(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 806 629**

(51) Int. CI.:

G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.04.2016 PCT/CN2016/080440**

(87) Fecha y número de publicación internacional: **01.12.2016 WO16188297**

(96) Fecha de presentación y número de la solicitud europea: **28.04.2016 E 16799186 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3306505**

(54) Título: **Método y dispositivo de entrada de información**

(30) Prioridad:

28.05.2015 CN 201510282846

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2021

(73) Titular/es:

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

(72) Inventor/es:

HE, YONG

(74) Agente/Representante:

VIDAL GONZÁLEZ, Maria Ester

DESCRIPCIÓN

Método y dispositivo de entrada de información

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de procesamiento de datos y en particular, a un método y aparato de entrada de información.

Antecedentes Técnicos

Con el desarrollo de tecnologías de comunicación móvil, los usuarios a menudo necesitan ingresar información en dispositivos móviles. Especialmente cuando la información se ingresa en un teléfono móvil, el tamaño de un teclado físico o un teclado virtual es relativamente pequeño debido al tamaño limitado del teléfono móvil, de modo que es fácil para un usuario ingresar información incorrectamente. Por ejemplo, el usuario tiene la intención de ingresar una letra a, pero en realidad ingresa una letra adyacente a la letra a, como la s.

La publicación de patente de los Estados Unidos US 2008/0066167 A1 a Andri para "Acceso basado en contraseña que incluye error permitido", publicado el 13 de marzo de 2009, divulga un sistema que permite a un usuario cliente acceder a información o servicios seguros utilizando un código de seguridad, incluso cuando el código de seguridad proporcionado por el usuario del cliente incluye uno o más errores. Un administrador del sistema puede seleccionar un nivel de tolerancia de error basado en un nivel mínimo de seguridad prescrito y el código de seguridad seleccionado por el usuario del cliente. La publicación afirma que la aplicación de la asignación de errores puede reducir la cantidad de veces que se le niega a un usuario cliente el acceso a la información o servicios solicitados debido a una entrada de código de seguridad incorrecta o mal escrita, al tiempo que garantiza que se conserve el nivel mínimo de seguridad prescrito.

Resumen de la invención

La invención se define en las reivindicaciones adjuntas. La presente solicitud tiene como objetivo resolver uno de los problemas técnicos en la técnica relacionada, al menos en cierta medida.

Por lo tanto, un objetivo de la presente aplicación es proponer un método de entrada de información, que puede reducir los errores de entrada causados por un teclado pequeño y mejorar los efectos de entrada.

Otro objetivo de la presente solicitud es proponer un aparato de entrada de información.

Los aspectos y ventajas adicionales de la presente solicitud se proporcionarán parcialmente en la siguiente descripción, y se harán parcialmente evidentes a partir de la siguiente descripción, o se conocerán a través de las prácticas de la presente aplicación.

Breve descripción de las figuras

Los aspectos y ventajas anteriores y/o adicionales de la presente solicitud se harán evidentes y fácilmente comprensibles a partir de la descripción de realizaciones con referencia a las figuras que se acompañan como sigue, en donde:

La Figura 1 es un diagrama de flujo esquemático de un método de entrada de información de acuerdo con una realización de la presente solicitud;
La Figura 2 es un diagrama de flujo esquemático de un método de entrada de información de acuerdo con otra realización de la presente solicitud;
La Figura 3 es un diagrama de flujo esquemático de un método de entrada de información de acuerdo con otra realización de la presente solicitud;
La Figura 4 es un diagrama de flujo esquemático de un método de entrada de información de acuerdo con otra realización de la presente solicitud;
La Figura 5 es un diagrama estructural esquemático de un aparato de entrada de información de acuerdo con otra realización de la presente solicitud; y
La Figura 6 es un diagrama estructural esquemático de un aparato de entrada de información de acuerdo con otra realización de la presente solicitud.

Descripción detallada

Las realizaciones de la presente solicitud se describirán en detalle a continuación, se muestran ejemplos de las realizaciones en las figuras adjuntas, donde los números de referencia idénticos o similares representan módulos o módulos idénticos o similares que tienen funciones idénticas o similares a lo largo del texto. Las realizaciones

descritas a continuación con referencia a las figuras adjuntas son ejemplares y solo pretenden explicar la presente solicitud, y no pueden interpretarse como limitantes de la presente solicitud.

La Figura 1 es un diagrama de flujo esquemático de un método de entrada de información de acuerdo con una realización de la presente solicitud, el método incluye:
S11. La información almacenada previamente se adquiere, la información almacenada previamente incluye la primera información de texto sin cifrar o la primera información cifrada, la primera información incluye la información establecida y la información asociada generada de acuerdo con la información establecida.

El método de esta realización puede usarse para la verificación de información en varios escenarios, por ejemplo, para verificación de contraseña, verificación de número de tarjeta de identificación, verificación de número de tarjeta bancaria, verificación de número de teléfono móvil, etc. En esta realización, la verificación de contraseña se toma como un ejemplo.

Antes de la verificación de la contraseña, un usuario puede preestablecer una contraseña. Por ejemplo, la contraseña se establece como x. Puede entenderse que la contraseña x establecida por el usuario puede incluir uno o más elementos de información y cada elemento de información puede ser un número, una letra o similar.

Además, tomando como ejemplo que la contraseña se almacena en un terminal de teléfono móvil, la contraseña puede almacenarse en texto sin cifrar en el terminal de teléfono móvil, por ejemplo, directamente almacenado como x. O, para mejorar la seguridad, una contraseña de texto sin cifrar se cifra antes de almacenarse, por ejemplo, una x cifrada almacenada en el terminal del teléfono móvil. Se puede entender que existen varios algoritmos de cifrado, que, por ejemplo, es específicamente un algoritmo Hash. En esta realización, se toma como ejemplo una contraseña cifrada de Hash almacenada en el terminal del teléfono móvil. Suponga que x se representa como H(x) después de realizar el cifrado Hash.

En la técnica anterior, la información almacenada previamente es H(x) como máximo y la verificación fallará si lo que ingresa el usuario no es x.

