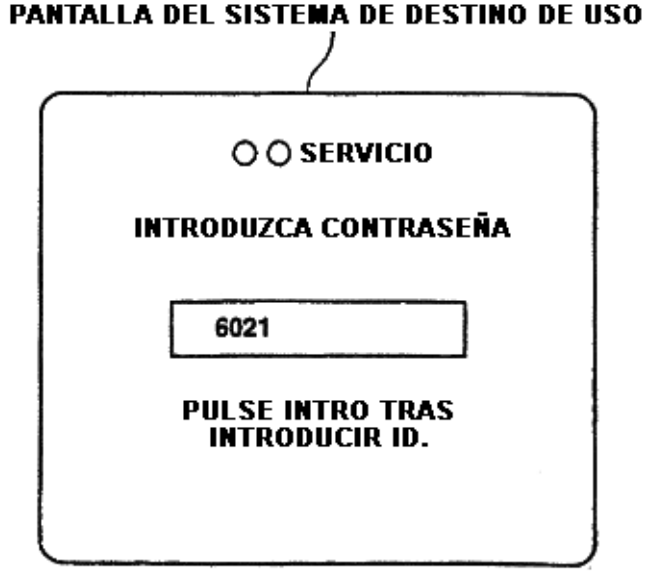

PANTALLA DEL SISTEMA DE DESTINO DE USO
SERVICIO
INTRODUZCA CONTRASEÑA
6021
PULSE INTRO TRAS
INTRODUCIR ID.

FIG.14

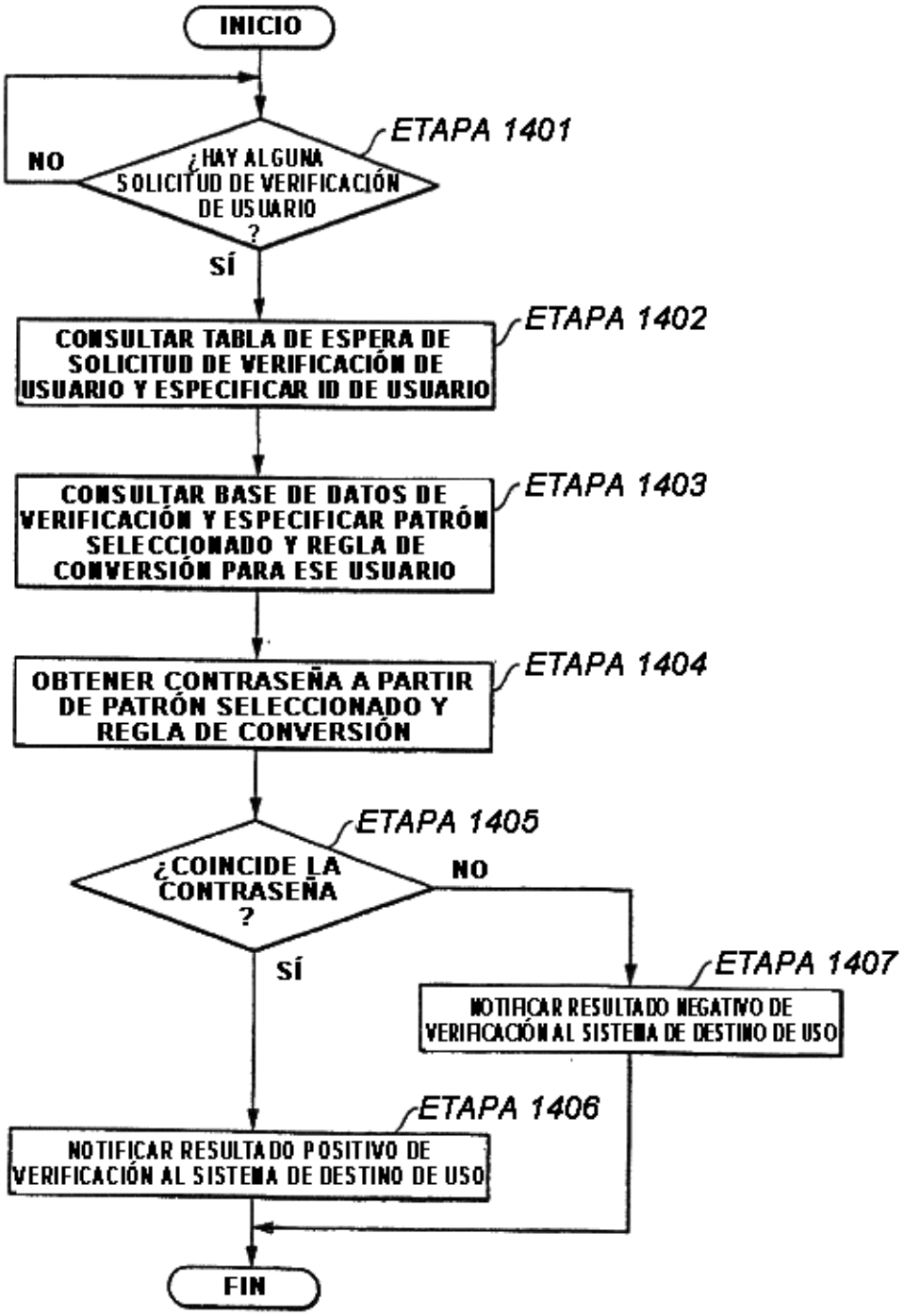

INICIO
ETAPA 1401
¿HAY ALGUNA SOLICITUD DE VERIFICACIÓN DE USUARIO ?
NO
SÍ
ETAPA 1402
CONSULTAR TABLA DE ESPERA DE SOLICITUD DE VERIFICACIÓN DE USUARIO Y ESPECIFICAR ID DE USUARIO
ETAPA 1403
CONSULTAR BASE DE DATOS DE VERIFICACIÓN Y ESPECIFICAR PATRÓN SELECCIONADO Y REGLA DE CONVERSIÓN PARA ESE USUARIO
ETAPA 1404
OBTENER CONTRASEÑA A PARTIR DE PATRÓN SELECCIONADO Y REGLA DE CONVERSIÓN
ETAPA 1405
¿COINCIDE LA CONTRASEÑA ?
NO
SÍ
ETAPA 1407
NOTIFICAR RESULTADO NEGATIVO DE VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
ETAPA 1406
NOTIFICAR RESULTADO POSITIVO DE VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
FIN

