(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 671 777**

(51) Int. CI.:

***G06F 21/31*** (2013.01)
***G06F 3/0488*** (2013.01)
***G06F 3/0482*** (2013.01)
***G06F 3/0484*** (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.10.2013 PCT/CN2013/086237**

(87) Fecha y número de publicación internacional: **23.04.2015 WO15054934**

(96) Fecha de presentación y número de la solicitud europea: **30.10.2013 E 13895604 (0)**

(97) Fecha y número de publicación de la concesión europea: **02.05.2018 EP 3059689**

(54) Título: **Aparato de autenticación y método de autenticación**

(30) Prioridad:

**17.10.2013 CN 201310487970**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**08.06.2018**

(73) Titular/es:

**SMART ELECTRONIC INDUSTRIAL (DONG GUAN) CO. LTD. (50.0%)**
**Long Jian Tian-Cun Huang Jiang-Zhen Dongguan, Guangdong 523750, CN y**
**ZHENG LI (50.0%)**

(72) Inventor/es:

**ZHENG, LI**

(74) Agente/Representante:

**LINAGE GONZÁLEZ, Rafael**

## DESCRIPCIÓN

Aparato de autenticación y método de autenticación

**Campo de la invención**

La presente invención se refiere a una tecnología electrónica de protección de seguridad y más particularmente, se refiere a un dispositivo de autenticación y A un método de autenticación relacionado.

**Antecedentes de la invención**

Con la mejora continua de la calidad de vida de las personas y la comprensión profunda de la seguridad, el dispositivo de autenticación y el método de autenticación relacionado se han utilizado ampliamente en diversas áreas de la vida de la gente. En una situación típica, actualmente casi todas las personas poseen al menos un teléfono móvil o tableta, y, en estos dispositivos, a menudo se puede encontrar el empleo de métodos de autenticación. De hecho, esta es una utilización específica de los aparatos de autenticación. Para un terminal móvil, generalmente se proporciona una pantalla de representación visual basada en el principio de retroalimentación táctil. Los modos más convenientes pueden incluir desbloqueo deslizante, desbloqueo facial, desbloqueo mediante el dibujo de un patrón particular en una pantalla de nueve cuadrículas y similares, todos los cuales son bien conocidos públicamente. Todos estos modos adolecen de algunos inconvenientes. Por ejemplo, el desbloqueo deslizante puede ser visto por otros completamente; el desbloqueo facial puede ser descifrado por una imagen estática; y desbloquear dibujando un patrón particular en una pantalla de nueve cuadrículas es de hecho una variación del teclado numérico de nueve cuadrículas, y también puede ser visto fácilmente por otros y, de este modo, ser descifrado. Aparentemente, estos métodos de autenticación de la técnica anterior utilizados en terminales móviles carecen por completo de seguridad y fiabilidad suficientes y, por lo tanto, son susceptibles de ser descifrados por el fisgoneo intencionado.

La tecnología de autenticación anterior se realizaba principalmente de forma mecánica. Por ejemplo, el bloqueo de combinación que se muestra ampliamente en distintos tipos de bolsos y maletas también es uno de los dispositivos de autenticación. Este tipo de aparato de autenticación que funciona mecánicamente de manera similar adolece de desventajas bien conocidas y, como resultado, los aparatos de autenticación electrónica reemplazarán gradualmente a los aparatos mecánicos de autenticación. Como tal, los aparatos de autenticación con contraseña pueden aplicarse no sólo en diversos terminales móviles electrónicos, sino también en otras situaciones en las que es necesaria la verificación por contraseña. Por ejemplo, en distintos tipos de bolsas de viaje y maletas se puede usar un dispositivo de verificación en su mecanismo de verificación electrónica de bloqueo. Si tomamos otros ejemplos, los dispositivos electrónicos domésticos tales como el televisor inteligente, el enrutador capaz de interacción hombre-máquina o el dispositivo de control central pueden usar el dispositivo anterior en su procedimiento de verificación. Si tomamos otro ejemplo adicional, el aparato de autenticación anterior también puede encontrar su aplicación en el sistema de control de acceso, cerraduras electrónicas de una máquina expendedora, una caja fuerte y una puerta de automóvil. Incluso se puede usar en cualquier producto nuevo que pueda surgir en el futuro y que puede requerir verificación de contraseña. Entendemos que el dispositivo de autenticación es tan importante que tiene una gran influencia en diversos aspectos de la vida humana. Por consiguiente, se desea proporcionar un buen dispositivo de autenticación y el método correspondiente en busca de una seguridad cada vez mayor.

Sin embargo, como se describió anteriormente, aunque el dispositivo de autenticación es muy importante, los métodos de autenticación actualmente disponibles no son tan satisfactorios. Durante el proceso de diseño de la industria, los diseñadores deben considerar no solo el rendimiento y la seguridad del producto como se discutió anteriormente, sino también el coste de producción y la conveniencia del producto. Por lo tanto, cómo equilibrar estos factores industriales se ha convertido en una fuerza motriz para mejorar continuamente las técnicas de autenticación que han avanzado gradualmente.

El documento WO 2004/077194 A2 divulga un método de introducción de contraseña en el que un conjunto de caracteres que comprende el conjunto de caracteres de la contraseña conocida se divide en subconjuntos que se representan visualmente para su selección.

