

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 924 270**

51 Int. Cl.:

G06F 21/45 (2013.01)

G06F 21/31 (2013.01)

G06F 21/36 (2013.01)

G06F (2012.01)

G06F 21/46 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **04.03.2014 E 20205443 (3)**

97 Fecha y número de publicación de la concesión europea: **13.07.2022 EP 3792797**

54 Título: **Aparato y procedimiento para configurar el acceso a las aplicaciones**

30 Prioridad:

05.03.2013 KR 20130023451

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

05.10.2022

73 Titular/es:

**SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu, Suwon-si
Gyeonggi-do 16677, KR**

72 Inventor/es:

YUN, YONG-SANG

74 Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

ES 2 924 270 T3

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

DESCRIPCIÓN

Aparato y procedimiento para configurar el acceso a las aplicaciones

Antecedente

Campo técnico

- 5 La presente divulgación se refiere en general a la configuración de una contraseña y a la liberación de un bloqueo por medio de la contraseña configurada en un dispositivo electrónico.

Descripción de la técnica relacionada:

10 Con los recientes avances en las tecnologías de la información y la comunicación, han proliferado muchos tipos de dispositivos electrónicos portátiles, tales como teléfonos inteligentes y tabletas. Se han implementado varias aplicaciones para SNS, juegos, fotografía, etc. en un dispositivo típico.

15 Generalmente, los dispositivos tales como los teléfonos inteligentes y similares han empleado una función de bloqueo de pantalla. El término "bloqueo de pantalla" se refiere a una condición de pantalla bloqueada en la que sólo se muestra una información predeterminada sin la realización de la mayoría de las funciones. El bloqueo de la pantalla se produce tras el paso de un tiempo predeterminado después de que no se haya detectado ninguna entrada del usuario en el dispositivo cuando no se están ejecutando aplicaciones que normalmente impiden que se produzca el bloqueo de la pantalla (tal como una aplicación de recepción de emisiones). La función de bloqueo de pantalla restringe la telefonía y evita que se exponga la información personal del usuario, incluidas las fotografías, la lista de transmisiones de mensajes de texto y otros datos similares.

20 Convencionalmente, si se configura una protección por contraseña para el dispositivo, un procedimiento para liberar el bloqueo de pantalla requiere la introducción de una contraseña predeterminada, tal como un patrón de números o patrones táctiles. Es decir, cuando se introduce la contraseña correcta, un dispositivo libera el bloqueo de pantalla y permite al usuario utilizar varias aplicaciones que se pueden ejecutar en el dispositivo.

25 Sin embargo, surge un problema en una situación en la que el dispositivo es compartido por varios usuarios. Es decir, cuando todos los usuarios tienen autoridad para utilizar todas las aplicaciones disponibles en el dispositivo, la información personal de cada usuario queda expuesta a otros usuarios. Además, cuando los padres y los hijos utilizan el dispositivo juntos, existe el problema de que los niños pequeños pueden ver inadvertidamente información inapropiada.

El documento US 2012/0084734 A1 describe un sistema de pantalla de bloqueo de acceso múltiple que permite acceder a diferentes niveles de funcionalidad en un dispositivo informático.

30 El documento US 2012/023573 A1 desvela un procedimiento para establecer una función de restricción de acceso para un dispositivo.

Sumario

Se desvela en la presente memoria un procedimiento para configurar la autoridad en un dispositivo electrónico para utilizar al menos una aplicación de forma diferente para una pluralidad de usuarios.

35 En un aspecto, se proporciona un procedimiento para configurar una contraseña en un dispositivo electrónico. Las entradas de los usuarios se reciben para establecer contraseñas para los respectivos niveles de usuario, en los que cada nivel de usuario está asociado con una autoridad diferente para acceder a las aplicaciones. Las contraseñas se registran para los respectivos niveles de usuario. Al menos una aplicación está asociada a uno de los niveles de usuario.

40 En otro aspecto, se proporciona un procedimiento para liberar un bloqueo en un dispositivo electrónico. El procedimiento incluye: recibir una contraseña de entrada para liberar la cerradura; comparar la contraseña de entrada con contraseñas configuradas para una pluralidad de niveles de usuario asociados con diferentes autoridades para al menos una aplicación; y liberar la cerradura en consideración de un nivel de usuario para la contraseña de entrada cuando la contraseña de entrada coincide con cualquiera de las contraseñas configuradas.

45 También se describen los aparatos para implementar los procedimientos.

Las implementaciones pueden tener la ventaja de evitar que ciertos usuarios accedan a información y contenidos inapropiados.

Breve descripción de los dibujos

50 Lo anterior y otros aspectos, características, y ventajas de de la presente invención se harán más evidentes a partir de la siguiente descripción detallada, tomada en conjunto con los dibujos adjuntos, en los cuales:

La FIG. 1A es un diagrama de flujo que ilustra un procedimiento para configurar una contraseña de acuerdo con realizaciones de la presente invención.

La FIG. 1B es una vista que ilustra un procedimiento para liberar un bloqueo de acuerdo con realizaciones de la presente invención;

5 La FIG. 2 es un diagrama de flujo que ilustra el procedimiento para configurar la contraseña de acuerdo con una realización de la presente invención;

Las FIGS. 3A a 3I son vistas que ilustran un ejemplo del procedimiento para configurar la contraseña de acuerdo con una realización de la presente invención;

10 Las FIGS. 4A a 4H son vistas que ilustran un ejemplo del procedimiento para liberar el bloqueo de acuerdo con una realización de la presente invención;

La FIG. 5 es un diagrama de flujo que ilustra un procedimiento para cambiar de nivel de usuario para cada aplicación de acuerdo con una realización de la presente invención;

Las FIGS. 6A y 6D son vistas que ilustran un procedimiento para cambiar un nivel de usuario para cada aplicación de acuerdo con una realización de la presente invención;

15 La FIG. 7 es un diagrama de flujo que ilustra procesos para configurar automáticamente un nivel de usuario a una aplicación descargada de acuerdo con una realización de la presente invención;

La FIG. 8 es una vista que ilustra un procedimiento para identificar la categoría de información de la aplicación de acuerdo con una realización de la presente invención; y

20 La FIG. 9 es un diagrama de bloques que ilustra un dispositivo electrónico al que se pueden aplicar las realizaciones de la presente invención.

Descripción detallada

En adelante en la presente memoria, se describirán en detalle diversas realizaciones de la presente invención con referencia a los dibujos adjuntos. En la siguiente descripción, una descripción detallada de las funciones y estructuras muy conocidas que se incorporan en la presente memoria se puede omitir para evitar oscurecer el objeto de la presente invención.

Como se ha descrito anteriormente, un procedimiento para liberar un bloqueo de acuerdo con la técnica convencional tiene la desventaja de que la información privada de una determinada persona puede quedar expuesta a otras, o que contenidos inapropiados pueden ser obtenidos por una determinada persona cuando usuarios plurales utilizan un dispositivo.

30 La presente invención aborda estos problemas al proporcionar un esquema en el que se configura una pluralidad de niveles de usuario para permitir que cada usuario acceda a las aplicaciones en función de su nivel, para de este modo evitar que la información privada y los contenidos inapropiados queden expuestos a los demás.

Un dispositivo electrónico ("dispositivo") en las realizaciones descritas en la presente memoria puede ser un dispositivo de información o comunicación portátil tal como un teléfono inteligente, una tableta PC, un teléfono móvil, un libro electrónico, una cámara, un reproductor de juegos, un reproductor de música, un dispositivo de Internet o cualquier otro dispositivo de procesamiento con una pantalla. El dispositivo electrónico también puede ser un dispositivo fijo, tal como un dispositivo de visualización integrado en un electrodoméstico.

Las FIGS. 1A y 1B son diagramas de flujo que ilustran los respectivos procedimientos 100a, 100b de establecer una contraseña, y liberar un bloqueo, de acuerdo con realizaciones de la presente invención.