FIG.15

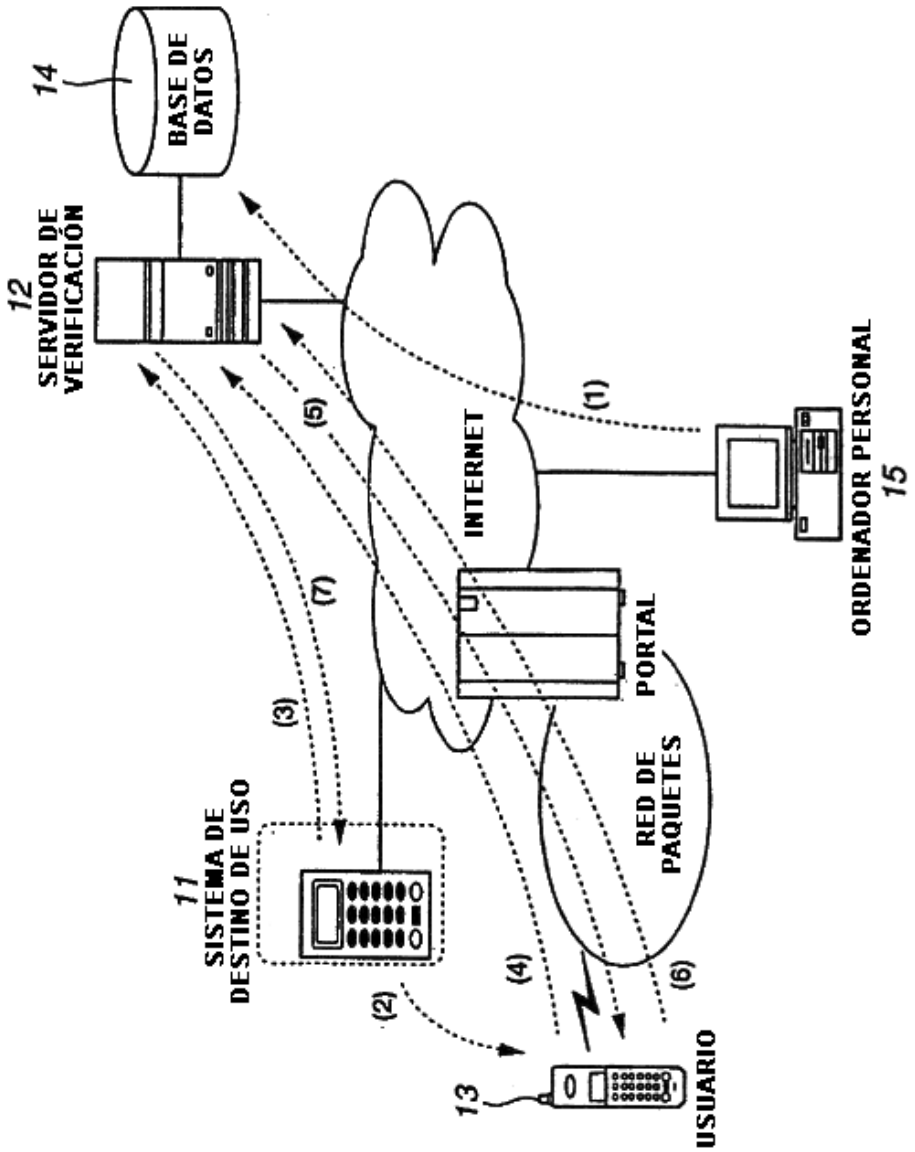

14
BASE DE DATOS
12
SERVIDOR DE VERIFICACIÓN
INTERNET
(1)
ORDENADOR PERSONAL
15
(5)
(7)
(3)
PORTAL
RED DE PAQUETES
11
SISTEMA DE DESTINO DE USO
(2)
(4)
(6)
13
USUARIO

FIG.16A

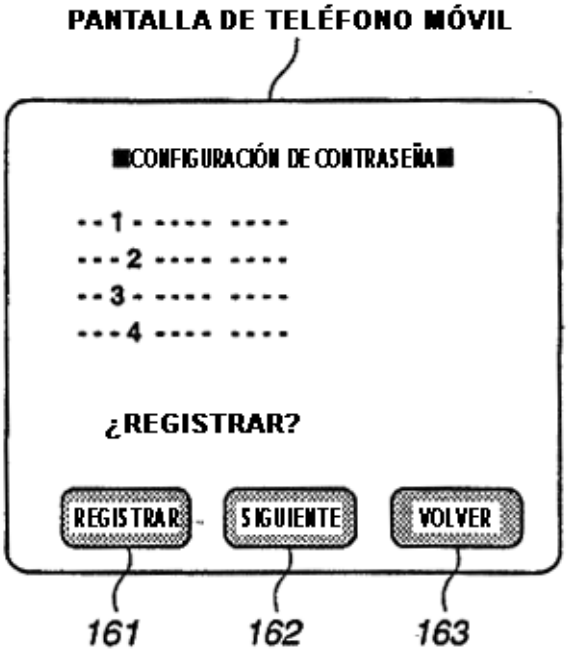


FIG.16B

FIG.17

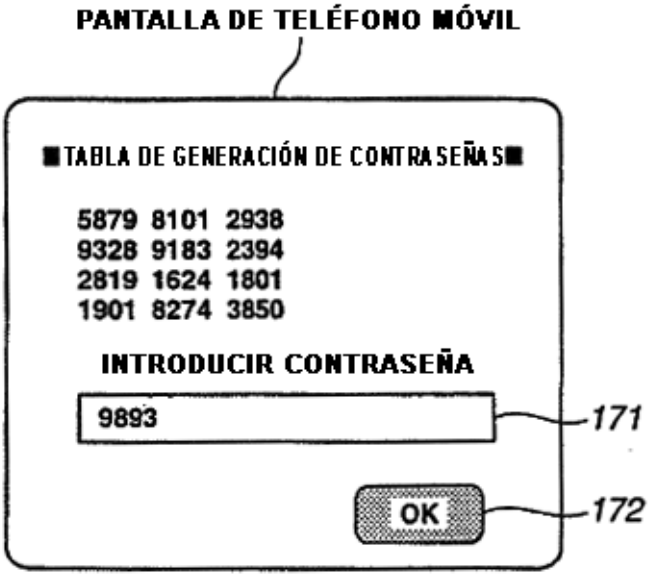

PANTALLA DE TELÉFONO MÓVIL
■TABLA DE GENERACIÓN DE CONTRASEÑAS■
5879 8101 2938
9328 9183 2394
2819 1624 1801
1901 8274 3850
INTRODUCIR CONTRASEÑA
9893
171
OK
172