**Sumario de la invención**

El objeto de la invención es superar los inconvenientes de la tecnología de la técnica anterior y proporcionar un dispositivo y un método de autenticación, que tengan una alta seguridad y sean fáciles de usar y que tengan una buena capacidad de ocultación.

La invención proporciona un método de autenticación como se define en las reivindicaciones adjuntas.

Con el propósito anterior, se propone la siguiente solución técnica.

De acuerdo con la invención, un método de autenticación para verificar contraseña introducida por un usuario

incluye los siguientes pasos:

(1) correspondiendo con un conjunto conocido de caracteres contenido en una contraseña predefinida, definir un conjunto candidato de caracteres construido por una pluralidad de caracteres, siendo dicho conjunto conocido de caracteres un subconjunto del conjunto candidato de caracteres;

(2) distribuir aleatoriamente todos los caracteres del conjunto candidato de caracteres en una pluralidad de subconjuntos candidatos de caracteres de modo que al menos un subconjunto candidato de caracteres incluya dos o más caracteres, y distribuir y representar visualmente de manera correspondiente los caracteres de los subconjuntos candidatos de caracteres en una pluralidad de regiones interactivas respectivamente; y

(3) recibir de los usuarios instrucciones concernientes a la selección de regiones interactivas específicas basadas en los caracteres de los conjuntos de caracteres conocidos, comprobar uno por uno si cada carácter del conjunto conocido de caracteres pertenece a los subconjuntos candidatos de caracteres correspondientes a las regiones interactivas específicas actualmente seleccionados por el usuario, y confirmar la autenticación exitosa y emitir señales que indican la autenticación exitosa cuando todos los caracteres del conjunto conocido de caracteres pertenecen a los subconjuntos candidatos de caracteres correspondientes a las regiones interactivas específicas actualmente seleccionadas por el usuario.

Para cada carácter del conjunto conocido de caracteres, se puede proporcionar un subconjunto candidato de caracteres a cada carácter del conjunto conocido. Alternativamente, los caracteres contenidos en cada subconjunto candidato de caracteres pueden cambiarse para cada carácter del conjunto conocido, proporcionando así un subconjunto candidato de caracteres a cada carácter del conjunto conocido. Específicamente, el paso (2) se realiza antes de comprobar cada carácter del conjunto conocido de caracteres de modo que cada subconjunto candidato de caracteres correspondiente a la región interactiva respectiva se actualice para cada carácter.

Preferiblemente, en el paso (2), todos los caracteres del conjunto candidato de caracteres respectivo se generan aleatoriamente y se distribuyen discretamente. Preferiblemente, en el paso (1), el conjunto conocido de caracteres es equivalente a la recolección de todos los subconjuntos candidatos de caracteres, mientras que en el paso (2), cada subconjunto candidato de caracteres incluye dos o más caracteres.

Siguiendo una realización de la invención, cada región interactiva se usa para recibir la acción de tocar del usuario para confirmar esta acción como las instrucciones del usuario de seleccionar una región interactiva correspondiente. Siguiendo otra realización de la invención, cada región interactiva está asociada con un circuito de entrada correspondiente, y la conmutación de cada circuito de entrada se transforma en instrucciones de selección de una región interactiva asociada con el circuito de entrada.

De acuerdo con una realización de la invención, en los pasos (2) y (3), de acuerdo con el orden por defecto de todos los caracteres en el conjunto conocido de caracteres, para cada personaje, se determinan varias regiones interactivas basadas en el método y la selección mencionados anteriormente de regiones interactivas específicas por parte del usuario; después de la selección por el usuario, se comprueba si un carácter actual pertenece a un subconjunto candidato de caracteres correspondiente a una región interactiva específica seleccionada actualmente por el usuario; el resultado de comprobación actual se establece como una etiqueta temporal; y se determina en base a la etiqueta temporal que la autenticación es exitosa si ningún carácter se etiqueta como error de autenticación.

De acuerdo con otra realización de la invención, en los pasos (2) y (3), de acuerdo con el orden por defecto de todos los caracteres en el conjunto conocido de caracteres, para cada carácter, se determinan varias regiones interactivas en base al método y la selección mencionados anteriormente de regiones interactivas específicas por parte del usuario; los datos de correlación entre el subconjunto candidato de caracteres correspondiente a una región de interacción específica seleccionada actualmente por el usuario y el carácter actual se establecen y almacenan, la misma operación de establecimiento y almacenamiento se realiza para el siguiente carácter hasta el último; después de que el usuario realice las instrucciones de selección para todos los caracteres del conjunto conocido de caracteres, se usan todos los datos de correlación y se comprueba cada uno de los datos de correlación para determinar si un carácter actual contenido en los datos de correlación pertenece al subconjunto candidato de caracteres contenido en el mismos datos de correlación, y el resultado de la comprobación actual se establece como una etiqueta temporal; y se determina en base a la etiqueta temporal que la autenticación es exitosa si ningún carácter se etiqueta como error de autenticación.

Para reducir el procedimiento de comprobación, en una realización variada de la invención, correspondiente a cualquier carácter del conjunto conocido de caracteres, cuando se comprueba que el carácter actual no está dentro del subconjunto candidato de caracteres correspondiente a una región interactiva específica seleccionada actualmente por el usuario, el método se termina para detener la realización de los siguientes pasos.

