(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 673 641**

(51) Int. CI.:

G06F 21/36 (2013.01)
G06F 3/048 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.03.2011 E 11160566 (3)**

(97) Fecha y número de publicación de la concesión europea: **09.05.2018 EP 2386974**

(54) Título: **Método y dispositivo para generar un valor secreto**

(30) Prioridad:

11.05.2010 EP 10305497

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.06.2018

(73) Titular/es:

THOMSON LICENSING (100.0%)
1-5, rue Jeanne d'Arc
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

ALESSIO, DAVIDE;
DESOBLIN, GILLES;
ELUARD, MARC y
MAETZ, YVES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y dispositivo para generar un valor secreto

Campo técnico

La presente invención se refiere de forma general a la autentificación de usuarios y, de forma más específica, a contraseñas gráficas.

Antecedentes

Esta sección sirve para introducir al lector en diversos aspectos de la técnica, que pueden estar relacionados con varios aspectos de la presente invención descritos y/o reivindicados más adelante. Se cree que esta descripción resultará útil para dotar al lector de información de antecedentes a efectos de facilitar una mejor comprensión de los diversos aspectos de la presente invención. En consecuencia, se entenderá que lo anteriormente descrito se interpretará de forma correspondiente, y no como un reconocimiento de la técnica anterior.

Una práctica utilizada desde hace tiempo consiste en el uso de contraseñas para proteger el acceso a diversos dispositivos, tal como, por ejemplo, ordenadores y teléfonos móviles. El sistema de contraseña más habitual requiere que un usuario utilice el teclado para introducir una cadena de caracteres. Un problema de estas contraseñas seguras, es decir, contraseñas difíciles de descifrar, consiste en que, con frecuencia, son difíciles de recordar y viceversa.

Debido a que, normalmente, es más fácil recordar imágenes que texto, diversas soluciones proponen el uso de contraseñas gráficas. Además, numerosos dispositivos nuevos no tienen ningún teclado físico. Por ejemplo, los teléfonos inteligentes solamente comprenden una pantalla táctil como dispositivo de entrada. En este caso, es necesario usar un teclado virtual para introducir una contraseña de texto. Su uso no resulta muy fácil por parte de un usuario, especialmente al usar contraseñas seguras (una mezcla de caracteres alfanuméricos con mayúsculas y minúsculas).

US 2009/0046929 describe un método de autentificación de imágenes gráficas en el que una imagen se divide en segmentos que comprenden una imagen secundaria y asociados a un código. El usuario crea la imagen final y el código final correspondiente seleccionando el grupo de imágenes secundarias.

En US 5559961 Blonder da a conocer una técnica en la que un usuario introduce la contraseña haciendo clic en una secuencia de zonas predeterminadas en una imagen predeterminada. US 2004/010721 da a conocer una solución similar.

Passlogix ha desarrollado esta idea en "Graphical Passwords: A Survey", Department of Computer Science, Georgia State University - http://www.acsac.org/2005/papers/89.pdf, de Suo y col. Para introducir una contraseña, los usuarios hacen clic en diversos elementos en una imagen en una secuencia predefinida.

S. Wiedenbeck y col. también desarrollan el sistema de Blonder en diversos artículos:

- "Authentication Using Graphical Passwords: Basic Results", en Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.
- "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", en Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.
- "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System", International Journal of Human Computer Studies, vol. 63, 2005, páginas 102-127.

Este sistema eliminaba límites predefinidos y permitía el uso de imágenes arbitrarias, de modo que un usuario puede hacer clic en cualquier posición en una imagen para crear una contraseña.

También según Suo y col., Passpoint desarrolló un sistema en el que se introduce una contraseña seleccionando una cara entre varias una pluralidad de veces.

Aunque estos sistemas funcionan razonablemente bien, los mismos presentan algunos inconvenientes, tales como vulnerabilidad a mirones: un intruso puede obtener la contraseña observando las selecciones/clics realizados por el usuario.

Por lo tanto, resulta evidente que existe la necesidad de una solución que permita superar este problema y que permita obtener un sistema con contraseñas gráficas a prueba de mirones. La presente invención da a conocer una solución de este tipo.

Resumen de la invención

En un primer aspecto, la invención se refiere a un método para generar un valor secreto. Un dispositivo visualiza una imagen inicial que comprende una pluralidad de elementos gráficos, teniendo cada elemento gráfico al menos dos variantes; recibe iterativamente una entrada de usuario para seleccionar una variante de un número de los elementos gráficos, generando de este modo una imagen modificada; y genera el valor secreto a partir de al menos las variantes seleccionadas de los elementos gráficos.