FIG.18

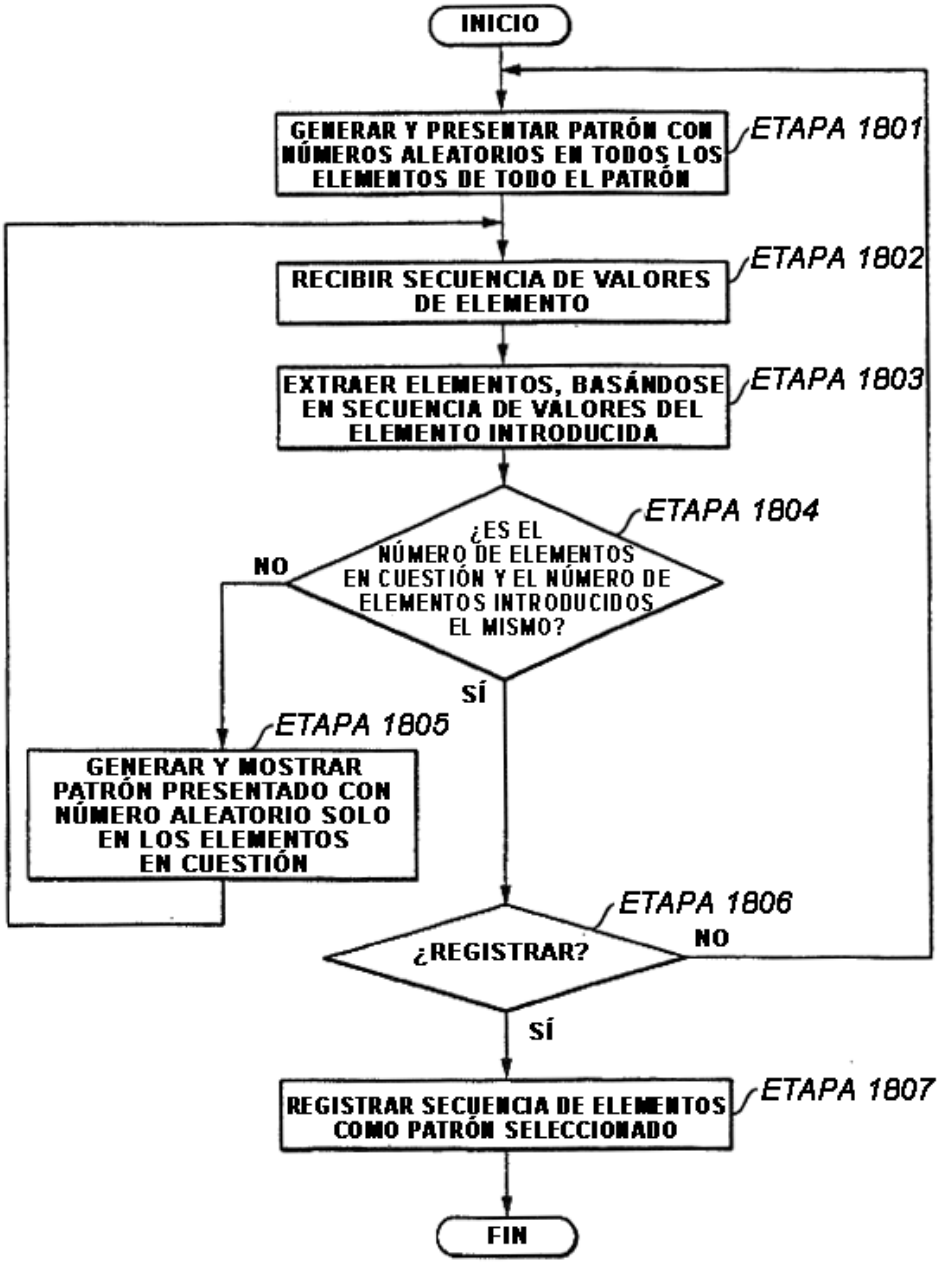

INICIO
GENERAR Y PRESENTAR PATRÓN CON NÚMEROS ALEATORIOS EN TODOS LOS ELEMENTOS DE TODO EL PATRÓN
ETAPA 1801
RECIBIR SECUENCIA DE VALORES DE ELEMENTO
ETAPA 1802
EXTRAER ELEMENTOS, BASÁNDOSE EN SECUENCIA DE VALORES DEL ELEMENTO INTRODUCIDA
ETAPA 1803
¿ES EL NÚMERO DE ELEMENTOS EN CUESTIÓN Y EL NÚMERO DE ELEMENTOS INTRODUCIDOS EL MISMO?
ETAPA 1804
NO
SÍ
GENERAR Y MOSTRAR PATRÓN PRESENTADO CON NÚMERO ALEATORIO SOLO EN LOS ELEMENTOS EN CUESTIÓN
ETAPA 1805
¿REGISTRAR?
ETAPA 1806
NO
SÍ
REGISTRAR SECUENCIA DE ELEMENTOS COMO PATRÓN SELECCIONADO
ETAPA 1807
FIN