De acuerdo con la invención, un dispositivo de autentificación para realizar el método como se ha mencionado anteriormente, incluye una unidad de control, una unidad de memoria y una pantalla táctil, almacenando dicha

unidad de memoria en ella la contraseña predefinida que contiene el conjunto conocido de caracteres, donde la unidad de control está destinada a ejecutar un programa implantado por dicho método; la unidad de memoria está destinada a almacenar datos intermedios candidatos generados por el programa implantado por dicho método; y la pantalla táctil está destinada a proporcionar dichas regiones interactivas al programa implantado por dicho método, para recibir la selección del usuario de las regiones interactivas y transformar dicha selección en instrucciones que indican la selección de las regiones interactivas específicas.

De acuerdo con la invención, otro dispositivo de autenticación para realizar el método como se ha mencionado anteriormente, incluye una unidad de control, una unidad de memoria, una serie de circuitos de entrada y una pantalla, almacenando dicha unidad de memoria en ella la contraseña predefinida que contiene el conjunto conocido de caracteres, en el que la unidad de control está destinada a ejecutar un programa implantado por dicho método; la unidad de memoria está destinada a almacenar datos intermedios candidatos generados por el programa implantado por dicho método; la pantalla táctil está destinada a proporcionar dichas regiones interactivas al programa implantado por dicho método; y los circuitos de entrada están conectados eléctricamente a la unidad de control de modo tal que cada circuito de entrada corresponde a una región interactiva respectiva, y cada circuito de entrada está destinado a transformar la conmutación de sí mismo en instrucciones que indican la selección de las regiones interactivas específicas.

La presente invención aporta los siguientes buenos efectos en comparación con la tecnología de la técnica anterior.

En esta invención, cada carácter contenido en una contraseña predefinida se toma como un subconjunto. Al proporcionar conjuntos candidatos de caracteres que contengan caracteres del mismo número o más que los caracteres contenidos en la contraseña predefinida, se produce una indefinición primaria para la contraseña. Además, antes de autenticar un primer carácter o cada carácter de la contraseña predefinida, el conjunto candidato de caracteres se divide de manera predeterminada o aleatoria en múltiples subconjuntos, y estos subconjuntos se representan visualmente en respectivas regiones interactivas múltiples, de modo que el usuario puede seleccionar estas regiones. Como tal, la selección de una región interactiva específica por parte del usuario corresponde a múltiples elementos de carácter, y cada vez que el usuario hace la selección, la disposición y combinación de los elementos de carácter de las respectivas regiones interactivas para el usuario pueden ser diferentes, de este modo, la indefinición de los caracteres seleccionados se mejora mucho. Incluso en el caso de que la operación de clics de selección del usuario durante el proceso de verificación de contraseñas sea vista por otros, estos últimos no podrán averiguar la secuencia precisa de contraseña, lo que mejorará en gran medida la seguridad de la verificación de contraseña. Por otro lado, después de que varios caracteres se clasifiquen aleatoriamente en múltiples grupos, cada grupo puede contener más de un carácter. En esta situación, el usuario ya no necesita botones (un área) para introducir la contraseña, ya que el número de botones es el mismo que el de las regiones interactivas. El número de botones convencionales se reduce al de las regiones interactivas de la invención. En consecuencia, la comodidad de la operación se mejora para el usuario. Además, el efecto de seguridad no se ve afectado en absoluto.

**Breve descripción de los dibujos**

La figura 1 muestra una vista esquemática de una estructura eléctrica de un dispositivo de autenticación de la invención; y

la figura 2 muestra una interfaz de operación del dispositivo de autenticación de la invención.

**Descripción detallada de la invención**

Diversas realizaciones de la invención se describen a continuación en mayor detalle con referencia a los dibujos.

Haciendo referencia a la figura 1, un dispositivo de autenticación de la invención de la invención *[sic.]* incluye una unidad 1 de control, una unidad 5 de memoria, una pantalla 3 de representación visual y varios circuitos 2 de entrada. La unidad 1 de control funciona para controlar todo el dispositivo y principalmente sirve para realizar un programa obtenido de acuerdo con el método de autentificación de la invención para realizar un proceso de autenticación. La unidad 5 de memoria funciona para almacenar de forma permanente o temporal diversos datos intermedios generados durante la operación del programa obtenido de acuerdo con el método de autentificación de la invención. Los datos intermedios pueden incluir, por ejemplo, la contraseña predefinida del usuario, unidades parciales o completas candidatas de información y unidades de información de selección que se formarán subsiguientemente. La unidad 5 de memoria también puede almacenar etiquetas predefinidas tales como imagen, voz y estado que pueden estar implicados durante el programa de almacenamiento. El experto en la técnica deberá tener en cuenta que la contraseña predefinida del presente método y dispositivo debe almacenarse permanentemente. Con respecto a otros datos usados en el método de la invención, el programa determina de manera flexible si estos datos se deben almacenar en la unidad de memoria. Por lo tanto, no debe entenderse que el uso de la unidad de memoria de la invención tiene limitaciones para la tecnología de almacenamiento usada en esta invención. Bajo el control de la unidad 1 de control, el método de autentificación de la invención realiza la interacción ser humano-máquina mediante los circuitos 2 de entrada y la pantalla de representación visual para realizar la operación de verificación de contraseña de la invención.