En esta realización, no solo se puede almacenar H(x), sino que también se puede obtener información asociada de acuerdo con x y la información obtenida después de que se realiza el cifrado Hash en la información asociada se almacena adicionalmente en el terminal del teléfono móvil.

Específicamente, con referencia a la Figura 2, el método de esta realización puede incluir, además:
S10. La información asociada se genera de acuerdo con la información establecida.

Opcionalmente, la etapa de generar información asociada de acuerdo con la información establecida incluye:

seleccionar aleatoriamente un elemento de información de la información establecida y adquirir un nuevo elemento de información correspondiente al elemento de información seleccionado, en donde la distancia entre las posiciones del nuevo elemento de información y el elemento de información seleccionado en un teclado está en un rango preestablecido; y

reemplazar el elemento de información seleccionado en la información establecida con el nuevo elemento de información para obtener la información asociada.

Por ejemplo, un elemento de la contraseña x establecido por el usuario es a, luego se selecciona un carácter a una pequeña distancia con un teclado virtual activado o un teclado físico como un nuevo carácter correspondiente a a. Suponiendo que el nuevo carácter se representa por una a', a' se usa para colocar a para componer una nueva contraseña x'. La nueva contraseña x' es información asociada de x. Después de realizar el cifrado de Hash, la información asociada cifrada puede representarse como: H(x'), H(x")..., y esta secuencia se registra como H'. Específicamente, por ejemplo, suponiendo que x es abcd y el carácter a una pequeña distancia con a incluye a', la información asociada de x incluye a'bcd. Además, suponiendo que el carácter a una pequeña distancia con un adicional incluye un a", la información asociada de x incluye además un a"bcd. Además, suponiendo que un carácter a una pequeña distancia con b incluye b', la información asociada de x incluye además ab'cd y el resto se puede hacer de la misma manera, de modo que se pueda obtener toda la información asociada.

Se puede entender que, el significado específico de una pequeña distancia arriba se puede establecer de acuerdo con las demandas reales. Por ejemplo, los caracteres que corresponden a cuatro teclas adyacentes pueden determinarse como los caracteres a una pequeña distancia o los caracteres a una distancia de no más de dos teclas se determinan como los caracteres a una pequeña distancia, y así sucesivamente.

S12. Se recibe información a verificar.

El usuario puede ingresar la información a verificar a través de un teclado.

Por ejemplo, el usuario ingresa una contraseña o similar utilizando un teclado virtual de un teléfono móvil.

S13. La información a verificar se verifica de acuerdo con la información almacenada previamente.

Cuando el terminal del teléfono móvil almacena directamente una contraseña de texto sin cifrar, la información de entrada puede compararse directamente con la información almacenada previamente y cuando son iguales, la verificación tiene éxito; de lo contrario, la verificación falla.

Esta realización toma el almacenamiento de la primera información cifrada como un ejemplo.

Cuando la información almacenada previamente es la primera información cifrada, la etapa de verificar la información a verificar de acuerdo con la información almacenada previamente incluye:

cifrar la información a verificar utilizando el mismo algoritmo de cifrado que el de la primera información para obtener información cifrada a verificar; y
comparar la información cifrada a verificar con la información almacenada previamente.

Suponiendo que la información de entrada que debe verificar el usuario es y, y se adopta un algoritmo de cifrado Hash, H(y) puede calcularse primero, y luego H(y) se compara con H(x) y H'.

S14. La información a verificar que se vuelve a ingresar se recibe si la información a verificar pertenece a la información asociada.

Por ejemplo, si H(y) pertenece a H', se puede recibir la información a verificar nuevamente. Posteriormente, la verificación puede realizarse nuevamente.

Con referencia a la Figura 3, en esta realización, cuando la información a verificar pertenece a la información asociada, se pueden realizar específicamente las siguientes etapas:
S141. Se recibe la información a verificar que se vuelve a ingresar y se realiza una orientación o se da un aviso obvio.

Específicamente, la etapa de realizar una orientación o dar un aviso obvio incluye:
prolongar el tiempo de visualización de texto sin cifrar de la información a verificar que se vuelve a ingresar después de recibir la información a verificar que se vuelve a ingresar.

La información que no es texto sin cifrar, como los símbolos *, generalmente se muestra finalmente durante la verificación de la contraseña y la información de texto sin cifrar ingresada por el usuario se puede mostrar por un corto tiempo antes de que se muestren los símbolos *.

En esta realización, cuando el tiempo de visualización de texto sin cifrar se prolonga, el tiempo de visualización de texto sin cifrar de cada elemento de información en la información a verificar puede prolongarse, o, solo el tiempo de visualización de texto sin cifrar de un elemento de información que se introduce incorrectamente la última vez se prolonga. Por ejemplo, si la información a verificar es abcd y se produce un error en a durante una primera detección, solo se puede prolongar el tiempo de visualización de texto sin cifrar de a, o el tiempo de visualización de texto sin cifrar de a, b, c y d pueden todos prolongarse. Además, también se pueden realizar ejecuciones similares durante la visualización en texto sin cifrar. Por ejemplo, solo el elemento de información que se ingresó incorrectamente la última vez se muestra en texto sin cifrar, o todos los elementos de información se muestran en texto sin cifrar.

Posteriormente, se pueden realizar las siguientes etapas:
S142. La verificación se realiza nuevamente.

Por ejemplo, el usuario puede verificar la información a verificar que se vuelve a ingresar de acuerdo con la información o la información que se muestra en texto sin cifrar. Después de que el usuario reciba nuevamente la información a verificar en el terminal del teléfono móvil, la información puede compararse con la información previamente almacenada, para obtener un resultado de verificación.

En esta realización, el tiempo para mostrar la información de entrada de texto sin cifrar se prolonga, de modo que el usuario puede ver mejor la entrada de información por sí mismo, para verificar si la información se ingresa correctamente. Se puede establecer el tiempo de prolongación específico.

En otro aspecto, haciendo referencia a la Figura 4, después de que el usuario verifique la información de entrada a verificar, el método puede incluir, además:
S15. Se determina que la verificación tiene éxito si la información a verificar es la misma que la información establecida.