En una primera realización preferida, el valor secreto es una contraseña.

En una segunda realización preferida, el dispositivo recibe una entrada de usuario para la selección de la imagen inicial, que también se usa para la generación del valor secreto.

En una tercera realización preferida, las imágenes gráficas se integran continuamente en la imagen inicial y la imagen modificada.

En una cuarta realización preferida, una entrada de usuario comprende la selección de un elemento gráfico y se proporciona al menos una variante en respuesta.

En una quinta realización preferida, la entrada de usuario para seleccionar una variante comprende una oferta simultánea de todas las variantes de un elemento gráfico para el usuario.

En un segundo aspecto, la invención se refiere a un dispositivo para generar un valor secreto. El dispositivo comprende un procesador para proporcionar una pantalla con una imagen inicial que comprende una pluralidad de elementos gráficos, teniendo cada elemento gráfico al menos dos variantes; recibir una entrada de usuario iterativa para seleccionar una variante de un número de los elementos gráficos, generando de este modo una imagen modificada; y generar el valor secreto a partir de al menos las variantes seleccionadas de los elementos gráficos.

En una primera realización preferida, el valor secreto es una contraseña.

En una segunda realización preferida, el procesador también recibe una entrada de usuario para la selección de la imagen inicial, siendo usada también por el procesador para la generación del valor secreto.

En una tercera realización preferida, el procesador también integra continuamente las variantes en la imagen inicial para generar la imagen modificada.

En una cuarta realización preferida, una entrada de usuario comprende la selección de un elemento gráfico y el procesador también está adaptado para proporcionar al menos una variante en respuesta. Resulta ventajoso que el procesador también esté adaptado para proporcionar todas las variantes del elemento gráfico seleccionado en respuesta a una entrada de usuario para seleccionar una variante.

En una quinta realización preferida, el procesador también está adaptado para proporcionar además el elemento gráfico visualizado originalmente.

Breve descripción de los dibujos

A continuación se describirán características preferidas de la presente invención, a título de ejemplo no limitativo, haciendo referencia a los dibujos que se acompañan, en los que:

la Figura 1 muestra un ejemplo de cómo es posible cambiar una imagen para generar una contraseña;

la Figura 2 muestra una pantalla ilustrativa para la introducción de una contraseña;

la Figura 3 muestra un diagrama de bloques de un aparato según una realización preferida de la presente invención;

la Figura 4 muestra ejemplos de diferentes elementos gráficos de una imagen;

la Figura 5 muestra cómo es posible cambiar los elementos gráficos;

la Figura 6 muestra la interacción preferida entre las fases de inscripción;

la Figura 7 muestra una pantalla ilustrativa durante la fase de inscripción restante;

la Figura 8 muestra una pantalla ilustrativa durante la fase de inscripción de error;

la Figura 9 muestra una variante de realización de entrada de usuario; y

la Figura 10 muestra un diagrama de flujo de un método para la generación de una contraseña según una

realización preferida de la presente invención.

Descripción de realizaciones

Una idea principal de la presente invención consiste en generar un secreto (tal como una contraseña) interactuando con una imagen inicial, modificando uno o más elementos gráficos en la misma, por ejemplo, una ventana, gente, vehículos y un cartel de una tienda. Los elementos gráficos pueden modificarse haciendo clic en los mismos, y cada clic puede sustituir el presente elemento gráfico por otro elemento gráfico predefinido que, preferiblemente, se integra continuamente en la imagen inicial. El secreto depende de la imagen final, que es diferente de la imagen inicial y se crea mediante la interacción por parte del usuario con el elemento gráfico. Debido a que el cerebro humano almacena las imágenes en el área de memoria a largo plazo, la probabilidad de recordar con éxito el secreto aumenta.

La Figura 1 muestra cómo es posible cambiar una imagen para generar una contraseña. La mitad superior de la Figura 1 muestra una imagen original visualizada cuando se requiere que el usuario introduzca su secreto. De este modo, el usuario hace clic en diversas áreas de la imagen para modificarla, y la contraseña se deriva de la imagen final mostrada en la mitad inferior de la Figura 1. A título de ejemplo, cuando el usuario hace clic en la calle vacía (un elemento gráfico), se mostrará un autobús (el siguiente elemento gráfico predefinido), al hacer un nuevo clic, se mostrará un taxi, y así hasta que se muestra el coche deportivo amarillo que puede observarse en la imagen final. En total, existen otras diez diferencias entre las dos versiones, diferencias que se usan para generar la contraseña.