En la interfaz de la figura 1, se muestra una pantalla 3 de representación visual que incluye cuatro esquinas y un área central. Hay cuatro regiones interactivas 31-34 ubicadas, respectivamente, en cuatro esquinas del área de representación visual, para representar visualmente todos los elementos de cuatro conjuntos candidatos para el usuario. Cada elemento es un carácter. Un área 4 de salida situada en el centro de la pantalla de representación visual está destinada principalmente a indicar el progreso de verificación durante el proceso de introducción de contraseña por el usuario. Obsérvese que en la invención no existe ningún límite con respecto a la ubicación de las regiones interactivas, como entendería el experto en la técnica.

Cuatro botones circulares situados cerca de las cuatro regiones interactivas de la pantalla de representación visual son botones 21-24 de los cuatro circuitos 2 de entrada para conmutar estos circuitos 2 respectivamente, de modo que la unidad 1 de control pueda detectar la conmutación de una circuito 2 de entrada específico y después transformarlo en la instrucción de seleccionar una región interactiva asociada con el circuito de entrada (botón). De esta manera, se acepta la entrada del usuario. En consecuencia, es evidente que la selección de una región interactiva específica puede hacerse presionando el botón correspondiente adyacente a la misma región interactiva correspondiente.

Las maneras de implantación anteriores se ven a menudo en bolsas, maletas y terminales POS (o terminales punto de venta). De acuerdo con una manera de implantación diferente, el circuito 2 de entrada puede simplificarse, y la pantalla de representación visual puede implantarse mediante una pantalla táctil ampliamente utilizada que tiene función táctil. Como tal, el dispositivo y el método de la presente invención se pueden combinar con diversos terminales móviles.

No importa cómo se optimice y seleccione el equipo físico informático (hardware), la implantación del método de autentificación de la invención no estará limitada.

El método de autentificación de la invención se basa en los siguientes principios generales.

En primer lugar, una unidad de memoria almacena la contraseña predefinida del usuario, y los medios de entrada de la contraseña predefinida pueden configurarse por el experto en la técnica de manera flexible. Es bien sabido que una contraseña generalmente se construye con caracteres. Una contraseña simple puede incluir 10 números 0-9. Por supuesto, también puede estar construida con otros caracteres, tales como letras del alfabeto inglés. Por comodidad para la descripción de la invención, supongamos que se presentan en la figura 2 caracteres tales como 0-9 y letras del alfabeto inglés a-d y similares. Cada secuencia de contraseña puede considerarse como un conjunto conocido de caracteres y cada carácter es un elemento del conjunto. Por supuesto, la secuencia de contraseña debería disponerse de acuerdo a un cierto orden. En el método de la invención, se define un conjunto candidato de caracteres para la secuencia de contraseña compuesta de múltiples caracteres conocidos dispuestos de acuerdo a un cierto orden. En este conjunto, todos los caracteres de la secuencia de contraseña, es decir, todos los elementos del conjunto conocido deberían incluirse en él. En otras palabras, el conjunto conocido de caracteres es un subconjunto del conjunto candidato de caracteres. El conjunto candidato de caracteres se obtiene al extender todos los elementos del conjunto conocido de caracteres. Esto se debe a que cuando el usuario establece una contraseña, normalmente se seleccionan algunos de entre un grupo de caracteres. Como tal, en general, un conjunto candidato de caracteres no es completamente igual al conjunto conocido de caracteres. Sin embargo, la presente invención no excluye situaciones en las que los dos conjuntos sean completamente iguales entre sí. De acuerdo con las matemáticas, la igualdad completa es un ejemplo específico de inclusión.

A continuación, después de que hayan sido definidos el conjunto candidato de caracteres y el conjunto conocido de caracteres, correspondientes a cada elemento del conjunto conocido de caracteres, todos los elementos del conjunto candidato de caracteres se distribuyen aleatoriamente en varios subconjuntos candidatos de caracteres. Es necesario asegurarse de que al menos un subconjunto candidato de caracteres incluye dos o más elementos. Los elementos de cada subconjunto candidato de caracteres se distribuyen de forma correspondiente y se representan visualmente mediante varias regiones interactivas. Por ejemplo, cuatro grupos de caracteres representados visualmente mediante las cuatro regiones interactivas respectivas están dispuestos irregularmente. Se observa que cuatro grupos de caracteres dispuestos aleatoriamente siguen ciertas regularidades, tales como el código ASCII, el número natural y similares, esta situación debería entenderse como un ejemplo específico de la distribución aleatoria de la invención y no debería excluirse de la presente invención. Hay un total de 14 caracteres en las cuatro regiones interactivas y pertenecen a cuatro subconjuntos candidatos de caracteres. Como estos 14 caracteres están agrupados en cuatro subconjuntos candidatos de caracteres, generalmente cada subconjunto candidato de caracteres necesariamente contiene elementos de múltiples caracteres. Esto asegura la expresión plural después de que cada subconjunto candidato de caracteres se represente visualmente en la región interactiva correspondiente. La elección de este subconjunto candidato específico de caracteres no se dirigirá ciertamente a un único carácter, mejorándose, de este modo, significativamente, la seguridad. En caso de que los diversos caracteres del conjunto candidato de caracteres se distribuyan en subconjuntos múltiples y el número de subconjuntos sea menor que el de los caracteres del conjunto candidato de caracteres, al menos un subconjunto candidato de caracteres contendrá dos o más elementos de caracteres. O bien algunos subconjuntos candidatos de caracteres pueden no contener caracteres, mientras que el resto de los subconjuntos candidatos de caracteres contienen todos los caracteres del

conjunto candidato de caracteres. Esto también asegurará que al menos un subconjunto candidato de caracteres contendrá dos o más elementos de caracteres. En teoría, siempre que sólo un subconjunto candidato de caracteres contenga más de un elemento de carácter, el proceso de autenticación será definitivamente plural, y los objetos de la invención se cumplirán. Sin embargo, la situación preferida es que cada subconjunto candidato de caracteres contenga dos o más elementos de caracteres para mejorar la indefinición de la verificación de contraseña. El experto en la técnica puede concebir diversas realizaciones modificadas de la invención en base a los tipos de cambios anteriores y, por lo tanto, se omite su descripción aquí.