Por ejemplo, cuando se almacena un valor obtenido después del cifrado Hash y la información que el usuario debe verificar es y, y se calcula para obtener H(y) y si H(y) es igual a H(x), la verificación tiene éxito.

S16. Se determina que la verificación falla si la información a ser verificada es diferente de la información establecida y no pertenece a la información asociada.

Por ejemplo, si H(y) es diferente de H(x) y H(y) no pertenece a H', se determina que la verificación falla. En este momento, se muestra al usuario información que indica que la contraseña se ingresó incorrectamente.

En esta realización, no solo se puede generar la información establecida sino también la información asociada obtenida de acuerdo con la información establecida y cuando la información a verificar pertenece a la información asociada, la verificación se realiza nuevamente. Se puede proporcionar otra oportunidad de verificación después de un error de entrada del usuario causado por un tamaño pequeño de un teclado u otras razones, se reducen así los errores de entrada causados por un tamaño pequeño de un teclado y mejorando los efectos de entrada. Es diferente de una falla de verificación directa debido a un error de entrada malicioso, por lo tanto, distingue efectivamente un error no intencional de un error malicioso y reduce las fallas de verificación de información causadas por un error de entrada no intencional.

La Figura 5 es un diagrama estructural esquemático de un aparato de entrada de información de acuerdo con otra realización de la presente solicitud. El aparato 50 incluye: un módulo de adquisición 51, un primer módulo de recepción 52, un módulo de verificación 53 y un segundo módulo de recepción 54.

El módulo de adquisición 51 se configura para adquirir la información almacenada previamente, la información almacenada previamente que incluye la primera información de texto sin cifrar o la primera información cifrada, la primera información que incluye la información establecida y la información asociada generada de acuerdo con la información establecida;

El método de esta realización puede usarse para la verificación de información en varios escenarios, por ejemplo, para verificación de contraseña, verificación de número de tarjeta de identificación, verificación de número de tarjeta bancaria, verificación de número de teléfono móvil, etc. En esta realización, la verificación de contraseña se toma como un ejemplo.

Antes de la verificación de la contraseña, un usuario puede preestablecer una contraseña. Por ejemplo, la contraseña se establece como x. Puede entenderse que la contraseña x establecida por el usuario puede incluir uno o más elementos de información y cada elemento de información puede ser un número, una letra o similar.

Además, tomando como ejemplo que la contraseña se almacena en un terminal de teléfono móvil, la contraseña puede almacenarse en texto sin cifrar en el terminal de teléfono móvil, por ejemplo, directamente almacenado como x. O, para mejorar la seguridad, una contraseña de texto sin cifrar se cifra antes de almacenarse, por ejemplo, una x cifrada almacenada en el terminal del teléfono móvil. Se puede entender que existen varios algoritmos de cifrado, que, por ejemplo, es específicamente un algoritmo Hash. En esta realización, se toma como ejemplo una contraseña cifrada de Hash almacenada en el terminal del teléfono móvil. Suponga que x se representa como H(x) después de realizar el cifrado Hash.

En la técnica anterior, la información almacenada previamente es H(x) como máximo y la verificación fallará si lo que ingresa el usuario no es x.

En esta realización, no solo se puede almacenar H(x), sino que también se puede obtener información asociada de acuerdo con x y la información obtenida después de que se realiza el cifrado Hash en la información asociada se almacena adicionalmente en el terminal del teléfono móvil.

Con referencia a la Figura 6, el aparato 50 incluye, además:
un módulo de configuración 55 configurado para seleccionar aleatoriamente un elemento de información de la información establecida y adquirir un nuevo elemento de información correspondiente al elemento de información seleccionado, en donde una distancia entre las posiciones del nuevo elemento de información y el elemento de información seleccionado en un teclado está en un rango preestablecido; y reemplace el elemento de información seleccionado en la información establecida con el nuevo elemento de información para obtener la información asociada.

Por ejemplo, un elemento de la contraseña x establecido por el usuario es a, luego se selecciona un carácter a una pequeña distancia con un teclado virtual activado o un teclado físico como un nuevo carácter correspondiente a a. Suponiendo que el nuevo carácter se representa por una a', a' se usa para colocar a para componer una nueva contraseña x'. La nueva contraseña x' es información asociada de x. Después de realizar el cifrado de Hash, la información asociada cifrada puede representarse como: H(x'), H(x")..., y esta secuencia se registra como H'. Específicamente, por ejemplo, suponiendo que x es abcd y el carácter a una pequeña distancia con a incluye a', la información asociada de x incluye a'bcd. Además, suponiendo que el carácter a una pequeña distancia con un

adicional incluye un a", la información asociada de x incluye además un a"bcd. Además, suponiendo que un carácter a una pequeña distancia con b incluye b', la información asociada de x incluye además ab'cd y el resto se puede hacer de la misma manera, de modo que se pueda obtener toda la información asociada.
Se puede entender que, el significado específico de una pequeña distancia arriba se puede establecer de acuerdo con las demandas reales. Por ejemplo, los caracteres correspondientes a cuatro teclas adyacentes pueden determinarse como los caracteres a una pequeña distancia o los caracteres a una distancia de no más de dos teclas se determinan como los caracteres a una pequeña distancia, o similares.

El primer módulo de recepción 52 se configura para recibir la información a verificar;
en donde el usuario puede ingresar la información a verificar a través de un teclado.

Por ejemplo, el usuario ingresa una contraseña o similar utilizando un teclado virtual de un teléfono móvil.

El módulo de verificación 53 se configura para verificar la información a verificar de acuerdo con la información almacenada;

Cuando el terminal del teléfono móvil almacena directamente una contraseña de texto sin cifrar, la información de entrada puede compararse directamente con la información almacenada previamente y cuando son iguales, la verificación tiene éxito; de lo contrario, la verificación falla.

Esta realización toma el almacenamiento de la primera información cifrada como un ejemplo.

Cuando la información almacenada previamente es la primera información cifrada, el módulo de verificación 53 se configura específicamente para:

cifrar la información a verificar utilizando el mismo algoritmo de cifrado que el de la primera información para obtener información cifrada a verificar; y

comparar la información cifrada a verificar con la información almacenada previamente.