40 Con referencia a la FIG. 1A, en la etapa 101a, un dispositivo permite a un usuario seleccionar las aplicaciones que están disponibles en cada uno de los múltiples niveles de usuario que están predefinidos. Cada nivel de usuario está designado con una autoridad diferente para utilizar al menos una aplicación que funciona de forma diferente en función del nivel de usuario operativo. Por ejemplo, una aplicación de reproducción de música puede evitar automáticamente la reproducción de canciones clasificadas para un oyente maduro cuando un usuario actual es reconocido como un usuario de nivel bajo (por ejemplo, un nivel infantil). En consecuencia, una o más aplicaciones pueden estar disponibles en cada nivel de usuario, y pueden ser seleccionadas para su ejecución en varios niveles de usuario.

50 A continuación, en la etapa 103a, al recibir diferentes entradas de usuario para establecer contraseñas en cada nivel de usuario, el dispositivo procede a la etapa 105b. En una realización, cada contraseña se puede configurar en forma de números o un patrón o combinación de los mismos.

En la etapa 105a, el dispositivo registra la contraseña de entrada para cada nivel de usuario y la aplicación seleccionada para un nivel de usuario correspondiente. Esta información registrada se utiliza cuando se ejecuta posteriormente una operación de liberación de un bloqueo.

55 La FIG. 1B es un diagrama de flujo que ilustra un procedimiento, 100b, de liberación de bloqueo de acuerdo con una realización de la presente invención. En la etapa 101b, cuando el dispositivo está en estado de bloqueo y un usuario introduce una contraseña para liberar el bloqueo, entonces en la etapa 103b, el dispositivo determina si la contraseña introducida coincide con alguna de las contraseñas registradas correspondientes a uno de los niveles de usuario. Si la contraseña coincide, entonces en la etapa 105b, el dispositivo lleva a cabo la liberación del bloqueo en

consideración del nivel de usuario correspondiente a la contraseña. Es decir, el dispositivo libera el bloqueo para que el usuario pueda utilizar sólo las aplicaciones que están registradas en el nivel de usuario correspondiente. En una implementación, liberar el bloqueo también puede permitir a un usuario utilizar todas las aplicaciones registradas en el nivel de usuario correspondiente y en uno o más niveles de usuario inferiores al nivel de usuario correspondiente.

5 En otras palabras, el dispositivo libera el bloqueo para que el usuario en un nivel de usuario superior esté habilitado para tener autoridad para usar las aplicaciones registradas en el nivel de usuario inferior.

En consecuencia, cuando las contraseñas para los diferentes niveles de usuario de un dispositivo común se registran como se acaba de describir, los usuarios asignados a los diferentes niveles tienen una autoridad diferente entre sí para acceder a las aplicaciones. Por lo tanto, existe la ventaja de que se puede bloquear la información inapropiada a un determinado usuario.

10

La FIG. 2 es un diagrama de flujo que ilustra un procedimiento más específico, 200, de establecer una contraseña de acuerdo con una realización de la presente invención. En la etapa 201, el dispositivo determina si un usuario hace una solicitud para establecer una pluralidad de niveles de usuario. Se trata de una solicitud para establecer las contraseñas correspondientes a cada nivel de usuario, en la que las aplicaciones disponibles dependen de cada nivel de usuario. La solicitud se puede lograr de forma selectiva a través de menús preestablecidos.

15

Cuando se recibe la solicitud, en la etapa 203, el dispositivo recibe una entrada de usuario que designa el número de niveles de usuario. En la presente invención, el dispositivo puede proporcionar al usuario una pantalla de guía para que el usuario introduzca el número de los niveles de usuario. Un ejemplo de pantalla de guía se muestra en la FIG. 3A.

20

Se observa que la etapa 203 se puede omitir de acuerdo con una manera de ajuste. Por ejemplo, un diseñador de dispositivos, un desarrollador de software, etc. puede preestablecer el número de niveles de usuario por defecto. En este caso, el dispositivo puede no pedir al usuario que introduzca un número de niveles de usuario.

En la etapa 205, el dispositivo proporciona al usuario una pantalla guía para que el usuario establezca las especificaciones de detalle relativas a cada nivel de usuario. Es decir, el dispositivo proporciona al usuario la pantalla guía para que éste seleccione las aplicaciones disponibles en cada nivel de usuario y establezca una contraseña relativa al nivel de usuario correspondiente. Algunos ejemplos de estas pantallas se describirán con referencia a las FIGS. 3B a 3D.

25

En los ejemplos de pantalla FIGS. 3B a 3D, se ilustra el ejemplo de establecer tres niveles de usuario. Sin embargo, el número de niveles de usuario puede ser variable de acuerdo con la selección o configuración del usuario.

30

Como se muestra en la FIG. 3B, el dispositivo puede proporcionar al usuario menús 302a, 302b y 302c que se utilizan para seleccionar las aplicaciones disponibles en cada nivel de usuario, y menús 304a, 304b y 304c que se utilizan para introducir una contraseña correspondiente a cada nivel de usuario.

Cuando el usuario selecciona un menú 302a para seleccionar las aplicaciones disponibles en un nivel de usuario 1, el dispositivo puede guiar categorías de aplicaciones al usuario como se muestra en la FIG. 3C. Cuando el usuario selecciona una o más categorías, el dispositivo registra las aplicaciones, que pertenecen a las categorías seleccionadas, como las aplicaciones disponibles en el nivel de usuario 1. Por ejemplo, cuando el usuario selecciona una categoría de "navegador web" como categoría de la aplicación disponible en el nivel de usuario 1, el dispositivo analiza la categoría de las aplicaciones almacenadas en él y registra las aplicaciones incluidas en "navegador web" como la aplicación que estará disponible en el nivel de usuario 1.

35

Las categorías de las respectivas aplicaciones se pueden identificar de varias maneras. Por ejemplo, el dispositivo puede analizar los metadatos de cada aplicación, para de este modo identificar una categoría de la aplicación correspondiente. Como se muestra en la FIG. 8, por otro lado, el dispositivo puede identificar la categoría de la aplicación correspondiente al analizar una página de descarga de la misma o una página vinculada a la página de descarga. De este modo, el dispositivo analiza los metadatos, la página de descarga o similares y analiza las palabras insertadas en una determinada etiqueta, para identificar la categoría de la aplicación correspondiente. Por ejemplo, el dispositivo analiza los metadatos de cada aplicación o de la página de descarga e identifica el valor de la propiedad de una determinada etiqueta, a fin de identificar la categoría de la aplicación correspondiente. En el caso de que una categoría 802 en el valor de la propiedad de la etiqueta determinada indique un juego 804, el dispositivo determina que la categoría de la aplicación correspondiente es un "juego". Por ejemplo, el dispositivo puede solicitar a un proveedor de aplicaciones que transmita información sobre la categoría de la aplicación correspondiente al dispositivo mientras transmite un título de la aplicación al proveedor de aplicaciones. A continuación, el dispositivo puede analizar la información recibida del proveedor de aplicaciones e identificar la categoría de cada aplicación.

40

45

50

Por otro lado, cuando el usuario selecciona un menú 304a (véase la FIG. 3B) para establecer una contraseña para el nivel de usuario 1, el dispositivo proporciona al usuario una pantalla como se muestra en la FIG. 3D en el que el usuario introduce la contraseña. La FIG. el 3D muestra un ejemplo de introducción de la contraseña en forma de patrón, en el que el usuario arrastra una entrada táctil entre diferentes puntos de la cuadrícula. Cuando el usuario introduce un patrón, formado por el cruce de dos puntos de rejilla 306a y 306b de puntos de rejilla plurales, como contraseña, por ejemplo, el dispositivo registra la contraseña introducida como contraseña con respecto al nivel de

55

usuario 1. Alternativamente, el dispositivo puede estar diseñado para recibir una entrada de contraseña a través de las teclas numéricas del dispositivo.