Sin embargo, se observa que aunque se ha descrito una solución que corresponde a cada elemento de contraseña de la secuencia de contraseña, todos los elementos se distribuyen aleatoriamente en el conjunto candidato de caracteres, durante el proceso de autenticación, también se actualizan los contenidos de cada subconjunto candidato de caracteres en tiempo real. Es decir, que la ordenación del carácter presentado por las respectivas regiones interactivas también se actualiza en tiempo real, garantizando de este modo una mayor seguridad. Sin embargo, la invención también describe la siguiente solución. Sólo antes de la verificación de un elemento de contraseña de una primera ubicación, los conjuntos candidatos de caracteres se distribuyen aleatoriamente como para formar subconjuntos candidatos de caracteres respectivos y mostrar caracteres en las cuatro regiones interactivas. Durante el proceso de verificación subsiguiente de los elementos de contraseña, los subconjuntos candidatos de caracteres ya no se actualizan. Esta solución también es factible. Aunque esta solución reduce la complejidad de la computación, aún mantiene la pluralidad y la ocultación. No será necesario que el usuario vuelva a leer los contenidos de los otros subconjuntos candidatos de caracteres para cada elemento de contraseña y, por lo tanto, esto puede mejorar la comodidad de la verificación de contraseña.

Además, en la solución anterior donde el conjunto candidato de caracteres se divide en múltiples subconjuntos candidatos de caracteres, la distribución de los elementos de los subconjuntos candidatos de caracteres es aleatoria y arbitraria. Sin embargo, la distribución no aleatoria de los elementos también es posible en la presente invención. Por ejemplo, se pueden almacenar con antelación, en la unidad de memoria, varias soluciones de ordenación en las que los subconjuntos candidatos de caracteres están dispuestos al azar. Estas diferentes soluciones de ordenación se pueden variar de acuerdo con cierto orden. Antes de la verificación de cada elemento de la contraseña, se puede usar una solución de ordenación diferente de acuerdo con su rango. Como resultado, las soluciones de ordenación se pueden actualizar dinámicamente y se garantiza que todos los caracteres en el subconjunto candidato de caracteres de una determinada solución se organicen aleatoriamente.

A continuación, correspondiéndose con cada elemento del conjunto conocido de caracteres, después de dividir el conjunto candidato de caracteres en varios subconjuntos candidatos de caracteres, se recibe la instrucción de seleccionar una región interactiva específica por el usuario en base a los elementos respectivos del conjunto conocido de caracteres. Se determina después si cada carácter de la secuencia de contraseña pertenece a un conjunto candidato de caracteres respectivo correspondiente a una región interactiva específica seleccionada actualmente por el usuario. Cuando todos los elementos del conjunto conocido de caracteres pertenecen al subconjunto candidato de caracteres correspondiente a la región interactiva específica seleccionada actualmente por el usuario, se emite una señal que indica una autenticación exitosa y se confirma que la autenticación está bien hecha. Como se expuso anteriormente, de acuerdo con una realización de la invención (véase la figura 2), la entrada de la instrucción de selección del usuario se puede realizar haciendo clic en los botones 21-24. De acuerdo con una realización no mostrada, cuando se usa una pantalla táctil, hacer clic en la región interactiva correspondiente posee el mismo efecto que introducir una instrucción de selección. La acción de hacer clic se transfiere a la unidad de control a través de dicha pantalla táctil y se transforma en instrucciones para seleccionar la región interactiva correspondiente. No importa qué medios se usen para realizar la selección de la región interactiva, en esencia es la selección del subconjunto candidato de caracteres. Por lo tanto, significa que el usuario legal conoce los elementos de caracteres que se muestran en la región interactiva e introduce el contenido correcto. Esta operación se aplica a cada elemento. De acuerdo con el orden predefinido de la secuencia de contraseñas, y para cada carácter de contraseña, el usuario se enfrenta a la selección de la región interactiva, obteniéndose así la región interactiva correspondiente a cada carácter de contraseña. Para este método, la autenticación se logra comprobando uno por uno si cada elemento del conjunto conocido de caracteres pertenece al subconjunto candidato de caracteres correspondiente a la región interactiva específica seleccionada por el usuario. Cuando un elemento actual del conjunto conocido de caracteres pertenece al subconjunto candidato de caracteres correspondiente a una región interactiva específica seleccionada actualmente por el usuario, se confirma que el usuario ha introducido el carácter de contraseña correcto. De lo contrario, el usuario ha introducido un carácter de contraseña incorrecto. Cuando se compruebe que varias operaciones de selección coinciden correctamente con todos los caracteres de la contraseña, significará que la contraseña se ha verificado con éxito. En este caso, el dispositivo de autenticación de la invención emite una señal, que indica una autenticación exitosa, a una unidad externa para otra operación posterior, tal como un desbloqueo, una transacción, un inicio de programa y similares, finalizando todo el proceso. Por supuesto, en caso de que el usuario introduzca un carácter de contraseña específico, y verifique un elemento específico del conjunto conocido de caracteres, pero el subconjunto candidato de caracteres correspondiente a una región interactiva específica falle en contener este elemento específico, significará que la autenticación de este carácter de contraseña específico falla. Por razones de seguridad, en el presente método, los pasos subsiguientes pueden finalizar mediante el programa, e incluso se puede proporcionar un aviso, garantizando de este modo la seguridad.