Suponiendo que la información de entrada que debe verificar el usuario es y, y se adopta un algoritmo de cifrado Hash, H(y) puede calcularse primero, y luego H(y) se compara con H(x) y H'.

El segundo módulo de recepción 54 se configura para recibir la información a verificar que se vuelve a ingresar si la información a verificar pertenece a la información asociada.

Por ejemplo, si H(y) pertenece a H', se puede recibir la información a verificar nuevamente. Posteriormente, la verificación puede realizarse nuevamente.

El segundo módulo receptor se configura además para:
se prolonga el tiempo de visualización de texto sin cifrar de la información a verificar que se vuelve a ingresar después de recibir la información a verificar.

La información que no es texto sin cifrar, como los símbolos *, generalmente se muestra finalmente durante la verificación de la contraseña y la información de texto sin cifrar ingresada por el usuario puede mostrarse por un corto tiempo antes de que se muestren los símbolos *.

En esta realización, cuando el tiempo de visualización de texto sin cifrar se prolonga, el tiempo de visualización de texto sin cifrar de cada elemento de información en la información a verificar puede prolongarse, o, solo el tiempo de visualización de texto sin cifrar de un elemento de información que se introduce incorrectamente la última vez se prolonga. Por ejemplo, si la información a verificar es abcd y se produce un error en a durante una primera detección, solo se puede prolongar el tiempo de visualización de texto sin cifrar de a, o el tiempo de visualización de texto sin cifrar de a, b, c y d pueden todos prolongarse. Además, también se pueden realizar ejecuciones similares durante la visualización en texto sin cifrar. Por ejemplo, solo el elemento de información que se ingresó incorrectamente la última vez se muestra en texto sin cifrar, o todos los elementos de información se muestran en texto sin cifrar.

En esta realización, el tiempo para mostrar la información de entrada de texto sin cifrar se prolonga, de modo que el usuario pueda ver mejor la entrada de información por sí mismo, para verificar si la entrada es correcta. Se puede establecer el tiempo de prolongación específico.

Con referencia a la Figura 6, el aparato 50 incluye, además:
un módulo de determinación 56 se configura para determinar que la verificación tiene éxito si la información a verificar es la misma que la información establecida; o determine que la verificación falla si la información a verificar es diferente de la información establecida y no pertenece a la información asociada.

Por ejemplo, cuando se almacena un valor obtenido después del cifrado Hash y la información que el usuario debe verificar es y, y se calcula para obtener H(y) y si H(y) es igual a H(x), la verificación tiene éxito.

Por ejemplo, si H(y) es diferente de H(x) y H(y) no pertenece a H', se determina que la verificación falla. En este momento, se muestra al usuario información que indica que la contraseña se ingresó incorrectamente.

En esta realización, no solo se puede generar la información establecida sino también la información asociada obtenida de acuerdo con la información establecida y cuando la información a verificar pertenece a la información asociada, la verificación se realiza nuevamente. Se puede proporcionar otra oportunidad de verificación después de un error de entrada del usuario causado por un tamaño pequeño de un teclado u otras razones, se reducen así los errores de entrada causados por un tamaño pequeño de un teclado y mejorando los efectos de entrada. Es diferente de una falla de verificación directa debido a un error de entrada malicioso, lo que distingue efectivamente un error involuntario de un error malicioso y reduce una falla de verificación de información causada por un error de entrada no intencional.

Debe observarse que, en la descripción de la presente solicitud, los términos "primero" y "segundo" se usan simplemente con el propósito de la descripción y no pueden interpretarse como indicativos o que implican una importancia relativa. Además, en la descripción de la presente solicitud, "múltiple" significa dos o más, a menos que se especifique lo contrario.

Puede entenderse que cualquier proceso o método descrito en los diagramas de flujo o descrito de cualquier otra manera en el presente documento incluye uno o más módulos, segmentos o partes para códigos de instrucciones ejecutables que realizan funciones lógicas particulares o etapas de proceso. Además, las realizaciones preferidas de la presente aplicación incluyen otras implementaciones, en las que la función puede realizarse en un orden diferente del que se representa o discute, incluyendo una manera sustancialmente simultánea o un orden opuesto basado en las funciones relacionadas. Esto debe ser entendido por los expertos en la materia a los que pertenecen las realizaciones de la presente solicitud.

Debe entenderse que cada parte de la presente aplicación puede realizarse mediante el hardware, el software, el firmware o su combinación. En las realizaciones anteriores, el software o firmware almacenado en la memoria puede ejecutar una pluralidad de etapas o métodos y ejecutarlos mediante el sistema de ejecución de instrucciones apropiado. Por ejemplo, si se implementa por el hardware, del mismo modo en otra realización, las etapas o métodos pueden implementarse mediante una o una combinación de las siguientes técnicas conocidas en la técnica: un circuito lógico discreto que tiene un circuito de puerta lógica para realizar una función lógica de una señal de datos, un circuito integrado específico de la aplicación que tiene un circuito de puerta lógica de combinación apropiada, un conjunto de puertas lógicas programables (PGA), un conjunto de puertas lógicas programables en campo (FPGA), etc.

Los expertos en la materia entenderán que todos o parte de las etapas en el método de realización anterior pueden lograrse ordenando al hardware relacionado con programas. Los programas pueden almacenarse en un medio de almacenamiento legible por computadora y los programas, cuando se ejecutan, incluyen uno o una combinación de las etapas en las realizaciones del método.

Además, las unidades de función en las realizaciones de la presente solicitud pueden integrarse en un módulo de procesamiento, o las unidades pueden proporcionarse físicamente de manera separada, o pueden integrarse dos o más unidades en un módulo. El módulo integrado puede realizarse en forma de hardware o en forma de módulo de función de software. Cuando el módulo integrado se realiza en forma de módulo de función de software y se vende o utiliza como un producto independiente, el módulo integrado también puede almacenarse en un medio de almacenamiento legible por computadora.

El medio de almacenamiento mencionado anteriormente puede ser una memoria de solo lectura, un disco magnético, un CD, etc.