FIG.19A

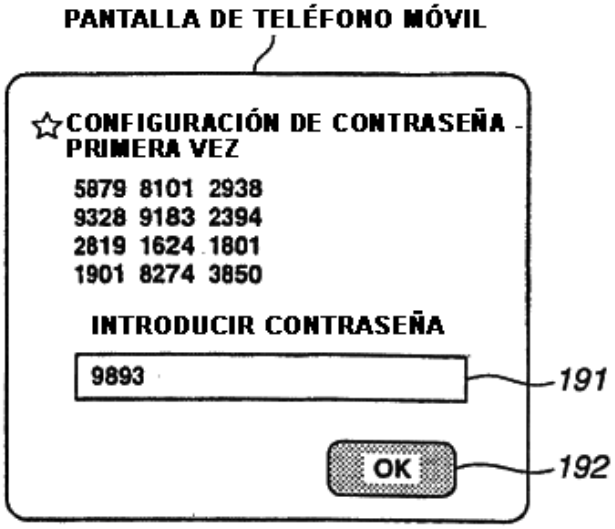


FIG.19B

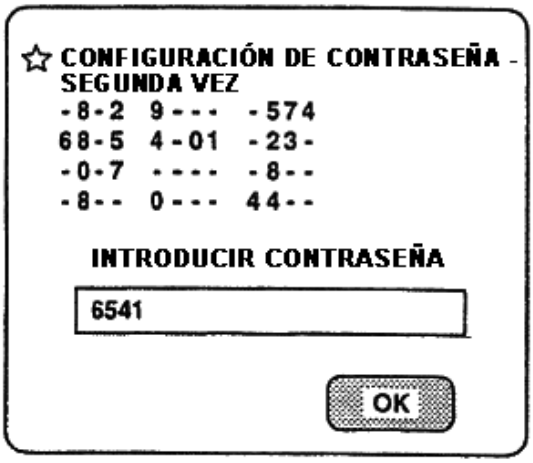


FIG.19C

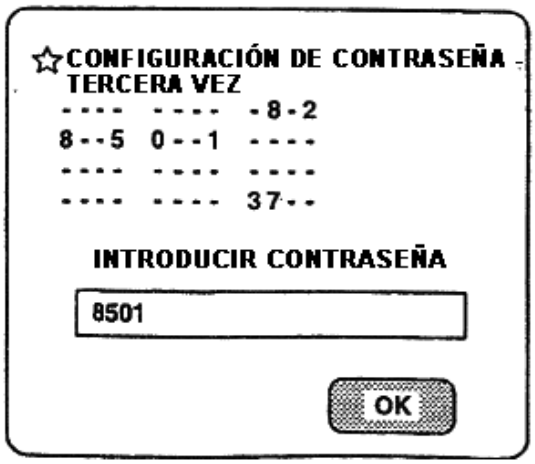


FIG.20


PANTALLA DE TELÉFONO MÓVIL
CONFIGURACIÓN DE CONTRASEÑA - PRIMERA VEZ
1--2 3--4
¿REGISTRAR?
REHACER
OK
202
201

FIG.21

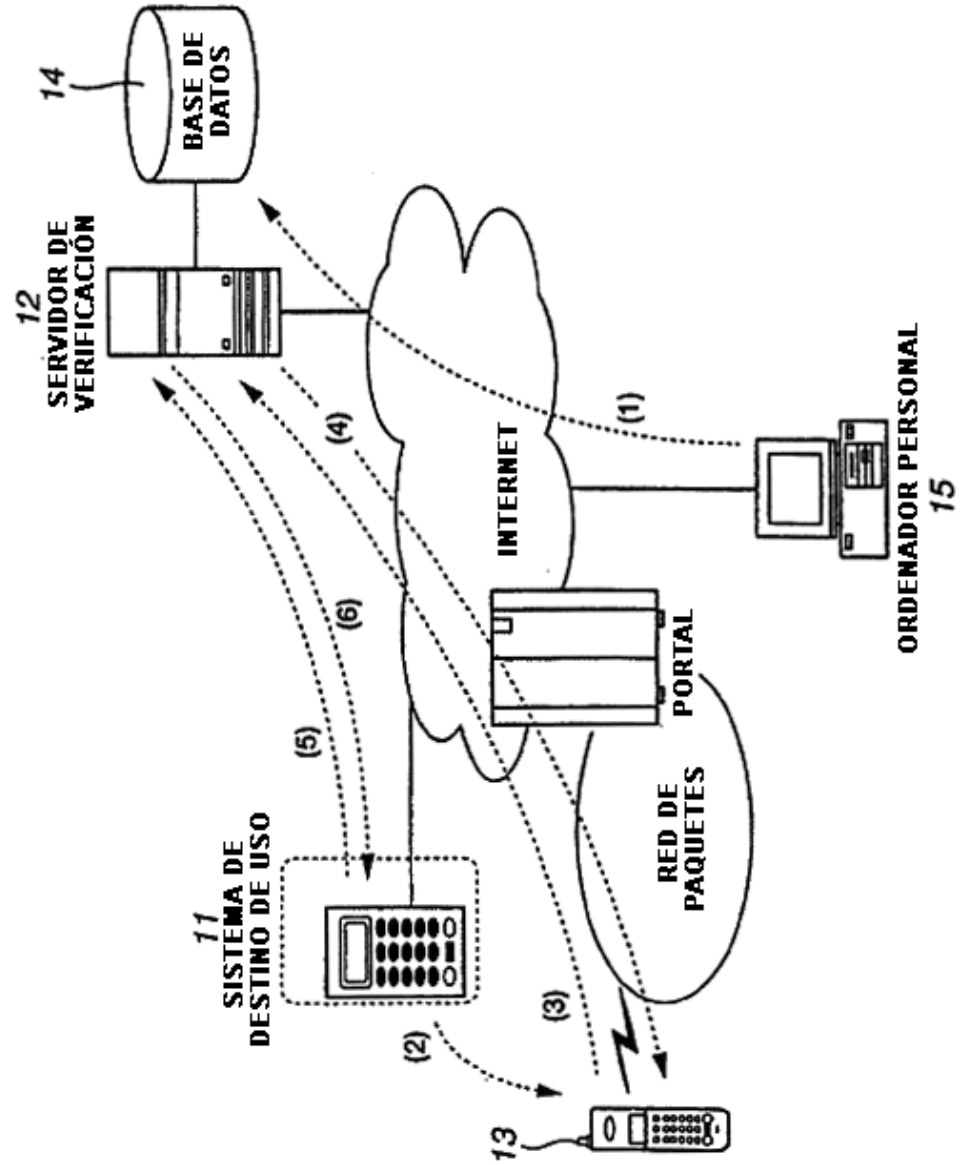

14
BASE DE DATOS
12
SERVIDOR DE VERIFICACIÓN
INTERNET
(1)
ORDENADOR PERSONAL
15
(4)
(6)
(5)
PORTAL
RED DE PAQUETES
11
SISTEMA DE DESTINO DE USO
(3)
(2)
13