Aparentemente, en el método de la invención, aunque un conjunto candidato de caracteres se divide en múltiples subconjuntos candidatos de caracteres, el número de subconjuntos es el mismo que el de las regiones interactivas, y el número de regiones interactivas es menor que el de los elementos de los subconjuntos candidatos de caracteres, los tiempos de cálculo aumentan para superar los inconvenientes resultantes de la insuficiencia de números de las regiones interactivas, ya que cada vez que se actualiza el subconjunto candidato de caracteres correspondiente a la región interactiva se realiza una reorganización aleatoria, garantizándose, de este modo, la seguridad.

Evidentemente, el método de la invención se realiza mediante un programa informático. El diseño del programa puede ser flexible. Para comprender fácilmente la presente invención a fin de poner la misma en práctica fácilmente, se describe a continuación la implantación del programa del método de verificación de la invención con referencia a los dibujos.

Un primer tipo de implantación de verificación:

En primer lugar, de acuerdo con el orden de disposición de los elementos respectivos del conjunto conocido de caracteres (es decir, el orden de disposición de los caracteres de contraseña incluidos en la secuencia de contraseña), se realizan los siguientes subpasos:

1. Todos los elementos del conjunto candidato de caracteres se seleccionan y se dividen en varios conjuntos, cada uno de los cuales es un subconjunto candidato de caracteres. El número de subconjuntos es el mismo que el de las regiones interactivas del dispositivo de autenticación. Preferiblemente, cada subconjunto candidato de caracteres contiene al menos dos elementos. A continuación, cada subconjunto candidato de caracteres corresponde a una región interactiva, y todos los elementos de los respectivos subconjuntos candidatos de caracteres están dispuestos correspondientemente en respectivas regiones interactivas, de manera que cada región interactiva representa visualmente varios caracteres.

2. El programa espera la entrada del usuario. Después de leer los caracteres que se muestran en los subconjuntos candidatos de caracteres de las respectivas regiones interactivas de la pantalla de representación visual, el usuario determina una región interactiva objetivo. La operación de selección se hace manualmente. Después de que el programa haya aceptado la instrucción del usuario de seleccionar una región interactiva específica en base a un elemento actual del conjunto conocido de caracteres, se comprueba inmediatamente si el elemento actual del conjunto conocido de caracteres pertenece al subconjunto candidato de caracteres representado visualmente de la región interactiva específica seleccionada por el usuario. Esta operación de comprobación se puede realizar comparando el elemento actual con los elementos del subconjunto candidato de caracteres, como entendería el experto en la técnica. Cuando el resultado de la comprobación es afirmativo, es decir, cuando el elemento actual pertenece al subconjunto candidato de caracteres, se establece el estado de una variable de etiqueta que funciona como una etiqueta temporal de autenticación exitosa; por ejemplo, a esta variable de etiqueta se le puede asignar el valor "Y" . De lo contrario, se establece que ha habido un fallo de autenticación y se le asigna el valor "N".

Los dos pasos anteriores se realizan para cada carácter de contraseña. En teoría, la verificación de cada carácter de contraseña requiere más de dos pasos.

Después de la finalización del ciclo anterior, con respecto a todos los caracteres de contraseña, el usuario ha elegido las respectivas regiones interactivas, lo que quiere decir que ha terminado de introducir la contraseña. Por lo tanto, se pueden realizar acciones de retroalimentación posteriores. Específicamente, en el presente método, el resultado de la autenticación puede depender del estado de la variable de etiqueta. Si la variable sigue siendo "Y", entonces la autenticación es exitosa y, subsiguientemente, la señal que muestra la autenticación exitosa se emite para permitir otra operación adicional. De lo contrario, el ciclo anterior finaliza siempre que a la variable de etiqueta se le haya asignado "N" incluso por una sola vez. En esta situación, se confirma que la autenticación falla, y se emite una señal que muestra la autenticación fallida, y el resultado se retroalimenta al usuario.

Un segundo tipo de implantación de verificación:

En primer lugar, de acuerdo con el orden de disposición de los elementos respectivos del conjunto conocido de caracteres, se realizan los siguientes subpasos.

1. Todos los elementos del conjunto candidato de caracteres se procesan y se dividen en varios conjuntos, cada uno de los cuales es un subconjunto candidato de caracteres que se representa visualmente en la región interactiva correspondiente. El número de subconjuntos es el mismo que el de las regiones interactivas del dispositivo de autenticación. Preferiblemente, cada subconjunto candidato de caracteres contiene al menos dos elementos. A continuación, cada subconjunto candidato de caracteres se corresponde con a una región interactiva, y todos los elementos de los respectivos subconjuntos candidatos de caracteres están dispuestos correspondientemente en respectivas regiones interactivas de manera que cada región interactiva muestra varios caracteres.