La referencia a lo largo de esta especificación a "una realización", "algunas realizaciones", "un ejemplo", "un ejemplo específico" o "algunos ejemplos" significa que una característica, estructura, material o característica específica descrita en relación con dicha realización o se incluye un ejemplo en al menos una realización o ejemplo de la presente solicitud. La expresión ilustrativa de estos términos a lo largo de esta especificación no se refiere necesariamente a una misma realización o ejemplo. Además, las características, estructuras, materiales o características específicas se pueden combinar de cualquier manera adecuada en una o más realizaciones o ejemplos.

Aunque las realizaciones de la presente solicitud se han mostrado y descrito en lo anterior, se apreciaría que las realizaciones anteriores son ejemplares y no pueden interpretarse como limitantes de la presente solicitud, y los expertos en la materia pueden hacer cambios, modificaciones, reemplazos y alternancias en las realizaciones dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de entrada de información realizado por un aparato de entrada de información (50), el método que comprende:
adquirir la información almacenada previamente, la información almacenada previamente que comprende la primera información de texto sin cifrar o la primera información cifrada, la primera información que comprende la información establecida y la información asociada generada de acuerdo con la información establecida (S11), en donde generar la información asociada (S10) comprende:
seleccionar aleatoriamente un elemento de información de la información establecida;
adquirir un nuevo elemento de información correspondiente al elemento de información seleccionado, en donde la distancia entre las posiciones del nuevo elemento de información y el elemento de información seleccionado en un teclado está dentro de un rango preestablecido; y
reemplazar el elemento de información seleccionado en la información establecida con el nuevo elemento de información para obtener la información asociada;
recibir la información a verificar (S12);
verificar la información a verificar de acuerdo con la información almacenada previamente (S13) y luego:
si la información a verificar pertenece a la información asociada (S14):
recibir la información a verificar que se vuelve a ingresar, y prolongar un tiempo de visualización de texto sin cifrar de la información a verificar que se vuelve a ingresar después de recibir la información a verificar que se vuelve a ingresar (S141);
de otra manera:
determinar que la verificación tiene éxito si la información a verificar es la misma que la información establecida (S15); y de otra manera
determinar que la verificación falla si la información a verificar es diferente de la información establecida y no pertenece a la información asociada (S16).

2. El método de acuerdo con la reivindicación 1, que comprende además verificar la información a verificar (S142) que se vuelve a ingresar.

3. El método de acuerdo con la reivindicación 1, en donde cuando la información almacenada previamente es la primera información cifrada, la etapa de verificar la información a verificar de acuerdo con la información almacenada previamente comprende:
cifrar la información a verificar utilizando el mismo algoritmo de cifrado que el de la primera información para obtener información cifrada a verificar; y
comparar la información cifrada a verificar con la información almacenada previamente.

4. El método de acuerdo con la reivindicación 3, en donde el algoritmo de cifrado es un algoritmo Hash.

5. Un aparato de entrada de información (50), que comprende:
un módulo de adquisición (51) configurado para adquirir la información almacenada previamente, la información almacenada previamente que comprende la primera información de texto sin cifrar o la primera información cifrada, la primera información que comprende la información establecida y la información asociada generada de acuerdo con la información establecida, en donde generar la información asociada comprende:
seleccionar aleatoriamente, mediante un módulo de configuración (55), un elemento de información de la información establecida;
adquirir, mediante el módulo de configuración (55), un nuevo elemento de información correspondiente al elemento de información seleccionado, en donde la distancia entre las posiciones del nuevo elemento de información y el elemento de información seleccionado en un teclado está dentro de un rango preestablecido; y
reemplazar, por el módulo de configuración (55), el elemento de información seleccionado en la información establecida con el nuevo elemento de información para obtener la información asociada;
un primer módulo receptor (52) configurado para recibir la información a verificar;
un módulo de verificación (53) configurado para verificar la información a verificar de acuerdo con la información almacenada previamente;
un módulo de determinación (56) configurado para (i) determinar que la verificación tiene éxito si la información a verificar es la misma que la información establecida y para (ii) determinar que la verificación falla si la información a verificar es diferente de la información establecida y no pertenece a la información asociada; y
un segundo módulo de recepción (54) configurado para recibir la información a verificar que se vuelve a ingresar si la información a verificar pertenece a la información asociada y para prolongar un tiempo de visualización de texto sin cifrar de la información a verificar que se vuelve a ingresar después de que se recibe la información a verificar que se vuelve a ingresar.

6. El aparato de acuerdo con la reivindicación 5, en donde el segundo módulo receptor (54) se configura además para verificar la información a verificar que se vuelve a ingresar.

7. El aparato de acuerdo con la reivindicación 5, en donde cuando la información almacenada es la primera información cifrada, el módulo de verificación se configura específicamente para:
cifrar la información a verificar utilizando el mismo algoritmo de cifrado que el de la primera información para obtener información cifrada a verificar; y
comparar la información cifrada a verificar con la información almacenada previamente.