El procedimiento descrito anteriormente con referencia a las FIGS. 3B a 3D se pueden ejecutar de forma idéntica cuando se establecen detalles relativos a otros niveles de usuario.

5 Volviendo a la FIG. 2, en la etapa 209, el dispositivo determina si el usuario solicita que el dispositivo almacene los detalles de los niveles de usuario y las contraseñas introducidas en las etapas anteriores. De ser así, en la etapa 209, el dispositivo identifica si se incluyen detalles inapropiados en los detalles introducidos por el usuario. Ejemplos de detalles inapropiados son las condiciones en las que: 1) el usuario no establece una contraseña para un determinado nivel de usuario; 2) el usuario no selecciona una aplicación para un determinado nivel de usuario; 3) una contraseña para un nivel de usuario superior es de menor complejidad (o seguridad) que la de un nivel de usuario inferior; 4) las contraseñas de diferentes niveles de usuario son idénticas entre sí, o 5) las aplicaciones seleccionadas relativas a diferentes niveles de usuario son idénticas entre sí. También se pueden predefinir otras condiciones.

15 En cuanto a la tercera condición anterior, es decir, el criterio de complejidad, éste puede estar predefinido, por ejemplo, en función del número de puntos de la cuadrícula en un caso de introducción de una contraseña en forma de patrón. Por ejemplo, un patrón que cruza tres puntos de la cuadrícula tiene una mayor complejidad que un patrón que cruza dos puntos de la cuadrícula. Además, en el caso de la introducción de números como contraseña, el criterio de complejidad se puede basar en el número de números/caracteres a introducir. Por ejemplo, una contraseña que incluya tres números tiene una mayor complejidad que una contraseña que incluya dos números.

20 Como resultado de la determinación de la etapa 209, cuando se determina que existen detalles inapropiados, el dispositivo procede a la etapa 211 y proporciona una pantalla de guía para que el usuario restablezca los detalles relativos al nivel de usuario correspondiente.

25 Por ejemplo, como se muestra en la FIG. 3E, se supone que una contraseña relativa al nivel de usuario 2 se introduce en forma de un patrón que cruza cinco puntos de la cuadrícula, y una contraseña relativa al nivel de usuario 3 se introduce en forma de un patrón que cruza cuatro puntos de la cuadrícula, como se muestra en la FIG. 3F. En este caso, dado que la complejidad de la contraseña de un nivel de usuario de rango alto (nivel de usuario 3) es inferior a la de un nivel de usuario de rango bajo (nivel de usuario 2), como se ha descrito anteriormente, el dispositivo determina que existen detalles inapropiados (y puede mostrar información de texto explicando el motivo) y solicita al usuario que vuelva a introducir una contraseña de cualquier nivel de usuario. La FIG. 3G muestra un ejemplo de un caso en el que el dispositivo permite al usuario introducir de nuevo una contraseña al solicitar al usuario que introduzca de nuevo la contraseña para el nivel de usuario 3.

30 Si en la etapa 209, el dispositivo determina que los detalles inapropiados no existen, el procedimiento pasa a la etapa 213 para almacenar los detalles introducidos por el usuario.

35 Como se ha mencionado anteriormente, se ha descrito a modo de ejemplo la selección de una o más aplicaciones para cada nivel de usuario por medio de la selección de categorías predeterminadas. Como se muestra en la FIG. 3H, sin embargo, ciertas aplicaciones se pueden adaptar a dos o más niveles de usuario. En este caso, cada nivel de usuario puede ser seleccionado de una lista de aplicaciones almacenada en el dispositivo.

Además, el procedimiento de introducción de la contraseña mediante el uso de un patrón se ha descrito anteriormente. Sin embargo, se puede introducir una contraseña mediante el uso de números en lugar de patrones.

40 Como se ha mencionado anteriormente, se ha descrito un procedimiento de configuración de los detalles para cada nivel de usuario de acuerdo con una realización de la presente invención con referencia a las FIGS. 2 y 3. La introducción posterior de una contraseña correcta para un nivel de usuario correspondiente es, por supuesto, necesaria para liberar un bloqueo para ese nivel, como se describe en relación con la FIG. 1B. Liberar un bloqueo en consideración a un nivel de usuario para una contraseña correspondiente significa que el bloqueo puede ser liberado para que un usuario pueda utilizar sólo las aplicaciones registradas en un nivel de usuario correspondiente. Por ejemplo, como se muestra en la FIG. 4A, se supone que una categoría de "navegador web" para un nivel de usuario 1 está registrada como una categoría de una aplicación disponible y una categoría de "telefonía" para un nivel de usuario 2 está registrada como una categoría de una aplicación disponible. Cuando se introduce una contraseña para el nivel de usuario 2, un dispositivo puede mostrar un icono 404 como se muestra en la FIG. 4B de la aplicación correspondiente a la categoría de "telefonía" que se registra en el nivel de usuario 2. En una implementación, también se muestran y se ponen a disposición los iconos de las aplicaciones para los niveles de usuario de menor rango. Por ejemplo, como en la FIG. 4A, se registra una categoría de "navegador web" y una categoría de "telefonía" para los niveles de usuario 1 y 2, respectivamente. Cuando se introduce una contraseña para el nivel de usuario 2, entonces, como se muestra en la FIG. 4C, un dispositivo puede mostrar tanto un icono 402 de la aplicación correspondiente a la categoría de "navegador web" registrada en el nivel de usuario 1 como un icono 404 de la aplicación correspondiente a la categoría de "telefonía" registrada en el nivel de usuario 2.

De acuerdo con otra realización de la presente invención, la liberación de un bloqueo en consideración de un nivel de usuario para una contraseña correspondiente significa que un dispositivo muestra todos los iconos de las

5 aplicaciones almacenadas en el mismo, pero sólo permite a un usuario utilizar las aplicaciones registradas en el nivel de usuario para una contraseña correspondiente, o las aplicaciones en ese nivel de usuario y niveles de usuario de rango inferior. Por ejemplo, cuando la contraseña introducida identifica a un usuario de nivel 2, el dispositivo muestra todos los iconos de las aplicaciones almacenadas en él, como se muestra en la FIG. 4D, pero no permite al usuario ejecutar una aplicación 406 registrada para un nivel de usuario 3.

10 De acuerdo con otra implementación, la liberación del bloqueo tras la introducción de la contraseña se implementa mostrando todos los iconos de las aplicaciones almacenadas en el dispositivo; sin embargo, los iconos de las aplicaciones registradas en el nivel de usuario para la contraseña correspondiente se muestran en un estado diferente al de los iconos de las aplicaciones restantes. Por ejemplo, las aplicaciones que no están disponibles debido a que el nivel de usuario actual es demasiado bajo se muestran de forma diferenciada. Ejemplos de este enfoque se ilustran en la FIG. 4E, en la que se utiliza una opacidad diferente para los iconos de las aplicaciones no disponibles ("apps"); y en la FIG. 4F, en la que los iconos de las aplicaciones no disponibles se sustituyen por imágenes predeterminadas 412 y en la FIG. 4G, en la que las imágenes predeterminadas 414 se superponen con los iconos de las aplicaciones no disponibles.

15 Además, en el caso de que sólo se registre una aplicación en un nivel de usuario para una contraseña correspondiente, después de introducir la contraseña correcta, la aplicación se puede ejecutar inmediatamente. Por ejemplo, cuando sólo una aplicación, que pertenece a una categoría de "navegador web", está registrada en un nivel de usuario 1 y una contraseña introducida por un usuario para liberar un bloqueo coincide con el nivel de usuario 1, un dispositivo puede ejecutar la aplicación correspondiente inmediatamente, como se muestra en la FIG. 4H.