2. El programa espera la entrada del usuario. Después de leer los caracteres que se muestran en los subconjuntos

candidatos de caracteres de las respectivas regiones interactivas de la pantalla de representación visual, el usuario determina una región interactiva objetivo. La operación de selección se hace manualmente. A diferencia del proceso de verificación anterior, después de que el programa acepte instrucciones del usuario para seleccionar una región interactiva específica en base a un elemento actual del conjunto conocido de caracteres, la verificación no se realiza inmediatamente. En cambio, establece datos de correlación entre el elemento actual y el subconjunto candidato de caracteres de una región interactiva respectiva seleccionada por el usuario, y almacena estos datos en la unidad de almacenamiento. Después de esto, vuelve al paso 1 para verificar el siguiente carácter de contraseña (elemento), hasta que se verifique el último carácter. Después, se realizan los siguientes pasos.

El ciclo anterior finaliza para aceptar la entrada y selección de caracteres de contraseña respectivos por parte del usuario, de tal manera que el usuario selecciona todos los elementos del conjunto conocido de caracteres, estableciéndose de este modo la relación correspondiente entre los elementos respectivos y los subconjuntos candidatos dinámicos de caracteres. En consecuencia, puede comenzar un nuevo ciclo. Específicamente, se invocan los datos de relación correspondientes, y se comprueba si un elemento actual incluido en cada grupo de datos de relación correspondientes pertenece a un subconjunto candidato de caracteres asociado con dichos datos. Si la respuesta es sí, entonces el resultado de la comprobación actual recibe una etiqueta temporal, y la variable de etiqueta correspondiente indica el éxito de la autenticación. De lo contrario, si el elemento actual falla en cuanto a pertenecer al subconjunto candidato de caracteres correspondiente seleccionado por el usuario, la variable de etiqueta indica un fallo de autenticación. El ciclo actual finalizará una vez que haya al menos un fallo de verificación según muestre la variable de etiqueta. En este caso, se confirma que la autenticación ha fallado en base a la indicación de la variable de etiqueta, y se emite una señal que representa un fallo de autenticación, mejorándose de este modo la eficacia del programa. Si se comprueban todos los elementos y no se encuentra ningún resultado de fallo de autenticación, entonces se confirma que la autenticación es exitosa en base a dicha etiqueta temporal, y se emite una señal que representa el éxito de la autenticación.

Se debe enfatizar que se pueden formar diversos programas de equipo lógico informático (software) debido al uso de diferentes lenguajes de programa, diferentes estilos de programación y similares. Las realizaciones anteriores son solo ilustrativas y no limitan el alcance de la invención.

En resumen, el dispositivo de autenticación de la invención se basa en el método de autentificación de la invención. Al causar indefinición para los contenidos introducidos por el usuario, los contenidos de entrada se vuelven plurales, garantizándose de este modo que no será proporcionará la contraseña durante el proceso de introducción. Además, al generar aleatoriamente el efecto dinámico de los contenidos introducidos por el usuario, aumenta la complejidad de la operación de contraseña. Esto exhaustiva y completamente mejora la seguridad y la comodidad del proceso de autenticación.

Aunque se han ilustrado anteriormente diversas realizaciones de la invención, un experto en la técnica entenderá que variaciones y mejoras hechas en las realizaciones ilustrativas caen dentro del alcance de la invención, y el alcance de la invención está sólo limitado por las reivindicaciones que se acompañan y sus equivalentes.

**REIVINDICACIONES**

1. Un método de autenticación para verificar contraseña introducida por un usuario, que comprende los siguientes pasos:

(1) correspondiendo con un conjunto conocido de caracteres contenido en una contraseña predefinida, definir un conjunto candidato de caracteres construido por una pluralidad de caracteres, siendo dicho conjunto conocido de caracteres un subconjunto del conjunto candidato de caracteres;

(2) distribuir aleatoriamente todos los caracteres del conjunto candidato de caracteres en una pluralidad de subconjuntos candidatos de caracteres tal que cada subconjunto candidato de caracteres incluya dos o más caracteres, y distribuir y representar visualmente todos los subconjuntos candidatos de caracteres en una pluralidad de regiones interactivas (31-34) respectivamente; y

(3) recibir del usuario instrucciones con respecto a la selección de una región interactiva específica (31-34) en base al primer carácter del conjunto conocido de caracteres, comprobando si el primer carácter del conjunto conocido de caracteres pertenece al subconjunto candidato de caracteres correspondiente a la región específica interactiva (31-34) actualmente seleccionada por el usuario;

(4) repetir los pasos (2) a (3) para los caracteres restantes del conjunto conocido de caracteres, y confirmar la autenticación exitosa y emitir señales que indiquen autenticación exitosa cuando todos los caracteres del conjunto conocido de caracteres pertenezcan a los subconjuntos candidatos de caracteres correspondientes a las regiones interactivas específicas (31-34) actualmente seleccionadas por el usuario.

2. El método de autentificación de acuerdo con la reivindicación 1, en el que, en el paso (1), el conjunto conocido de caracteres es equivalente a la recolección de todos los conjuntos candidatos de caracteres.