FIG.22

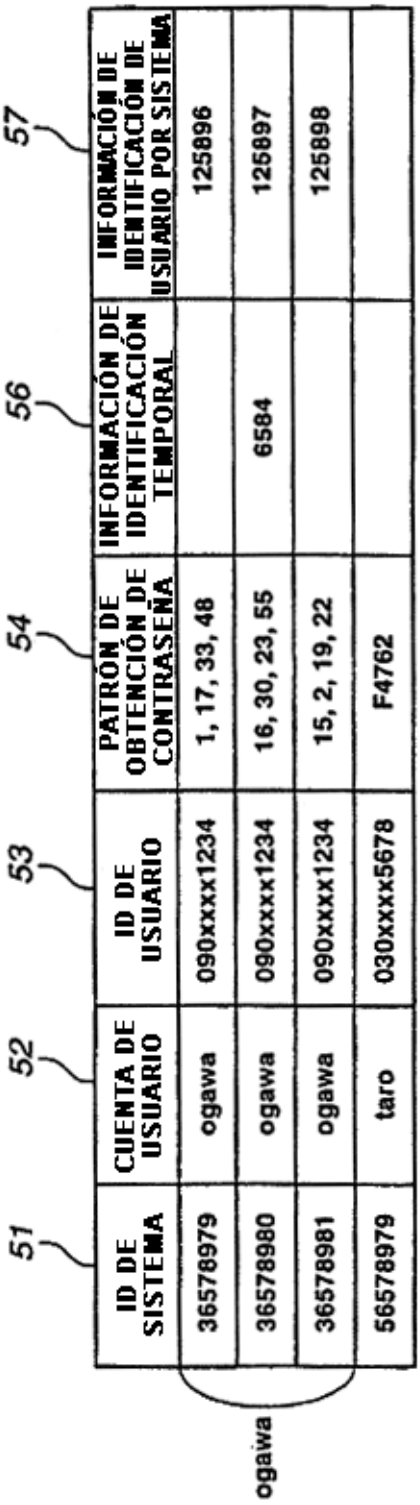

51
52
53
54
56
57
ID DE SISTEMA
CUENTA DE USUARIO
ID DE USUARIO
PATRÓN DE OBTENCIÓN DE CONTRASEÑA
INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL
INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA
36578979 ogawa 090xxxx1234 1, 17, 33, 48 125896
36578980 ogawa 090xxxx1234 16, 30, 23, 55 6584 125897
36578981 ogawa 090xxxx1234 15, 2, 19, 22 125898
56578979 taro 030xxxx5678 F4762
ogawa

FIG.23

100 ID DE EVENTO	101 ID DE SISTEMA	102 ID DE USUARIO	103 PATRÓN PRESENTADO	104 INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL
:	:	:	:	:
100	36578979	090xxxx1234	58798...	6584
:	:	:	:	:
:	:	:	:	:

FIG.24

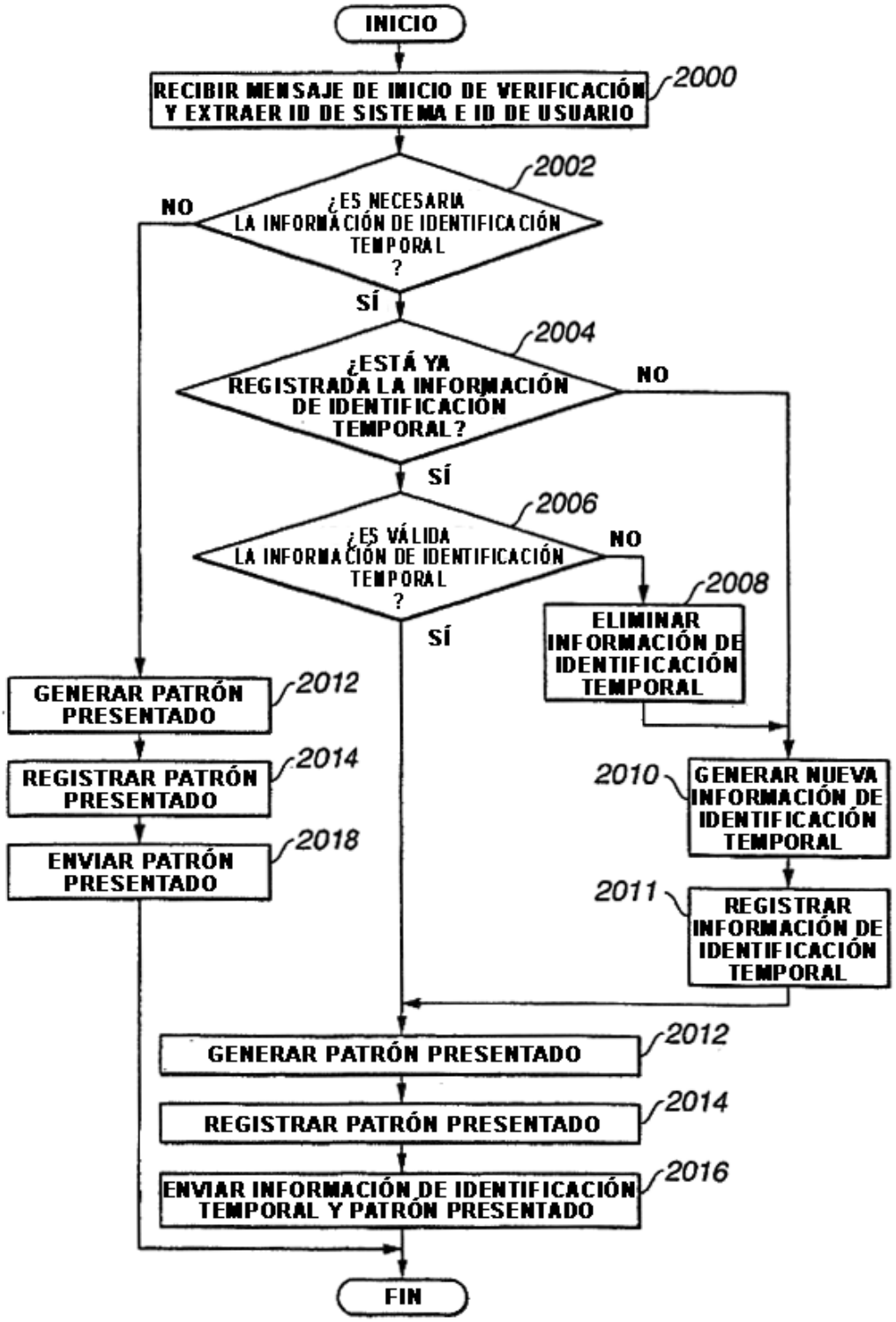

INICIO
RECIBIR MENSAJE DE INICIO DE VERIFICACIÓN Y EXTRAER ID DE SISTEMA E ID DE USUARIO
2000
¿ES NECESARIA LA INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL ?
2002
NO
SÍ
¿ESTÁ YA REGISTRADA LA INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL?
2004
NO
SÍ
¿ES VÁLIDA LA INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL ?
2006
NO
SÍ
ELIMINAR INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL
2008
GENERAR PATRÓN PRESENTADO
2012
REGISTRAR PATRÓN PRESENTADO
2014
ENVIAR PATRÓN PRESENTADO
2018
2010
GENERAR NUEVA INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL
2011
REGISTRAR INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL
GENERAR PATRÓN PRESENTADO
2012
REGISTRAR PATRÓN PRESENTADO
2014
ENVIAR INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL Y PATRÓN PRESENTADO
2016
FIN