20 Se han descrito procedimientos de liberación de bloqueo de acuerdo con las realizaciones de la presente invención con referencia a la FIG. 4A a 4H. Los niveles de usuario de cada aplicación se pueden modificar posteriormente. Por ejemplo, como se describe anteriormente con referencia a la FIG. 3C, al seleccionar una categoría de aplicaciones y una aplicación adaptada a cada nivel de usuario, un usuario puede designar por separado y configurar las respectivas aplicaciones para que pertenezcan a niveles de usuario diferentes entre sí, aunque las aplicaciones estén incluidas en la misma categoría. En lo sucesivo, los procesos de cambio de los niveles de usuario para cada aplicación se describirán con referencia a las FIGS. 5 a 6.

25 La FIG. 5 es un diagrama de flujo que ilustra un ejemplo de procedimiento de cambio de niveles de usuario 500 para cada aplicación de acuerdo con una realización de la presente invención.

30 Al recibir una solicitud de usuario en la etapa 501 para un cambio de los niveles de usuario, es decir, una solicitud para cambiar los niveles de usuario para cada aplicación, un dispositivo procede a la etapa 503 y recibe una contraseña introducida por el usuario.

35 El dispositivo identifica si la contraseña introducida por el usuario coincide con un nivel de usuario de rango superior en la etapa 505. De no ser así, los niveles de usuario no son modificables y el dispositivo permanece en modo de espera de la contraseña correcta de rango superior (indicada por la línea de flujo de vuelta a la consulta 505). Si la contraseña introducida coincide con el nivel de usuario de rango superior, el dispositivo procede a la etapa 507 en la que el dispositivo permite al usuario, que pertenece al nivel de usuario de rango superior, cambiar el nivel de usuario para cada aplicación.

40 El dispositivo proporciona una pantalla guía para que el usuario pueda cambiar el nivel de usuario para cada aplicación, en la etapa 507. Por ejemplo, el dispositivo puede mostrar una lista de las aplicaciones registradas en cada nivel de usuario, como se muestra en la FIG. 6A. En consecuencia, el usuario puede seleccionar cualquiera de las aplicaciones y cambiar el nivel de usuario para la aplicación correspondiente, como se muestra en la FIG. 6B. De acuerdo con las realizaciones de la presente invención, el dispositivo puede mostrar un nivel de cada aplicación en forma de una imagen 602 (véase la FIG. 6C), y el usuario puede cambiar el nivel de usuario para cada aplicación deslizando la imagen correspondiente 602 (por ejemplo, al alargar el indicador de nivel, como indica la línea de flecha). Cuando el nivel de usuario para cualquiera de las aplicaciones se cambia de un nivel de usuario 2 a un nivel de usuario 3 como se muestra en las FIGS. 6A a 6C, el dispositivo registra la aplicación correspondiente como aplicación disponible en el nivel de usuario 3.

45 Una vez que el usuario está satisfecho con los cambios a nivel de usuario, el usuario puede solicitar que los cambios sean almacenados a través de un comando de entrada adecuado en la etapa 509, con lo cual el dispositivo finalmente almacena los cambios en la etapa 511.

50 Una realización en la que sólo el usuario perteneciente al nivel de usuario de rango superior cambia el nivel de usuario para cada aplicación, se ha descrito con referencia a la FIG. 5. En una realización alternativa, los usuarios que no pertenecen al nivel de usuario de rango superior pueden cambiar el nivel de usuario para cada aplicación.

55 La forma de cambiar el nivel de usuario para cada aplicación se ha descrito con referencia a la FIG. 5. La técnica de esta realización se puede aplicar de forma idéntica a un caso de cambio de las aplicaciones disponibles para cada nivel de usuario, o a un caso de cambio de la contraseña para cada nivel de usuario. Es decir, cuando el dispositivo recibe una solicitud del usuario, el dispositivo puede proporcionar una pantalla de guía para que un usuario cambie los detalles de cada nivel de usuario, por ejemplo las contraseñas y las aplicaciones disponibles, a través de la

pantalla de guía, como se muestra en la FIG. 6D.

Con referencia a la FIG. 6D, el dispositivo proporciona un menú para que el usuario añada o elimine un nivel de usuario a través del menú. En una realización, cuando se elimina cualquier nivel de usuario, el dispositivo puede registrar las aplicaciones, que están incluidas en el nivel de usuario que se va a eliminar, en el nivel de usuario de menor rango entre los niveles de usuario superiores al del nivel de usuario eliminado. Por ejemplo, cuando se elimina un nivel de usuario 1, las aplicaciones incluidas en un nivel de usuario 1 se pueden registrar en un nivel de usuario 2 que es el nivel de usuario de menor rango de un nivel de usuario 2 y un nivel de usuario 3 que son de mayor nivel que el nivel de usuario 1. De acuerdo con esta realización, en un estado en el que los niveles de usuario 1 a 3 están configurados, cuando el nivel de usuario 1 se elimina, el nivel de usuario 2 se puede cambiar al nivel de usuario 1, y el nivel de usuario 3 se puede cambiar al nivel de usuario 2.

Los procedimientos para cambiar varios detalles relacionados con el nivel de usuario de acuerdo con las realizaciones se han descrito con referencia a las FIGS. 5 y 6. Después de establecer los niveles de usuario y de descargar una nueva aplicación, es deseable establecer automáticamente un nivel de usuario para la nueva aplicación. En lo sucesivo, se describirán los procedimientos de configuración automática de los niveles de usuario para una aplicación descargada..

La FIG. 7 es un diagrama de flujo que ilustra un procedimiento de ejemplo, 700, de establecimiento automático de niveles de usuario para una nueva aplicación descargada ("app") de acuerdo con una realización de la presente invención. En la realización que se describirá a continuación con referencia a la FIG. 7, se supone que la selección de una aplicación para cada nivel de usuario se puede lograr por medio de la selección de una categoría de la aplicación, como se describe con referencia a la FIG. 3C.

Un dispositivo identifica si se ha descargado una aplicación en la etapa 701. Si es así, el dispositivo identifica una categoría de la aplicación descargada en la etapa 703. En la presente memoria, la categoría de la aplicación descargada puede ser identificada de diferentes maneras. Por ejemplo, el dispositivo analiza los metadatos de la aplicación descargada para identificar la categoría de la misma. En otro enfoque, como se muestra en la FIG. 8, el dispositivo puede analizar una página vinculada a una página de descarga de la aplicación correspondiente para identificar la categoría de la aplicación. Es decir, el dispositivo puede analizar los metadatos, la página de descarga o similares y analizar las palabras insertadas en una determinada etiqueta, a fin de identificar la categoría de la aplicación. Por ejemplo, el dispositivo puede analizar los metadatos o la página de descarga de la aplicación descargada y analizar un valor de propiedad de la etiqueta determinada para identificar la categoría de la aplicación. Si el valor de la propiedad de la etiqueta determinada es categoría 802 y juego 804, el dispositivo determina que la categoría de la aplicación es "juego". En otro ejemplo, el dispositivo transmite información de la aplicación, por ejemplo el título de la misma, a un proveedor de aplicaciones, al tiempo que solicita al proveedor de aplicaciones que transmita al dispositivo información sobre la categoría de la aplicación correspondiente. A continuación, el dispositivo puede analizar la información recibida del proveedor de la aplicación para identificar la categoría de la misma.

Volviendo a la FIG. 7, el dispositivo registra la aplicación descargada como una aplicación disponible en un nivel de usuario que incluye la categoría identificada.

Los procedimientos de configuración de contraseñas para niveles de usuario plurales respectivamente y de liberación de un bloqueo se han descrito con referencia a las FIGS. 1 a 8. En lo sucesivo, la configuración de un dispositivo al que se aplican las realizaciones de la presente invención se describirá con referencia a la FIG. 9.

La FIG. 9 es un diagrama de bloques que ilustra un dispositivo electrónico 900 al que se pueden aplicar las realizaciones de la presente invención. El dispositivo 900 lleva a cabo convenientemente las dos funciones de un dispositivo para establecer una contraseña y un dispositivo para liberar un bloqueo. Cabe señalar, que al menos uno de los elementos estructurales de acuerdo con la realización mostrada en la FIG. 9 se pueden omitir.