3. El método de autentificación de acuerdo con la reivindicación 1, en el que cada región interactiva (31-34) se usa para recibir una acción táctil del usuario y confirmar esta acción como las instrucciones del usuario de seleccionar una región interactiva correspondiente (31-34).

4. El método de autentificación de acuerdo con la reivindicación 1, en el que cada región interactiva (31-34) está asociada con un correspondiente circuito (2) de entrada, y la conmutación de cada circuito (2) de entrada se transforma en instrucciones de selección de una región interactiva (31-34) asociada con el circuito (31-34) de entrada.

5. El método de autentificación de acuerdo con la reivindicación 1, en el que, correspondiendo a cualquier carácter del conjunto conocido de caracteres, cuando se comprueba que el carácter actual no está dentro del subconjunto candidato de caracteres correspondiente a una específica región interactiva (31-34) seleccionada actualmente por el usuario, el método se termina para detener la ejecución de los siguientes pasos.

6. Un dispositivo de autentificación para realizar el método de acuerdo con una cualquiera de las reivindicaciones anteriores 1-3 y 5, que comprende una unidad (1) de control, una unidad (5) de memoria y una pantalla táctil (3), almacenando dicha unidad (5) de memoria la contraseña predefinida que contiene el conjunto conocido de caracteres en ella, en el que la unidad (1) de control está destinada a ejecutar un programa implantado por dicho método; la unidad (5) de memoria está destinada a almacenar el programa implantado por dicho método; y la pantalla táctil (3) está destinada a proporcionar dichas regiones interactivas (31-34) al programa implantado por dicho método, para recibir la selección de usuario de las regiones interactivas (31-34) y transformar dicha selección en instrucciones que indican la selección de las específicas regiones interactivas (31-34).

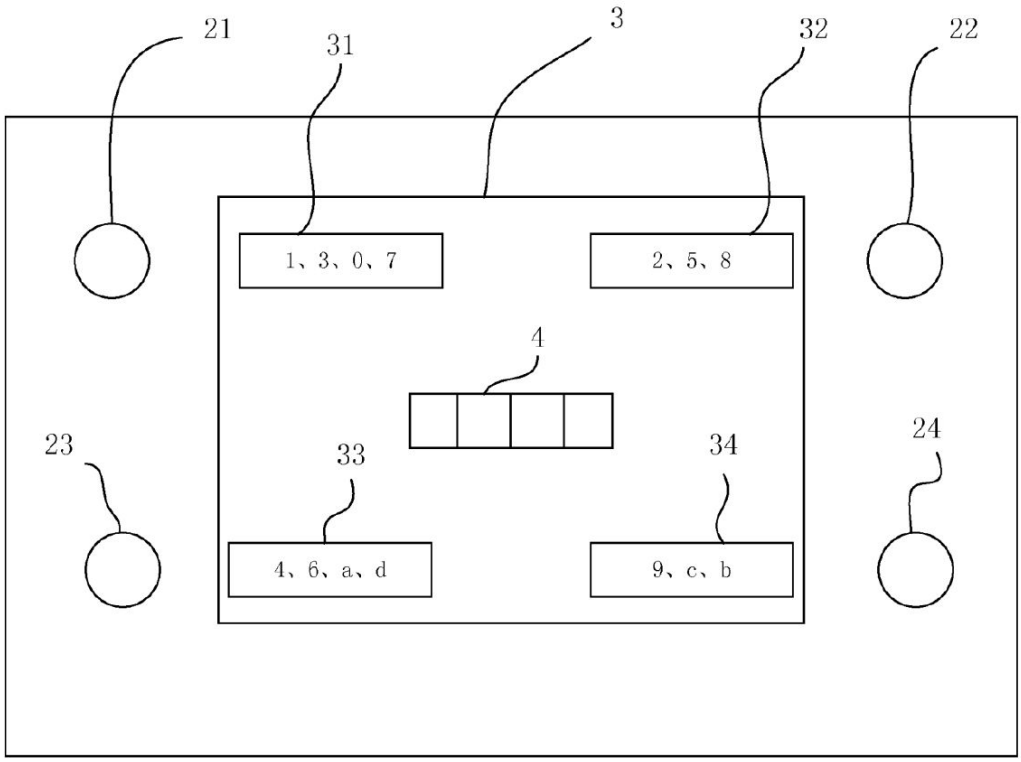


Figura 1

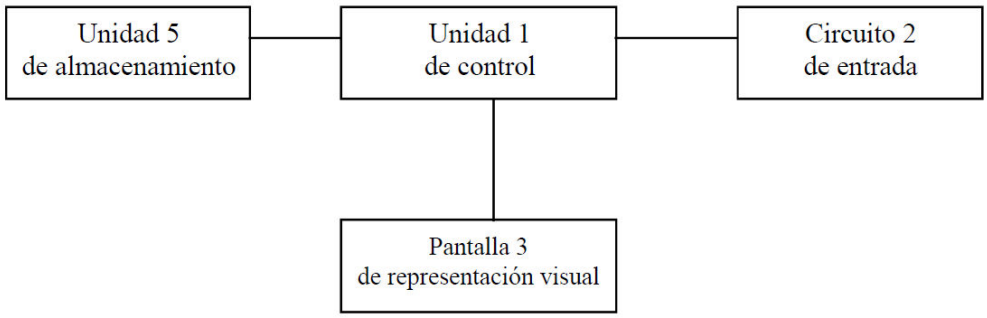


Figura 2