Todos los elementos gráficos están predefinidos e integrados en el sistema. Por lo tanto, tal como podrá observarse, resulta bastante difícil notar las diferencias, de forma específica, si el intruso no ha visto la imagen anteriormente, lo que significa que se obtiene una buena protección contra ataques de mirones, siendo la excepción el uso de cámaras para registrar las modificaciones (y/o la imagen final).

La descripción de la presente memoria se centra en la introducción de una contraseña, aunque se entenderá que son posibles otros usos de un secreto así generado en diversos sistemas criptográficos (p. ej., teclas de encriptación secreta), pudiendo necesitar dichos usos otros mecanismos de derivación.

Realización preferida

Tal como ya se ha mencionado, la realización preferida se refiere a la introducción de un secreto aplicado al campo de las contraseñas. A efectos de simplicidad, se considera que la imagen final es la contraseña.

Todos los elementos gráficos están predefinidos e integrados en el sistema, es decir, preferiblemente, no es posible que un intruso vea cuáles son los elementos gráficos. Además, las imágenes se seleccionan preferiblemente de forma correcta a efectos de obtener una buena variedad de posibilidades de modificación. Por ejemplo, un sol naciente en una playa vacía resultaría bastante limitativo, mientras que una calle de una ciudad ofrece numerosos elementos diferentes a modificar.

La Figura 2 muestra una pantalla ilustrativa para la introducción de contraseñas. Cuando se solicita al usuario en primer lugar la introducción de su contraseña, la pantalla comprende la imagen inicial, un botón de validación, un botón de reinicio y, posiblemente, un botón para cambiar a otro usuario.

La Figura 3 muestra un diagrama de bloques de un aparato según una realización preferida de la presente invención. El aparato 300 comprende una pantalla 310 de visualización adaptada para mostrar las imágenes y pantallas mostradas, por ejemplo, en las Figuras 1 y 2. El aparato 300 comprende además al menos un procesador 320 (en adelante “procesador”), al menos una memoria 330 y medios 340 de entrada de usuario. Los medios 340 de entrada de usuario pueden ser la pantalla 310 de visualización, si es táctil, aunque, por ejemplo, también pueden ser un ratón y/o un teclado. El procesador está adaptado para llevar a cabo los métodos de la invención, tales como modificar elementos gráficos a voluntad del usuario y generar la contraseña. Se entenderá que el aparato 300 también puede actuar como un terminal sin inteligencia que transmite al menos parte de las interacciones entre un usuario y un servidor externo. También se entenderá que el aparato 300 puede estar implementado como una pluralidad de dispositivos, por ejemplo, una pantalla, una interfaz de usuario y un dispositivo de computación que comprende el procesador 320 y suministra imágenes a la pantalla y recibe una entrada de usuario de la interfaz de usuario.

La Figura 4 muestra los diferentes elementos gráficos de la imagen, representándose cada elemento gráfico como un rectángulo ilustrativo. Estos elementos gráficos también pueden ser indicados al usuario para facilitar la selección, por ejemplo, la primera vez que se selecciona la contraseña. Además, tal como se muestra en la Figura 4, es posible destacar el elemento gráfico ‘presente’.

La Figura 5 muestra cómo es posible cambiar los elementos gráficos haciendo clic en los mismos. Cada vez que el usuario hace clic en el elemento gráfico, se muestra la siguiente “versión” del elemento gráfico, sustituyendo el previo. La Figura 5 muestra cómo tres clics sucesivos afectan el elemento gráfico en la zona del cartel de parada de autobús, en la parte derecha inferior de la imagen original. El orden de presentación

de los elementos gráficos puede ser fijo y predefinido o dinámico y aleatorio.

Cuando el usuario ha restablecido la imagen final modificando los elementos gráficos, se pulsa el botón de validación y se comprueba la contraseña. De hecho, si la imagen visualizada es la misma que la imagen final, la contraseña se verifica exitosamente, con lo cual, por ejemplo, se obtiene un acceso.

Si el usuario comete un error durante la introducción de la contraseña, es posible pulsar el botón de reinicio, que restablece la imagen inicial y cancela las modificaciones ya realizadas.