El dispositivo 900 incluye un controlador 910, una unidad de entrada 920, una unidad de salida 930, una memoria 940 y una unidad de comunicación 950.

El controlador 910 controla las diversas operaciones descritas anteriormente en relación con las FIGS. 1 a 8. De este modo, en el momento de establecer una contraseña, el controlador 910 permite a un usuario seleccionar una o más aplicaciones para ser utilizadas en cada nivel de usuario a través de la unidad de entrada 920 con relación a una pluralidad de niveles de usuario que tienen respectivamente una autoridad para utilizar una o más aplicaciones, y recibe una contraseña para ser utilizada para liberar un bloqueo en cada nivel de usuario a través de la unidad de entrada 920. En este momento, el controlador 910 permite a un usuario seleccionar al menos una categoría entre las múltiples categorías establecidas para una aplicación. Como resultado, el usuario puede seleccionar al menos una aplicación para ser utilizada en cada nivel de usuario. Además, el controlador 910 permite al usuario seleccionar individualmente al menos una aplicación a utilizar en cada nivel de usuario de una lista de las aplicaciones almacenadas en la memoria 940.

El controlador 910 registra la contraseña de entrada para cada nivel de usuario y la aplicación seleccionada para el nivel de usuario correspondiente. A fin de registrar la contraseña y la aplicación, el controlador 910 puede mostrar

una pantalla guía en la unidad de salida 930 para que el usuario seleccione e introduzca los detalles de cada nivel de usuario, es decir, la contraseña y la aplicación.

5 Antes de que el controlador 910 permita al usuario seleccionar al menos una aplicación a utilizar en cada nivel de usuario, por otro lado, recibe el número de los niveles de usuario a través de la unidad de entrada 920. En consecuencia, el controlador 910 muestra la pantalla guía en la unidad de salida 930 para que el usuario seleccione el número de los niveles de usuario.

10 En los casos en que la complejidad de la contraseña de entrada para cualquier nivel de usuario es menor que la de una contraseña para un nivel de usuario de rango bajo, la complejidad de la contraseña de entrada para cualquier nivel de usuario es mayor que la de una contraseña para un nivel de usuario de rango alto, o la complejidad de la contraseña de entrada para cualquier nivel de usuario es idéntica a la de una contraseña para otro nivel de usuario, el controlador 910 recibe una contraseña para el nivel de usuario correspondiente introducida por el usuario de nuevo. En consecuencia, el controlador 910 muestra la pantalla guía en la salida 930 para que el usuario introduzca de nuevo una contraseña para el nivel de usuario correspondiente.

15 Cuando se descarga al menos una aplicación, el controlador 910 identifica una categoría de la aplicación descargada y registra la aplicación descargada como una aplicación a utilizar en un nivel de usuario al que pertenece la categoría identificada. En este momento, el controlador 910 analiza al menos uno de los metadatos y la página de descarga de la aplicación correspondiente y una página vinculada a la página de descarga de la aplicación correspondiente e identifica la categoría de la aplicación descargada.

20 Al recibir una solicitud de cambio de nivel de usuario de al menos una aplicación, el controlador 910 registra la aplicación correspondiente como aplicación a utilizar en el nivel de usuario que se solicita cambiar. En consecuencia, el controlador 910 muestra una pantalla guía en la unidad de salida 930 para que el usuario cambie un nivel de usuario para cada aplicación.

25 Al recibir una solicitud de eliminación de un nivel de usuario, el controlador 910 registra la aplicación registrada en el nivel de usuario correspondiente como una aplicación que se utilizará en el nivel de usuario de menor rango entre los niveles de usuario de alto rango del nivel de usuario que se solicita eliminar. En consecuencia, el controlador 910 muestra una pantalla guía en la unidad de salida 930 para que el usuario pueda eliminar o añadir un nivel de usuario.

30 Al liberar un bloqueo, el controlador 910 recibe una contraseña para liberar el bloqueo a través de la unidad de entrada 920, y compara la contraseña introducida y las contraseñas almacenadas en la memoria 940. A continuación, el controlador 910 libera el bloqueo teniendo en cuenta un nivel de usuario para la contraseña correspondiente en el que la contraseña introducida es idéntica a cualquiera de las contraseñas almacenadas.

35 Al liberar el bloqueo, el controlador 910 puede ordenar la visualización de los iconos de las aplicaciones a utilizar en el nivel de usuario correspondiente a la contraseña de entrada en la unidad de salida 930. Los iconos de las aplicaciones que no estarán disponibles en el nivel de usuario correspondiente se pueden mostrar en un estado diferente al de los iconos de las aplicaciones que se utilizarán en el nivel de usuario correspondiente. Por ejemplo, el controlador 910 ordena la visualización de los iconos de las aplicaciones que no están disponibles en el nivel de usuario correspondiente en un estado diferente al de los iconos de las aplicaciones que se utilizan en el nivel de usuario correspondiente, de cualquier manera, al aplicar diferentes opacidades a los iconos de las aplicaciones que se utilizan en el nivel de usuario correspondiente y a los iconos de las aplicaciones que no están disponibles en el nivel de usuario correspondiente, cambiar los iconos de las aplicaciones no disponibles a una imagen predeterminada, y superponer la imagen predeterminada sobre los iconos de las aplicaciones no disponibles.

Además, el controlador 910 puede no mostrar los iconos de las aplicaciones que no estén disponibles en el nivel de usuario correspondiente.

45 Por otro lado, cuando sólo hay una aplicación disponible en el nivel de usuario correspondiente a la contraseña introducida por el usuario, el controlador 910 puede llevar a cabo una aplicación inmediatamente.

La unidad de entrada 920 transmite la información introducida por el usuario al controlador 910.

La unidad de salida 930 muestra diversas pantallas de guía bajo el control de la unidad 910 de control.

La unidad de entrada 920 y la unidad de salida 930 incluyen preferentemente una pantalla táctil.

La memoria 940 almacena detalles para cada nivel de usuario.

50 La unidad de comunicación 950 se comunica con dispositivos externos, preferentemente con la capacidad de utilizar diferentes mecanismos de comunicación.

Se apreciará que las realizaciones de la presente invención se pueden implementar en forma de hardware, software o una combinación de hardware y software. Cuando la realización de la presente invención se puede implementar en un software, éste puede ser ejecutado por uno o más procesadores que utilicen diversos sistemas operativos o

plataformas. Además, el software puede programarse mediante el uso de cualquiera de una variedad de lenguajes de programación adecuados, y también se puede compilar en códigos de ensamblaje o códigos intermedios que se pueden llevar a cabo en un marco o una máquina virtual.

5 Además, las realizaciones de la presente invención se pueden implementar por medio de un medio de almacenamiento legible por el procesador, por ejemplo una memoria, un disquete, un disco duro, un disco compacto, un disco óptico o una cinta magnética, adecuados para almacenar un programa o programas que incluyan instrucciones para implementar las realizaciones ejemplares de la presente invención.