FIG.25

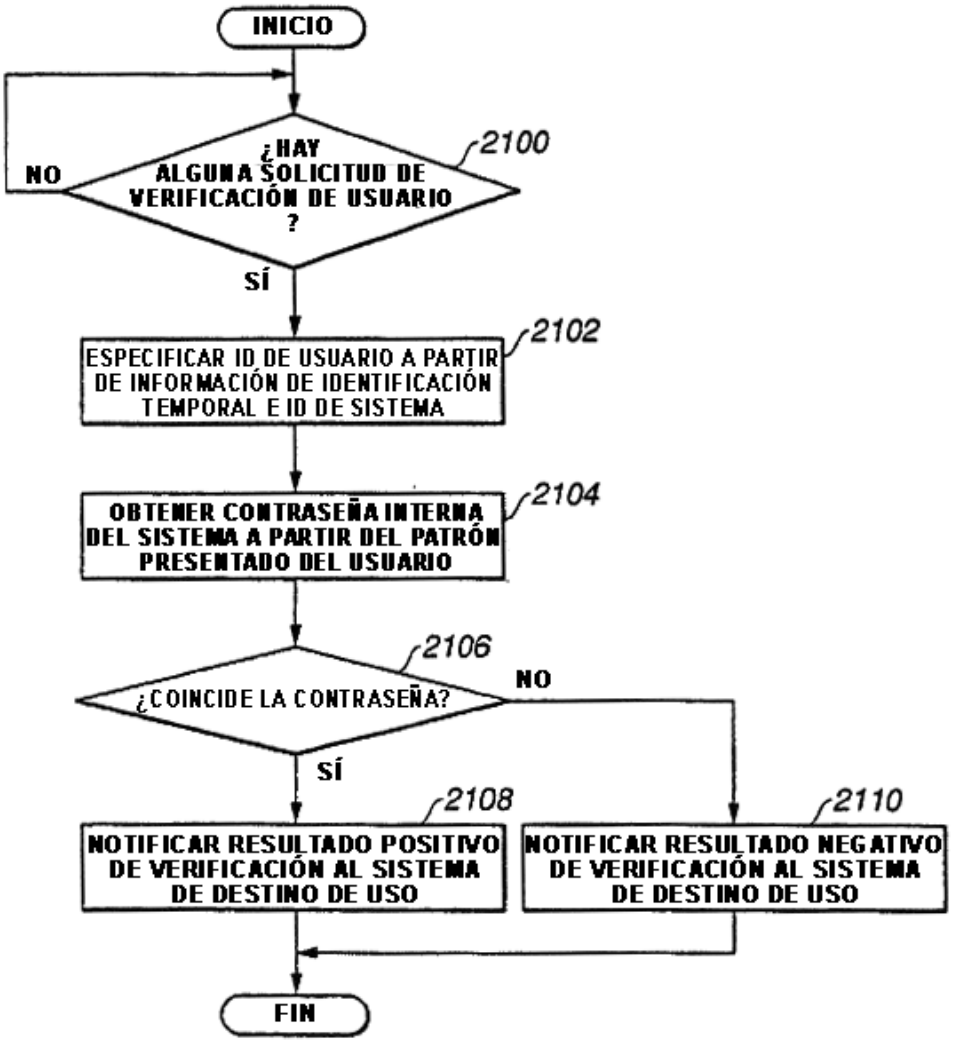

INICIO
¿HAY ALGUNA SOLICITUD DE VERIFICACIÓN DE USUARIO ?
2100
NO
SÍ
ESPECIFICAR ID DE USUARIO A PARTIR DE INFORMACIÓN DE IDENTIFICACIÓN TEMPORAL E ID DE SISTEMA
2102
OBTENER CONTRASEÑA INTERNA DEL SISTEMA A PARTIR DEL PATRÓN PRESENTADO DEL USUARIO
2104
¿COINCIDE LA CONTRASEÑA?
2106
NO
SÍ
NOTIFICAR RESULTADO POSITIVO DE VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
2108
NOTIFICAR RESULTADO NEGATIVO DE VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
2110
FIN