La inscripción se produce cuando un nuevo usuario (sin contraseña) crea una contraseña o cuando un usuario existente genera una nueva contraseña. De forma ventajosa, la inscripción comprende las fases de:

- Selección: el usuario interactúa para seleccionar la contraseña
- Recordatorio: la contraseña se muestra al usuario
- Práctica: el usuario practica la introducción de la contraseña
- Error: el usuario cometió un error durante la práctica

La Figura 6 muestra la interacción preferida entre las fases de inscripción.

La inscripción se inicia con una selección 610 de contraseña, en la que puede visualizarse una pantalla, tal como la mostrada en la Figura 4, a efectos de permitir al usuario identificar elementos gráficos. Si el usuario hace clic en el elemento gráfico 'presente' (el destacado en la Figura 4), el mismo se modifica, tal como se ha descrito anteriormente en la presente memoria. La pantalla de la Figura 4 también comprende un indicador de la seguridad de la contraseña, cuyo valor depende de forma ventajosa del número total de elementos gráficos modificables, del número de alternativas para cada elemento gráfico y del número de elementos gráficos ya modificados por el usuario.

Si el usuario comete un error, es posible empezar por el principio usando el botón "reinicio"; como alternativa, un botón "deshacer" permite cancelar la última acción.

Cuando el usuario está satisfecho con la imagen resultante, la contraseña puede validarse seleccionando el botón "validar", tras lo cual se inicia la fase 620 de recordatorio.

En la fase 620 de recordatorio, la imagen seleccionada se visualiza con los elementos gráficos modificados destacados, tal como se muestra en la Figura 7. De este modo, el usuario tiene la opción de validar la contraseña (finalizando de este modo la inscripción), reiniciar la contraseña (para volver a la fase 610 de selección de contraseña) o practicar la contraseña. En este último caso, se inicia la fase 630 de práctica.

En la fase 630 de práctica de contraseña, el usuario puede practicar la introducción de la contraseña. El usuario puede cancelar la práctica para volver a la fase 620 de recordatorio de contraseña a efectos de ver la contraseña seleccionada. La práctica exitosa también da lugar al retorno a la fase 620 de recordatorio de contraseña, mientras que la práctica no exitosa da lugar al paso a la fase 640 de error, en la que se visualizan los errores, tal como se muestra en la Figura 8, antes de volver a la práctica 630 de contraseña para realizar otro intento.

En la fase 640 de error es preferible indicar los elementos gráficos seleccionados correctamente de una manera y los elementos gráficos seleccionados incorrectamente de otra manera.

Espacio de contraseña

Para mejorar el espacio de la contraseña, es posible tener en cuenta el orden de selección de los elementos gráficos. En este caso, el secreto no se deriva de la imagen final, sino de la interacción en su conjunto, que va de la imagen inicial a la imagen final.

El tamaño del espacio de la contraseña puede calcularse tal como sigue: una imagen tiene e zonas sensibles (elementos gráficos) que tienen cada una v posibles variaciones. Para simplificar la notación y las fórmulas, se asumirá que todas las zonas tienen el mismo número de posibles variaciones; este grupo de variaciones "alfabeto de símbolos" para una zona se indica como e_i. También existe un estado adicional para cada zona: el estado inicial (por defecto), no considerado en el alfabeto.

Para introducir una contraseña, el usuario modifica en la imagen un número n de zonas, mientras que las zonas e-n restantes se dejan en el estado por defecto.

El tamaño Ω del espacio de contraseña para un n determinado, teniendo en cuenta la hipótesis de que el orden en el que se modifican las zonas no importa, está determinado por el número de múltiplos de n multiplicado por el número de todos los posibles estados de las zonas seleccionadas, de modo que se

obtiene:

$$\Omega = \binom{e}{n} v^n$$

Si también se tiene en cuenta el orden de entrada, entonces el tamaño Ω del espacio de contraseña para un *n* determinado se obtiene mediante:

$$\Omega = \binom{e}{n} n! \cdot v^n = \frac{e!}{(e-n)!} v^n$$

El tamaño Ω de la totalidad del espacio de contraseña, sumando con respecto a *n* en el intervalo [0, ..., e], viene dado, en el primer caso (no ordenado), por:

$$\Omega = \sum_{n=0}^{e} \binom{e}{n} v^n = (1+v)^e$$

En el segundo caso (ordenado), el tamaño Ω de la totalidad del espacio de contraseña, sumando con respecto a *n* en el intervalo [0, ..., e], viene dado por:

$$\Omega = \sum_{n=0}^{e} \binom{e}{n} n! \cdot v^n = \sum_{n=0}^{e} \frac{e!}{(e-n)!} v^n = 1 + ev + e(e-1)v^2 + \ \ldots + e!\, v^e.$$

Se entenderá que, en ambos casos, Ω crece exponencialmente con el número de zonas sensibles.