10 Si bien la presente invención se muestra y se describe con referencia a determinadas realizaciones ejemplares de la misma, aquellos expertos en la técnica comprenderán que diversos cambios en la forma y los detalles se pueden llevar a cabo en la misma sin apartarse del ámbito de la invención como se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo (900) electrónico que comprende:
 - una memoria (940);
 - una pantalla táctil (920, 930); y
 - un procesador (910) configurado para:
 - almacenar, a través de la memoria, una contraseña para permitir el cambio de detalles, incluidos los detalles de las aplicaciones disponibles relacionadas con un nivel de usuario, en las que el nivel de usuario está asociado a una autoridad para acceder a las aplicaciones;
 - recibir una solicitud de usuario (501) para cambiar los detalles, incluidos los detalles de las aplicaciones disponibles relacionadas con un nivel de usuario;
 - en respuesta a la solicitud recibida del usuario para cambiar los detalles, incluidos los detalles de las aplicaciones disponibles relacionadas con un nivel de usuario, controlar la pantalla táctil para que muestre una pantalla de introducción de la contraseña;
 - recibir una entrada de contraseña (503) a través de la pantalla de entrada de contraseña;
 - si (505) la contraseña recibida corresponde a la contraseña almacenada, proporcionar (507) en la pantalla táctil al menos una pantalla de guía para cambiar los detalles, incluidos los detalles de las aplicaciones disponibles relacionadas con el nivel de usuario, la al menos una pantalla de guía que comprende una lista de las aplicaciones para cada una de las cuales se puede cambiar una opción de restricción de acceso;
 - si se modifican los detalles, incluidos los detalles de las aplicaciones disponibles relacionadas con el nivel de usuario, registrar (511) la información de configuración de acceso modificada en la memoria; y
 - controlar la pantalla táctil para que muestre los iconos de las aplicaciones no disponibles para el nivel de usuario de forma que se distingan de los iconos de las aplicaciones autorizadas para el acceso.

2. El dispositivo electrónico de la reivindicación 1, en el que el procesador está configurado además para:
 - mostrar una lista de una pluralidad de categorías como la al menos una pantalla guía, en la que al menos una aplicación corresponde a una de entre la pluralidad de categorías; y
 - si se selecciona una categoría específica de entre la pluralidad de categorías, establecer al menos una aplicación perteneciente a la categoría específica seleccionada de acuerdo con el nivel de usuario.

3. El dispositivo electrónico de la reivindicación 2, que además comprende una unidad de comunicación:
 - en el que el procesador está configurado además para:
 - descargar, a través de la unidad de comunicación, al menos una aplicación;
 - identificar una categoría de la al menos una aplicación descargada; y
 - establecer la descarga de al menos una aplicación con un mismo nivel de usuario que la categoría identificada.

4. El dispositivo electrónico de la reivindicación 3, en el que el procesador está configurado además para analizar al menos uno de los metadatos, una página de descarga y una página vinculada a la página de descarga de la al menos una aplicación descargada con el fin de identificar la categoría de la al menos una aplicación descargada.

5. El dispositivo electrónico de la reivindicación 1, en el que la al menos una aplicación funciona de forma diferente de acuerdo con el nivel de usuario.

6. El dispositivo electrónico de la reivindicación 5, en el que la al menos una aplicación comprende un reproductor de música, y el reproductor de música evita la reproducción de canciones clasificadas para un oyente maduro de acuerdo con el nivel de usuario cuando el dispositivo electrónico funciona en un nivel infantil.

7. El dispositivo electrónico de la reivindicación 1, en el que los iconos de las aplicaciones no disponibles se muestran por medio del uso de una opacidad diferente.

8. El dispositivo electrónico de la reivindicación 1, en el que se utilizan imágenes predeterminadas para los iconos de las aplicaciones no disponibles en una posición correspondiente a los iconos de las aplicaciones no disponibles.