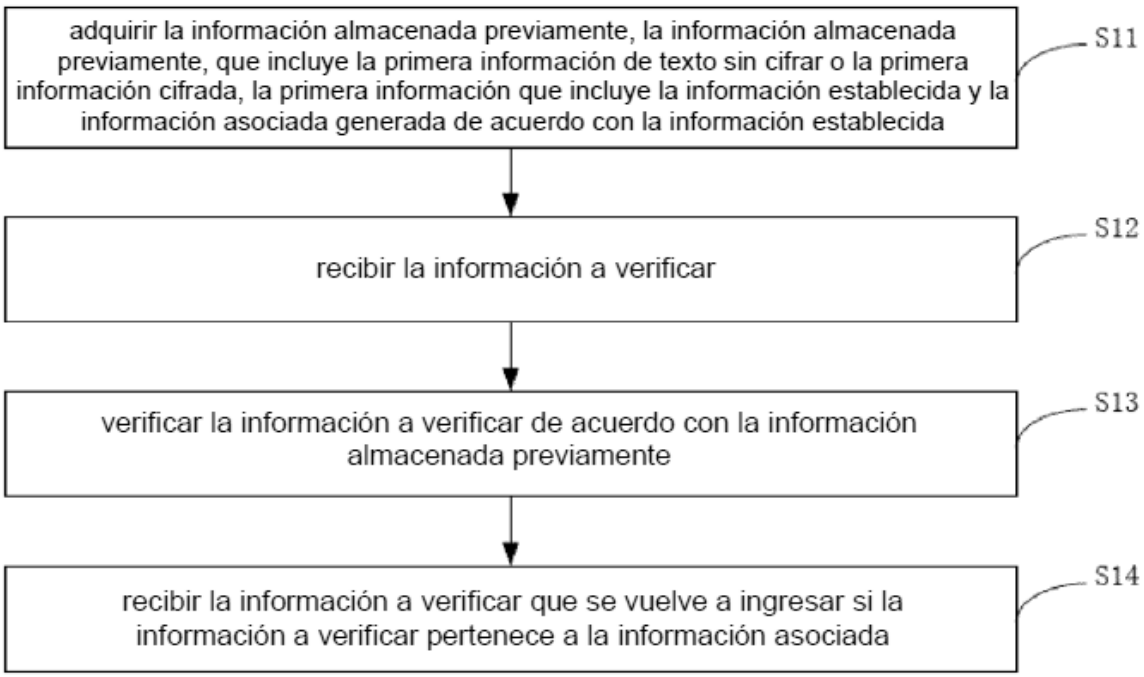
adquirir la información almacenada previamente, la información almacenada previamente, que incluye la primera información de texto sin cifrar o la primera información cifrada, la primera información que incluye la información establecida y la información asociada generada de acuerdo con la información establecida
S11
recibir la información a verificar
S12
verificar la información a verificar de acuerdo con la información almacenada previamente
S13
recibir la información a verificar que se vuelve a ingresar si la información a verificar pertenece a la información asociada
S14

Figura 1

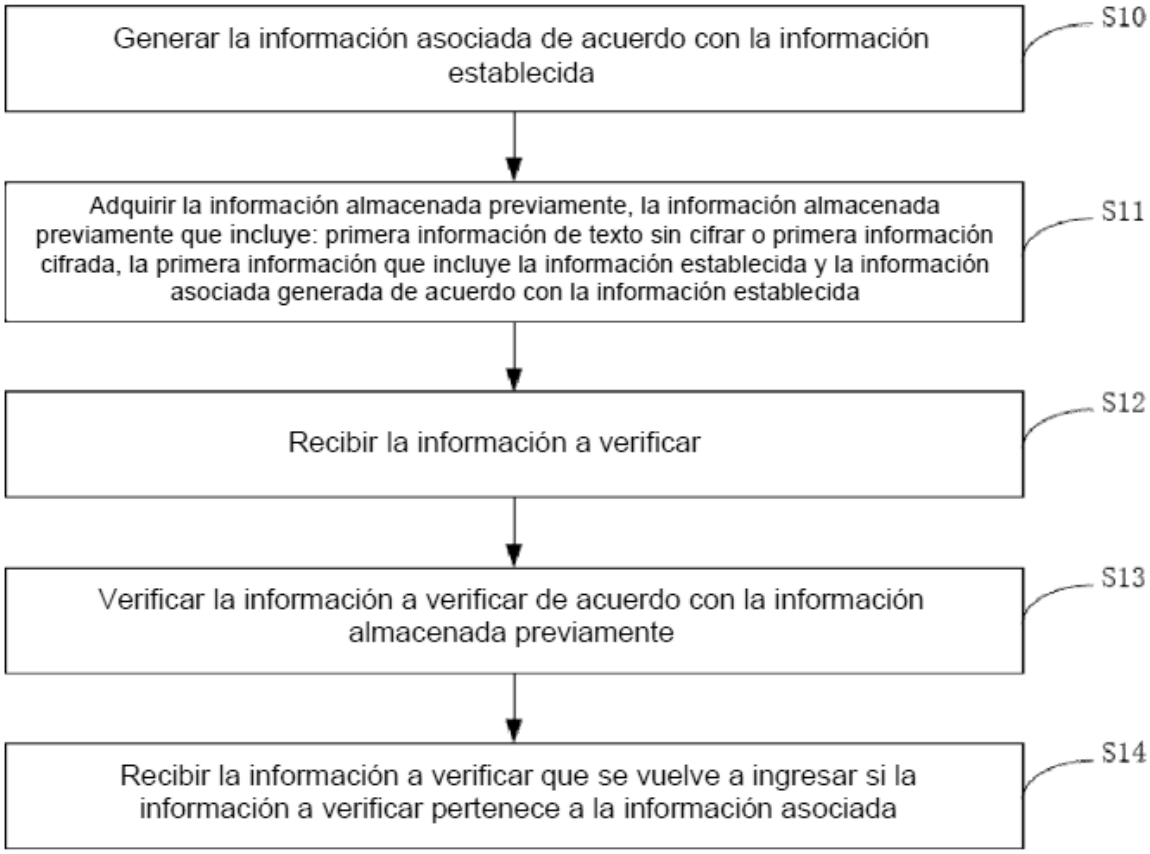
Generar la información asociada de acuerdo con la información establecida
S10
Adquirir la información almacenada previamente, la información almacenada previamente que incluye: primera información de texto sin cifrar o primera información cifrada, la primera información que incluye la información establecida y la información asociada generada de acuerdo con la información establecida
S11
Recibir la información a verificar
S12
Verificar la información a verificar de acuerdo con la información almacenada previamente
S13
Recibir la información a verificar que se vuelve a ingresar si la información a verificar pertenece a la información asociada
S14