Las fórmulas son bastante similares a las usadas para códigos PIN (o contraseñas clásicas), constituyendo una diferencia principal un nuevo elemento: la selección de la zona modificada. La seguridad de los códigos PIN y de las contraseñas clásicas se basa en el tamaño y la longitud del alfabeto. Una contraseña gráfica que permite seleccionar “dónde” modificar la contraseña (y dónde no hacerlo) permite una mayor variabilidad para un tamaño de un alfabeto de símbolos y una longitud (número de zonas modificadas) determinados. Esta selección se representa mediante el coeficiente binomial y contribuye positivamente al espacio de la contraseña.

A continuación se describirá un ejemplo comparativo con un código PIN. Un código PIN de 4 dígitos tiene un alfabeto de 10 elementos (dígitos) y 4 zonas modificables, obteniéndose un total de 10000 posibilidades. Usando los mismos parámetros numéricos en el contexto de una contraseña gráfica con una imagen de aproximadamente 30 zonas modificables, se obtienen:

$$\binom{30}{4} \cdot 10^4 = 27\,405 \cdot 10\,000 = 274\,050\,000$$

posibilidades.

Incluso una imagen más sencilla, por ejemplo, solamente con 8 zonas modificables, permite obtener una mejora remarcable en el espacio de contraseña:

$$\binom{8}{4} \cdot 10^4 = 70 \cdot 10\,000 = 700\,000.$$

Estos números también pueden ser más grandes (en un factor de 24) si se tiene en cuenta el orden.

En teoría, las contraseñas gráficas son seguras, o más seguras, en comparación con una contraseña clásica, siempre que se seleccione un “alfabeto” adecuado para las variaciones. Esto se verifica fácilmente observando el comportamiento asintótico de las fórmulas usadas. En contraseñas textuales clásicas, es muy habitual usar símbolos ASCII alfanuméricos, obteniéndose un tamaño de alfabeto de 62 (minúsculas, mayúsculas y dígitos). En el contexto de contraseñas gráficas, los símbolos del alfabeto son imágenes u objetos y su número es prácticamente ilimitado. Por otro lado, en un uso práctico de un sistema de este tipo, el grupo de variaciones no puede ser tan grande como en las contraseñas clásicas sensibles a

mayúsculas/minúsculas.

Comparando los dos sistemas numéricamente: por ejemplo, para obtener un espacio de contraseña aproximadamente con el mismo tamaño que una contraseña alfanumérica sensible a mayúsculas/minúsculas de 8 caracteres (sugerencia habitual en páginas web), es posible usar 12 zonas modificadas con un alfabeto de 16 elementos; numéricamente, $62^8 \approx 16^{12}$. No obstante, debe observarse que estos números no tienen en cuenta el factor debido a la selección del subconjunto de zonas modificadas entre las zonas disponibles (por ejemplo, aproximadamente 30), lo que supone una ventaja para la contraseña gráfica. También debe observarse que un sistema con estos parámetros podría aproximarse al límite práctico de este sistema de contraseña gráfica, ya que la representación de 16 (o más) elementos en la pantalla puede resultar confusa, aunque a este nivel sigue siendo factible.

Como una primera variante, el sistema propone diferentes imágenes iniciales, en vez de una única, otorgando de este modo al usuario la capacidad de seleccionar una imagen antes de modificarla para introducir la contraseña. Por lo tanto, es posible mejorar el espacio de contraseña.

Como una segunda variante, todos los posibles elementos gráficos se muestran al hacer clic en los mismos. Esta posibilidad se muestra en la Figura 9. La segunda variante puede permitir entradas más rápidas (ya que no son necesarios más de dos clics para seleccionar el elemento gráfico), aunque debe observarse que es menos resistente a mirones.