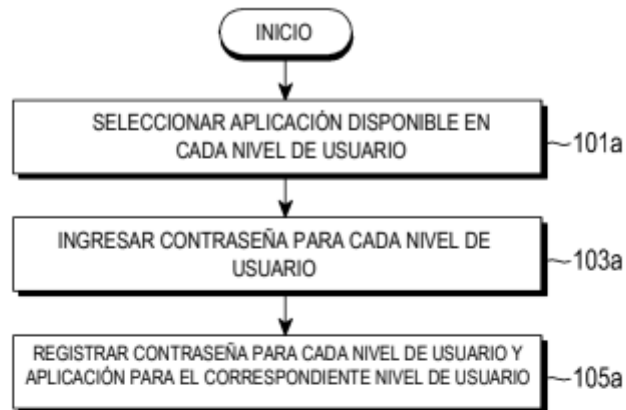


FIG.1A

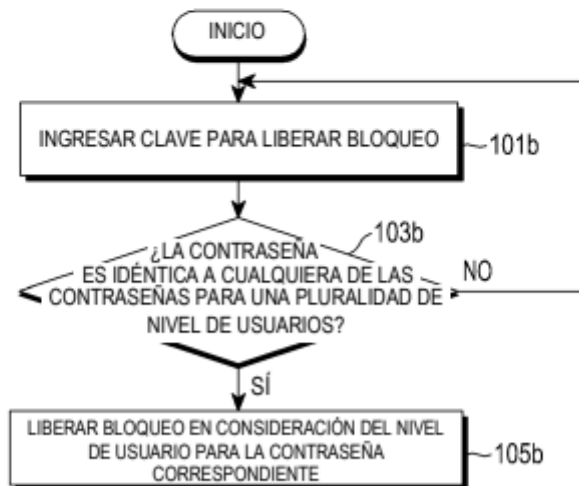


FIG.1B

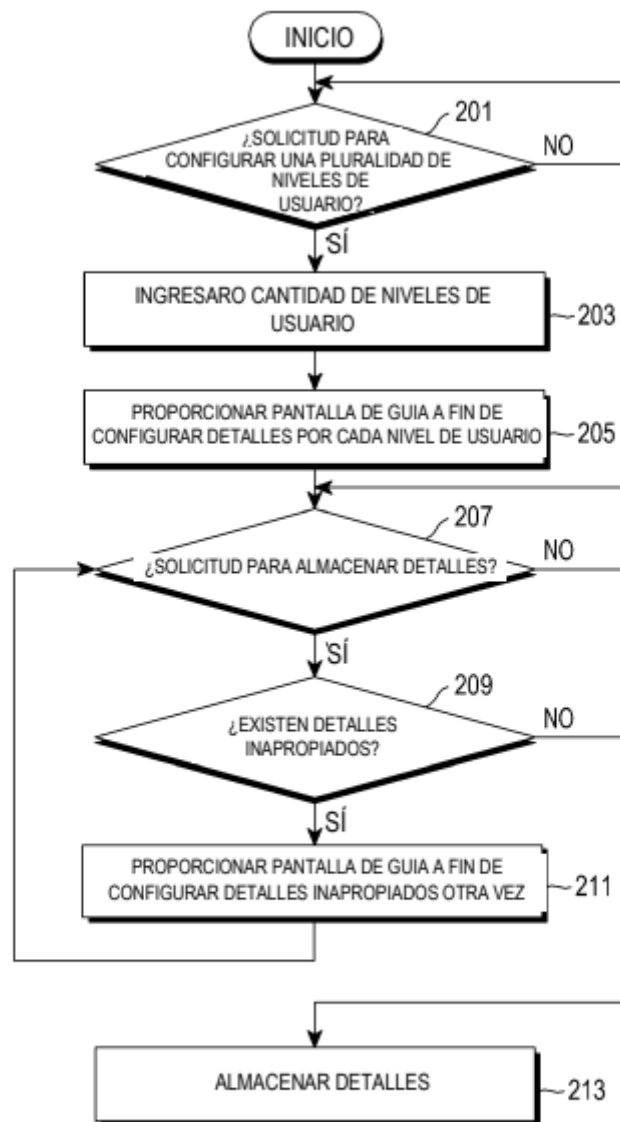


FIG.2



FIG.3A

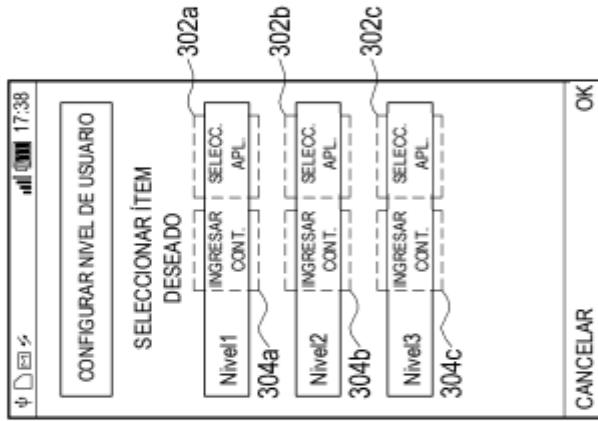


FIG.3B

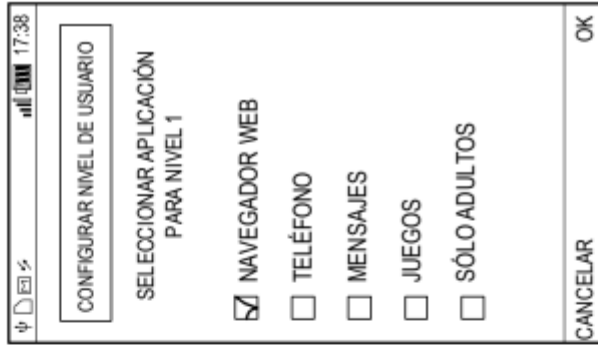


FIG.3C

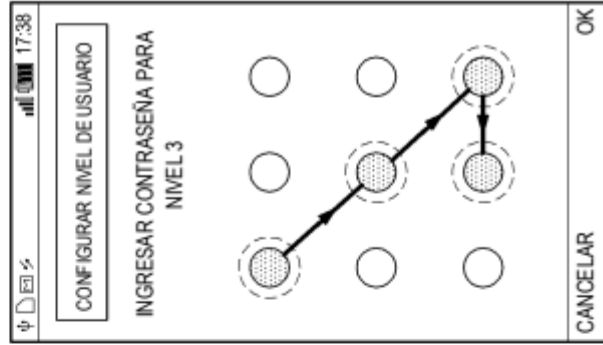


FIG.3D

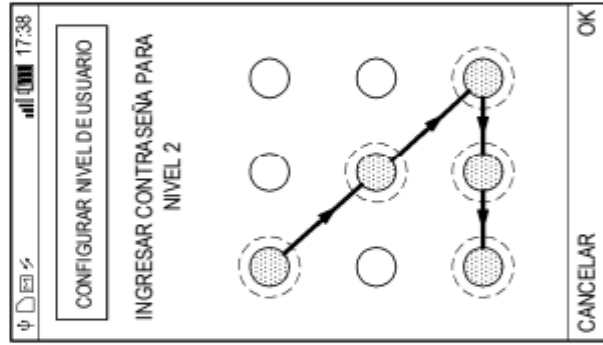


FIG.3E

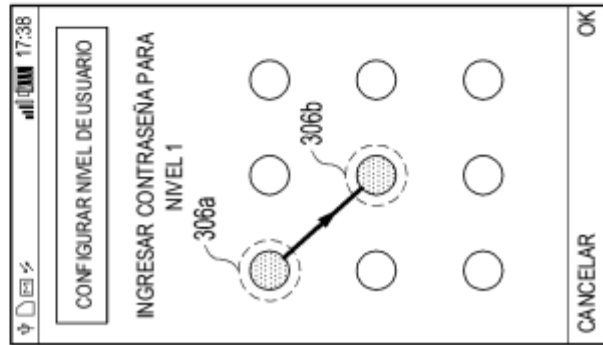


FIG.3F

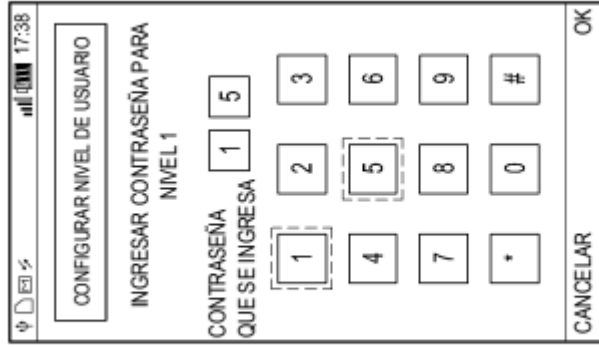


FIG.3I

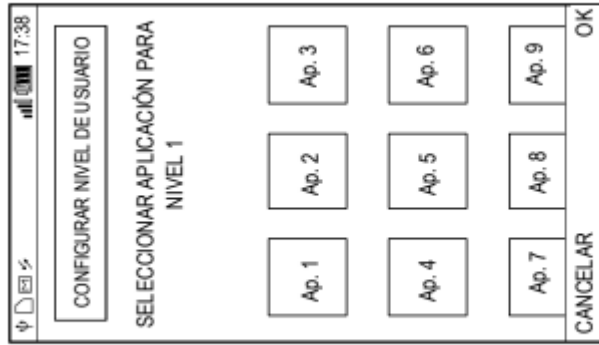


FIG.3H

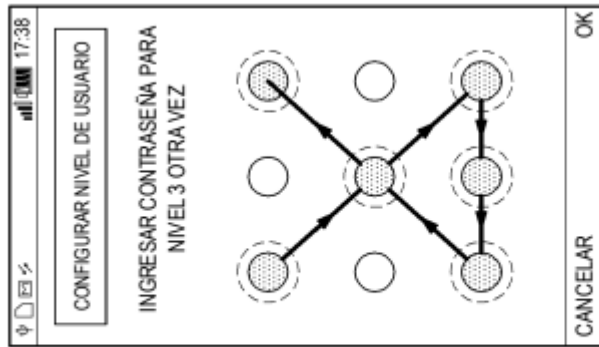


FIG.3G

| NIVEL DE USUARIO | CATEGORÍA |
|------------------|--------------------------------|
| NIVEL 1 | NAVEGADOR WEB |
| NIVEL 2 | TELÉFONO |
| NIVEL 3 | MENSAJES, JUEGOS, SÓLO ADULTOS |