FIG.26

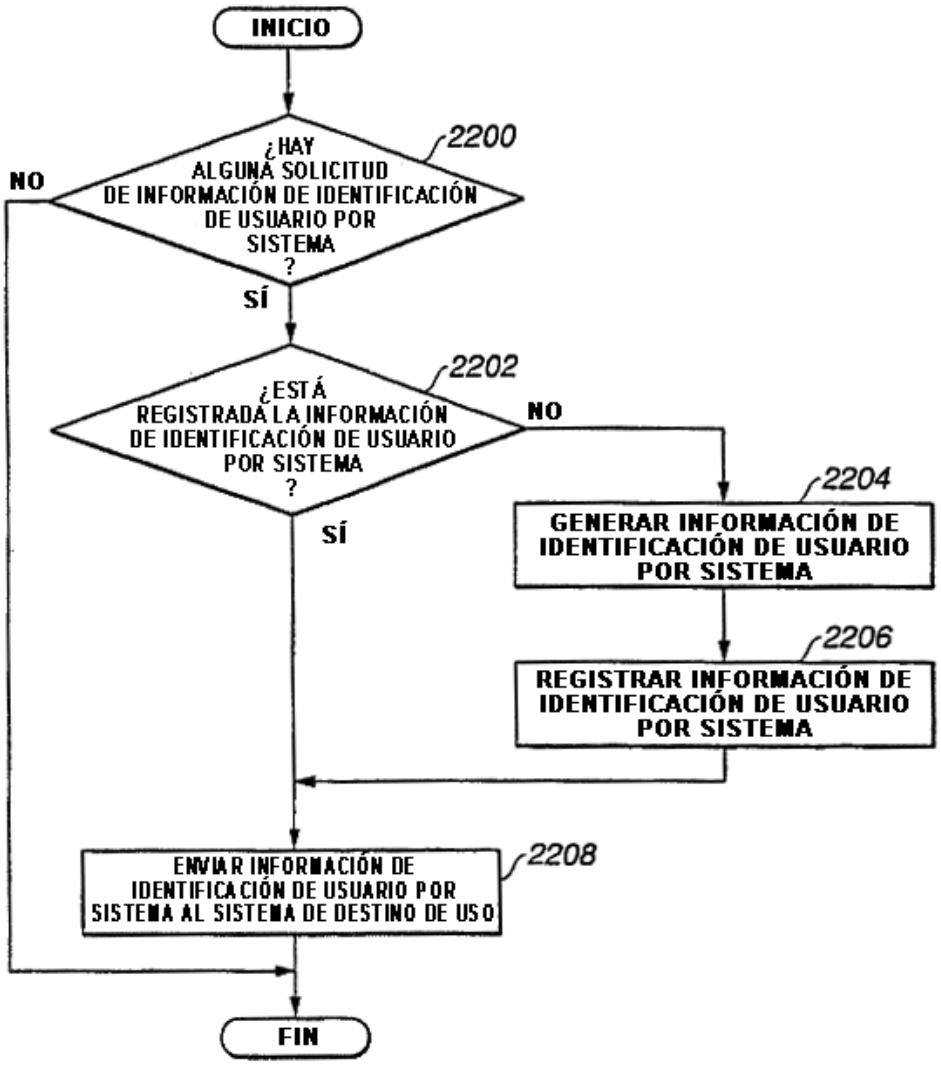

INICIO
¿HAY ALGUNA SOLICITUD DE INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA ?
2200
NO
SÍ
¿ESTÁ REGISTRADA LA INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA ?
2202
NO
SÍ
GENERAR INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA
2204
REGISTRAR INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA
2206
ENVIAR INFORMACIÓN DE IDENTIFICACIÓN DE USUARIO POR SISTEMA AL SISTEMA DE DESTINO DE USO
2208
FIN

FIG.27


INICIO
GENERAR TABLA DE CONVERSIÓN DE NÚMEROS ALEATORIOS
2300
GENERAR ID DE IDENTIFICACIÓN INTERNA DE USUARIO PARA CADA USUARIO
2302
GENERAR TABLA DE CONVERSIÓN POR SISTEMA PARA CADA SISTEMA DE DESTINO DE USO
2304
GENERAR ID DE IDENTIFICACIÓN INTERNA DEL SITIO PARA CADA SISTEMA DE DESTINO DE USO
2306
SUMAR ID DE IDENTIFICACIÓN INTERNA POR SISTEMA A ID DE IDENTIFICACIÓN INTERNA DE USUARIO
2308
CONVERTIR USANDO TABLA DE CONVERSIÓN POR SISTEMA
2310
CONVERTIR USANDO TABLA DE CONVERSIÓN DE NÚMEROS ALEATORIOS
2312
CONVERTIR USANDO TABLA DE CONVERSIÓN POR SISTEMA
2314
FIN