Figura 2

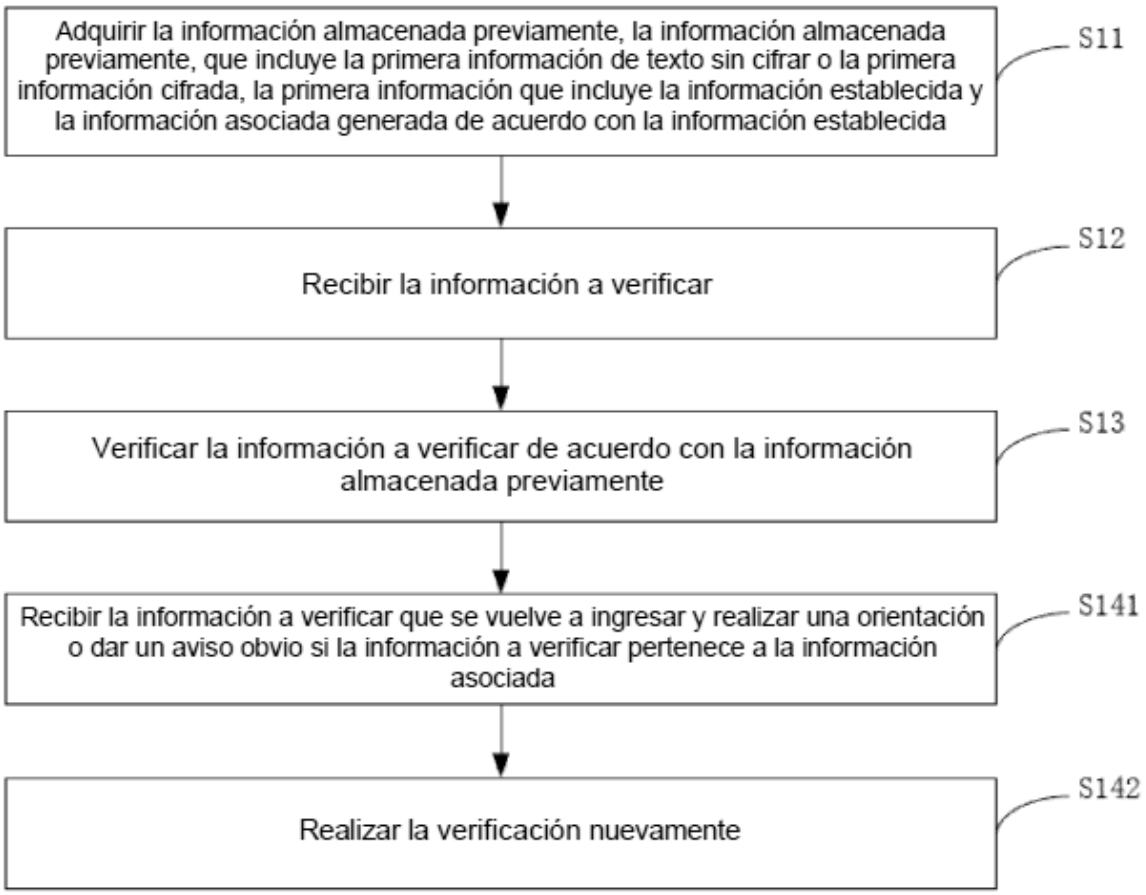
Adquirir la información almacenada previamente, la información almacenada previamente, que incluye la primera información de texto sin cifrar o la primera información cifrada, la primera información que incluye la información establecida y la información asociada generada de acuerdo con la información establecida
S11
Recibir la información a verificar
S12
Verificar la información a verificar de acuerdo con la información almacenada previamente
S13
Recibir la información a verificar que se vuelve a ingresar y realizar una orientación o dar un aviso obvio si la información a verificar pertenece a la información asociada
S141
Realizar la verificación nuevamente
S142

Figura 3

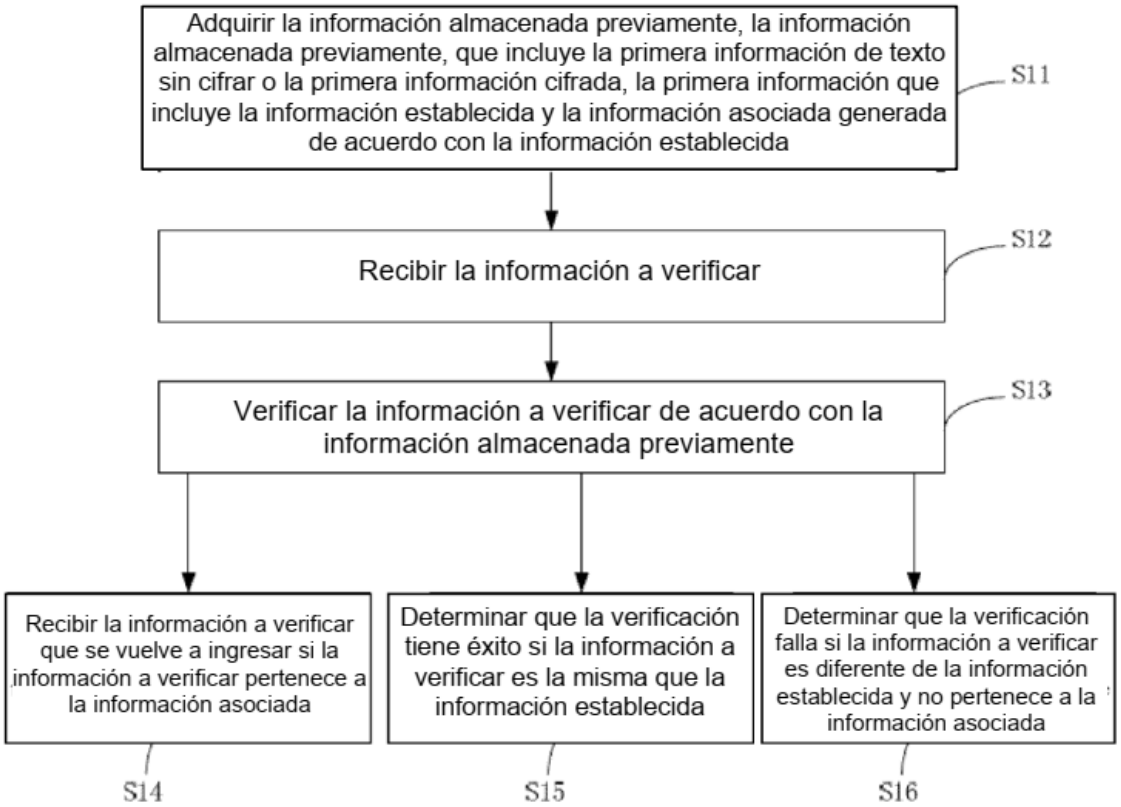
Adquirir la información almacenada previamente, la información almacenada previamente, que incluye la primera información de texto sin cifrar o la primera información cifrada, la primera información que incluye la información establecida y la información asociada generada de acuerdo con la información establecida
S11
Recibir la información a verificar
S12
Verificar la información a verificar de acuerdo con la información almacenada previamente
S13
Recibir la información a verificar que se vuelve a ingresar si la información a verificar pertenece a la información asociada
S14
Determinar que la verificación tiene éxito si la información a verificar es la misma que la información establecida
S15
Determinar que la verificación falla si la información a verificar es diferente de la información establecida y no pertenece a la información asociada
S16