FIG.4A

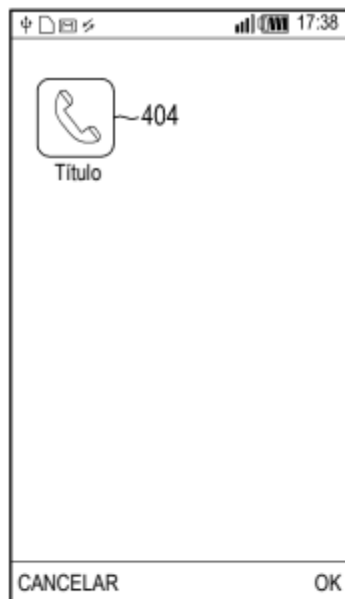


FIG.4B

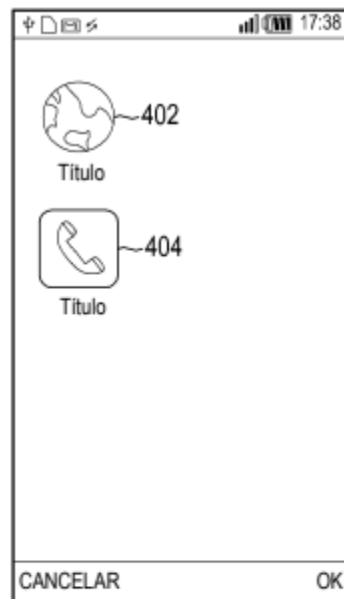


FIG.4C



FIG. 4D



FIG. 4E

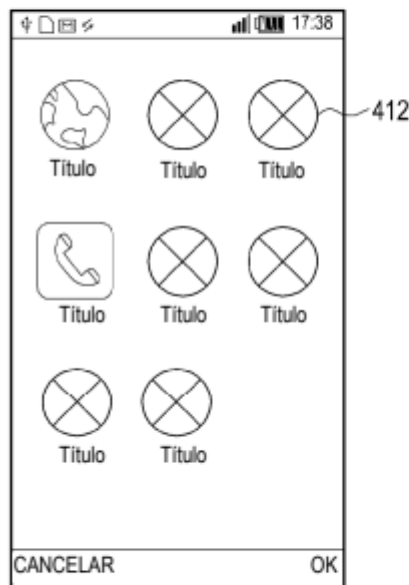


FIG. 4F



FIG. 4G

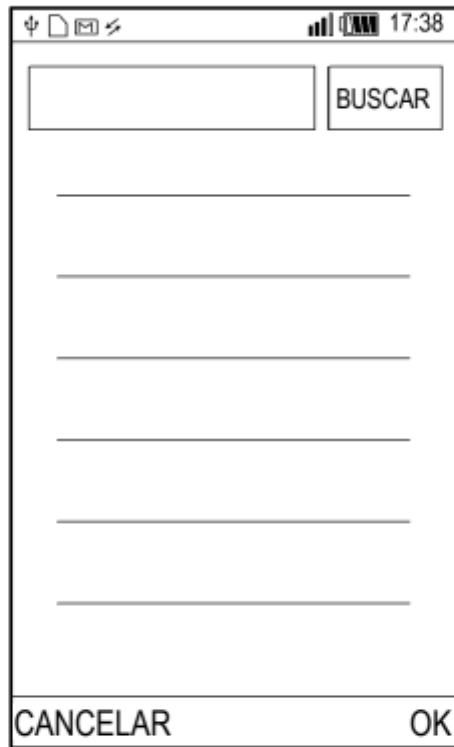


FIG.4H

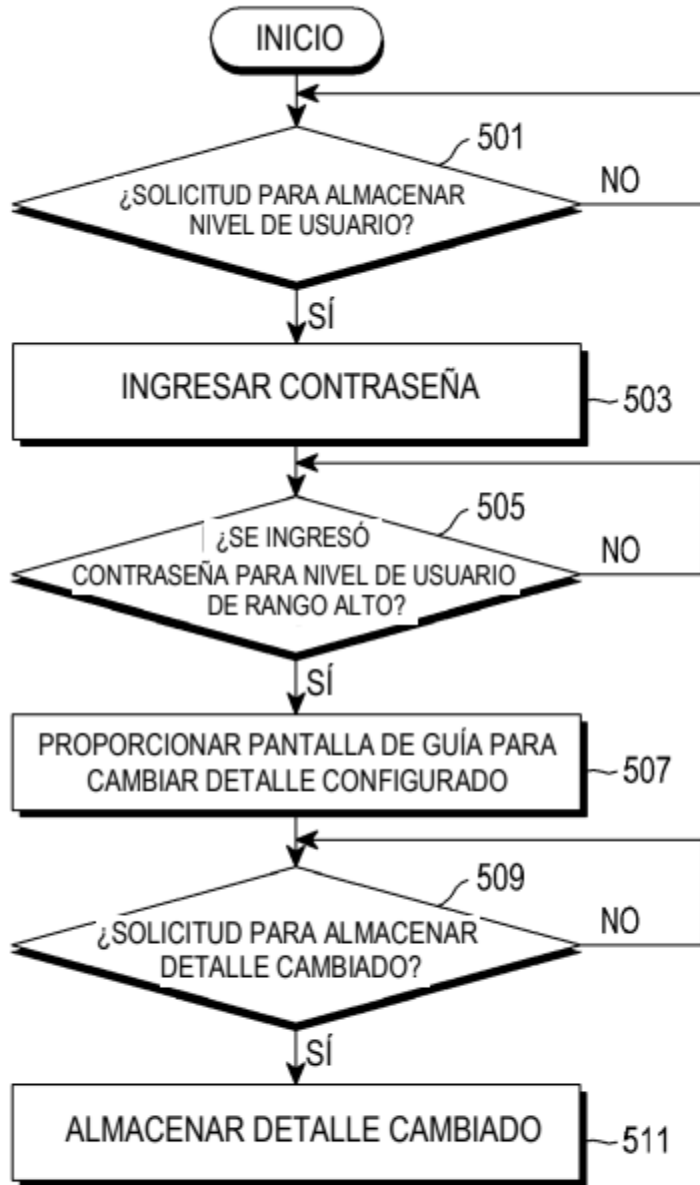


FIG.5

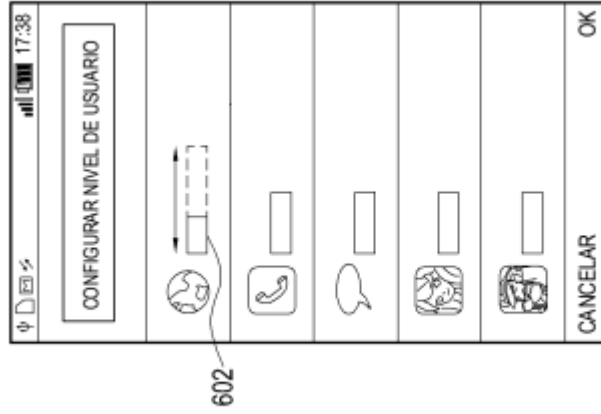


FIG.6C

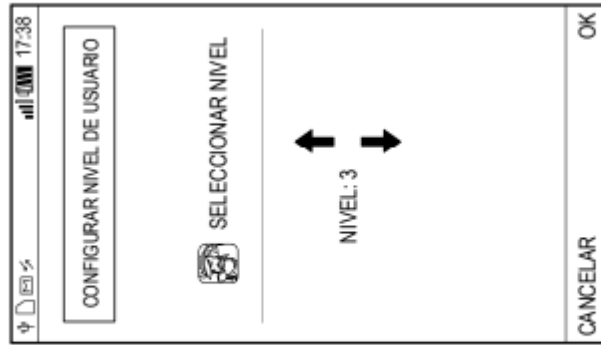


FIG.6B

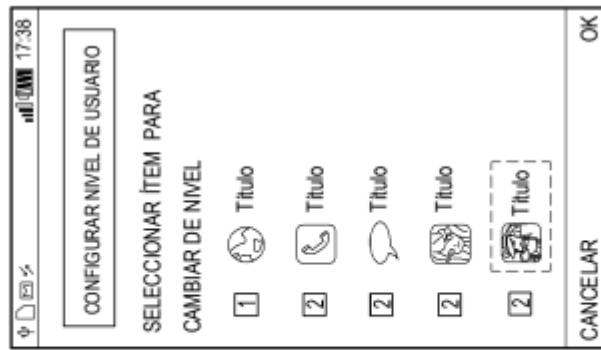


FIG.6A



FIG.6D



FIG.7

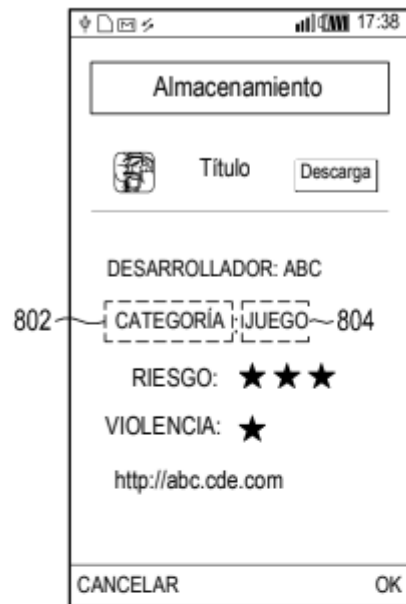


FIG.8

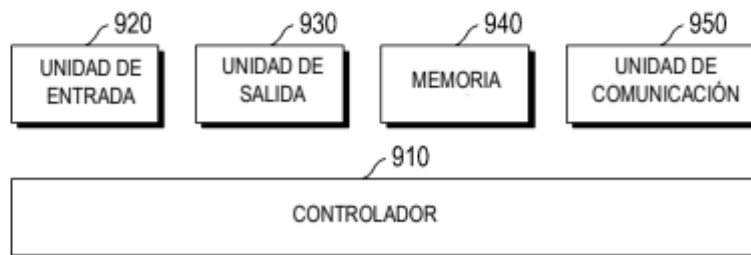


FIG.9