FIG.28

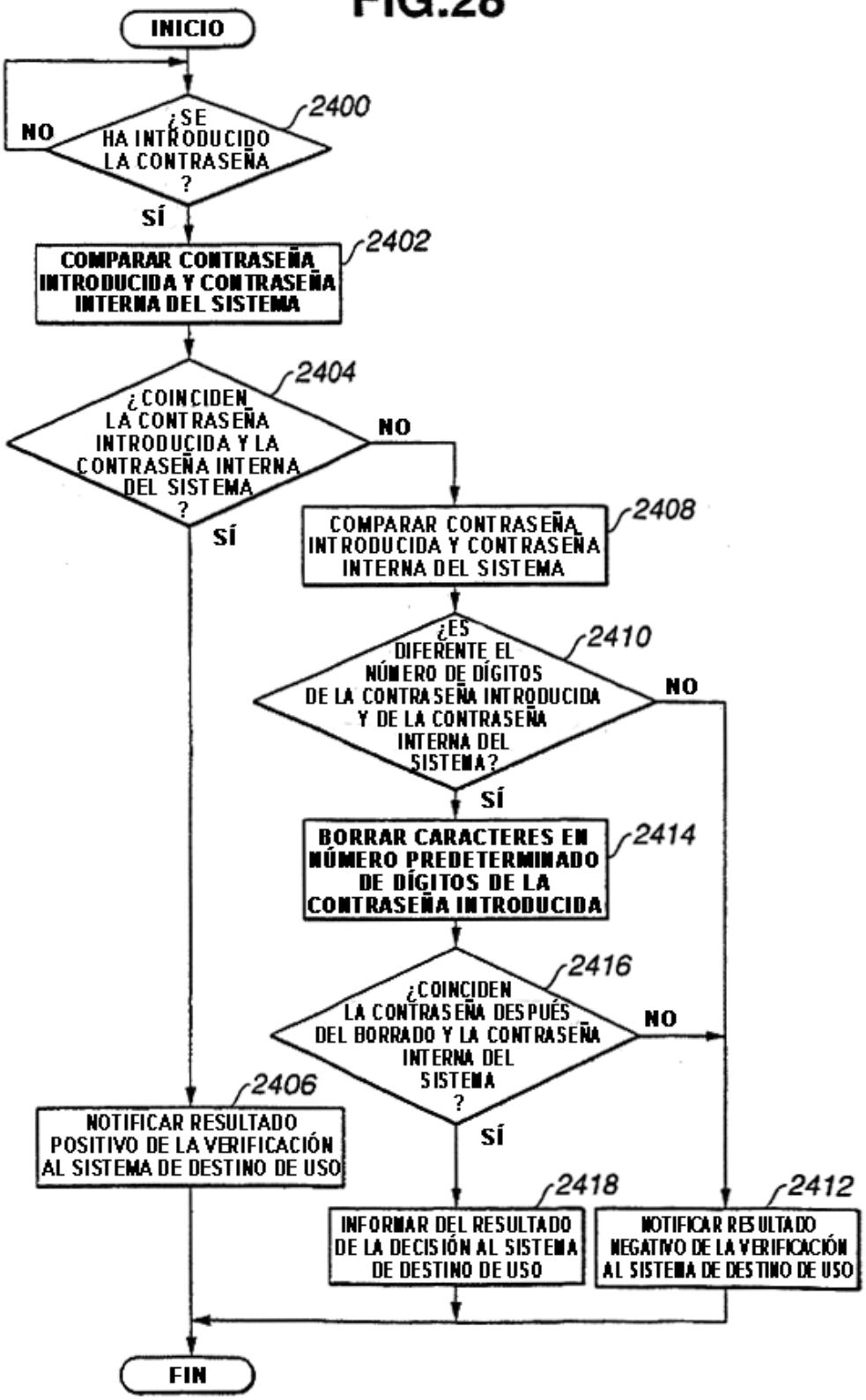
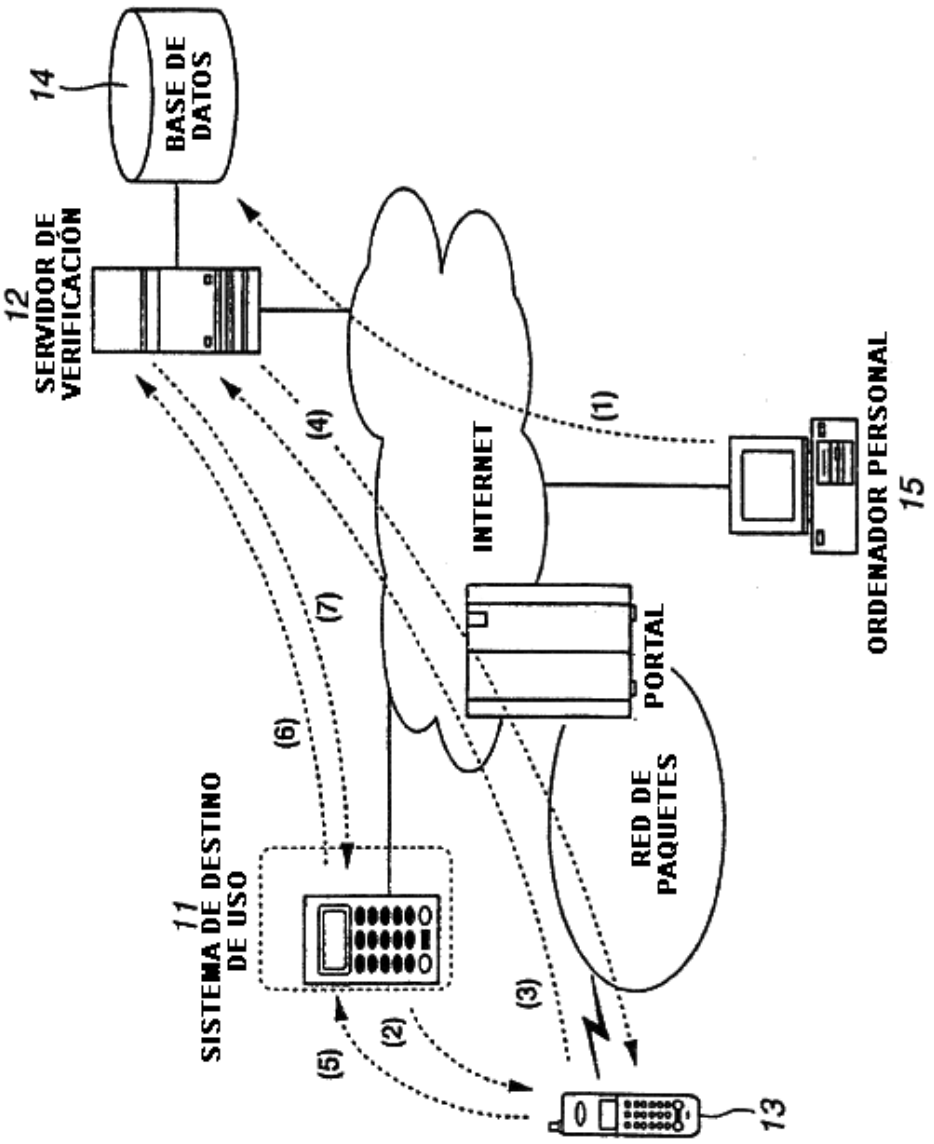

INICIO
¿SE HA INTRODUCIDO LA CONTRASEÑA ?
2400
NO
SÍ
COMPARAR CONTRASEÑA INTRODUCIDA Y CONTRASEÑA INTERNA DEL SISTEMA
2402
¿COINCIDEN LA CONTRASEÑA INTRODUCIDA Y LA CONTRASEÑA INTERNA DEL SISTEMA ?
2404
NO
SÍ
COMPARAR CONTRASEÑA INTRODUCIDA Y CONTRASEÑA INTERNA DEL SISTEMA
2408
¿ES DIFERENTE EL NÚMERO DE DÍGITOS DE LA CONTRASEÑA INTRODUCIDA Y DE LA CONTRASEÑA INTERNA DEL SISTEMA?
2410
NO
SÍ
BORRAR CARACTERES EN NÚMERO PREDETERMINADO DE DÍGITOS DE LA CONTRASEÑA INTRODUCIDA
2414
¿COINCIDEN LA CONTRASEÑA DESPUÉS DEL BORRADO Y LA CONTRASEÑA INTERNA DEL SISTEMA ?
2416
NO
SÍ
NOTIFICAR RESULTADO POSITIVO DE LA VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
2406
INFORMAR DEL RESULTADO DE LA DECISIÓN AL SISTEMA DE DESTINO DE USO
2418
NOTIFICAR RESULTADO NEGATIVO DE LA VERIFICACIÓN AL SISTEMA DE DESTINO DE USO
2412
FIN

FIG.29

CÓDIGO DE FUNCIÓN	PROCESO PARA NOTIFICACIÓN
0	PARA PRACTICAR
1	SOLO LECTURA
2	EMERGENCIA
:	:
:	:
9	FICTICIO
:	:
:	:

FIG.30


14
BASE DE DATOS
12
SERVIDOR DE VERIFICACIÓN
INTERNET
(1)
(4)
(7)
(6)
ORDENADOR PERSONAL
15
PORTAL
RED DE PAQUETES
11
SISTEMA DE DESTINO DE USO
(3)
(2)
(5)
13