Figura 4

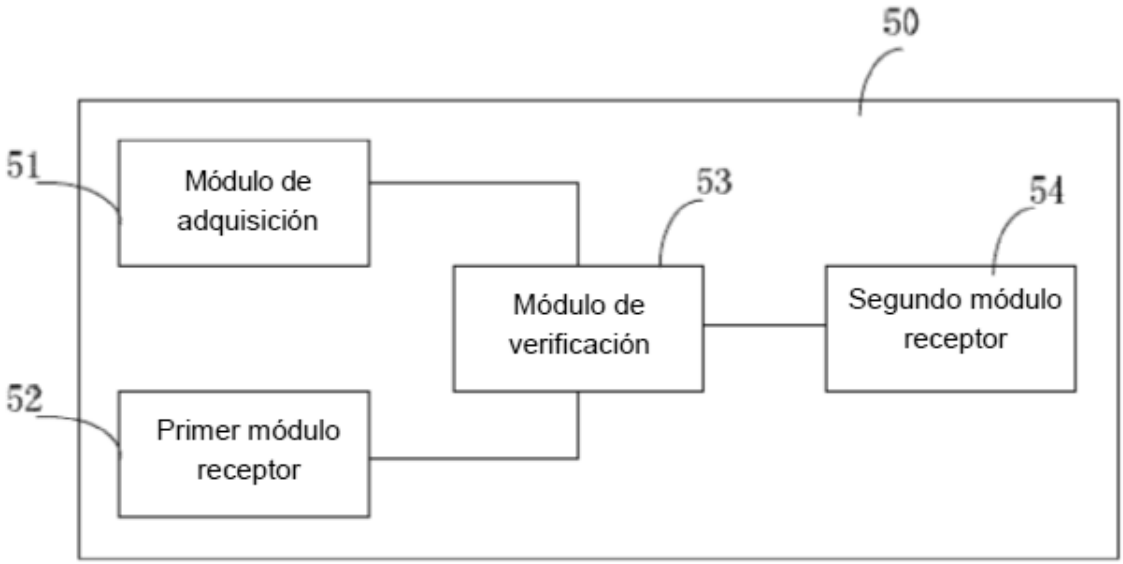
50
51
Módulo de adquisición
53
54
Módulo de verificación
Segundo módulo receptor
52
Primer módulo receptor

Figura 5

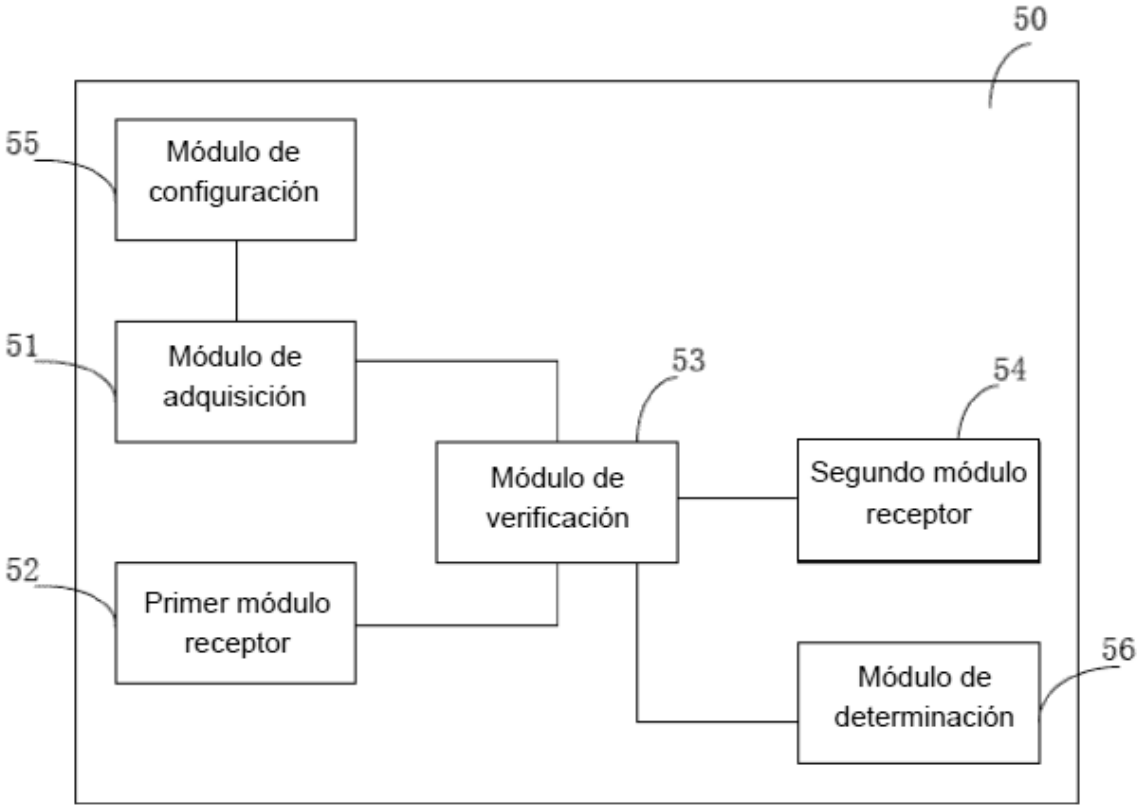
50
55
Módulo de configuración
51
Módulo de adquisición
53
54
Módulo de verificación
Segundo módulo receptor
52
Primer módulo receptor
56
Módulo de determinación

Figura 6