La Figura 10 muestra un diagrama de flujo de un método para la generación de una contraseña según una realización preferida de la presente invención. El método se inicia en la etapa 1010, a la que sigue la etapa opcional de seleccionar 1020 la imagen inicial. La entrada de usuario se recibe para modificar 1030 un elemento gráfico y el elemento gráfico seleccionado se muestra al usuario. Debe observarse que el elemento gráfico seleccionado no es necesariamente el elemento gráfico seleccionado por el usuario; siendo posible su cambio. También debe observarse que es posible que el elemento gráfico visualizado inicialmente se muestre después de un número de clics, en cuyo caso, dependiendo de la implementación, este elemento gráfico puede considerarse o no considerarse un elemento gráfico modificado.

A continuación, en la etapa 1040, se verifica si la contraseña es completa, por ejemplo, comprobando si el usuario ha validado la contraseña. Si este no es el caso, el método vuelve a la modificación de un elemento gráfico. No obstante, si la contraseña es completa, se genera la contraseña 1050. Por ejemplo, la forma de la contraseña generada puede ser una lista de los elementos gráficos seleccionados, una combinación de los elementos gráficos (seleccionados o en su totalidad) o una combinación de la imagen final entera.

Se entenderá que el presente sistema permite obtener un sistema de contraseña gráfica que:

- Permite reducir el riesgo de ataques de diccionario. De hecho, las palabras comunes representan un gran subconjunto en un espacio de contraseña textual válido y, con frecuencia, se usan para reducir el esfuerzo de memorización de contraseñas. Este subconjunto resulta con frecuencia bien conocido y compartido con la gente. En el contexto de una contraseña gráfica, unos pocos elementos gráficos, en caso de estar presentes, son “mejores” o “más probables” que otros.

- Permite obtener un buen nivel de seguridad de manera sencilla y familiar. Por ejemplo, es posible su uso por parte de gente mayor con problemas de visión o por parte de niños antes de aprender a leer y escribir.

- Permite el uso de contraseñas más largas, ya que es relativamente fácil asociar imágenes y relaciones entre objetos en una configuración de imagen específica. De hecho, las personas usan la memoria a largo plazo para almacenar imágenes, permitiendo de este modo recordar mejor las imágenes en comparación con el texto.

- Permite su uso con dispositivos sin teclados que pueden ser difíciles de usar.

- Puede ser menos sensible a técnicas de ingreso mediante clic básicas y más resistente a mirones.

Cada característica descrita en la descripción y en las reivindicaciones y en los dibujos (en caso adecuado) puede usarse independientemente o según cualquier combinación adecuada. Los números de referencia que aparecen en las reivindicaciones son únicamente ilustrativos y no tendrán ningún efecto limitativo en el alcance de las reivindicaciones.

REIVINDICACIONES

1. Método para generar un valor secreto, comprendiendo el método las etapas en un dispositivo (300) de:

- visualizar una imagen inicial que comprende una pluralidad de elementos gráficos, teniendo cada elemento gráfico al menos dos variantes;
- recibir (1030) iterativamente una entrada de usuario en un elemento gráfico para seleccionar una variante de un número de los elementos gráficos, generando de este modo una imagen modificada; y
- generar (1050) el valor secreto a partir de al menos las variantes seleccionadas de los elementos gráficos.

2. Método según la reivindicación 1, en el que el valor secreto es una contraseña.

3. Método según la reivindicación 1, que comprende además una etapa de recibir una entrada de usuario para la selección de la imagen inicial, usándose también la imagen inicial seleccionada para la generación del valor secreto.

4. Método según la reivindicación 1, en el que los elementos gráficos se integran continuamente en la imagen inicial y la imagen modificada.

5. Método según la reivindicación 1, en el que una entrada de usuario comprende la selección de un elemento gráfico y el método comprende además la etapa de proporcionar al menos una variante en respuesta.

6. Método según la reivindicación 5, en el que la etapa de proporcionar comprende proporcionar simultáneamente todas las variantes del elemento gráfico seleccionado al usuario.

7. Dispositivo (300) para generar un valor secreto, comprendiendo el dispositivo (300) un procesador (320) para:

- proporcionar una pantalla (310) con una imagen inicial que comprende una pluralidad de elementos gráficos, teniendo cada elemento gráfico al menos dos variantes;
- recibir una entrada de usuario iterativa en un elemento gráfico para seleccionar una variante de un número de los elementos gráficos, generando de este modo una imagen modificada; y
- generar el valor secreto a partir de al menos las variantes seleccionadas de los elementos gráficos.

8. Dispositivo según la reivindicación 7, en el que el valor secreto es una contraseña.

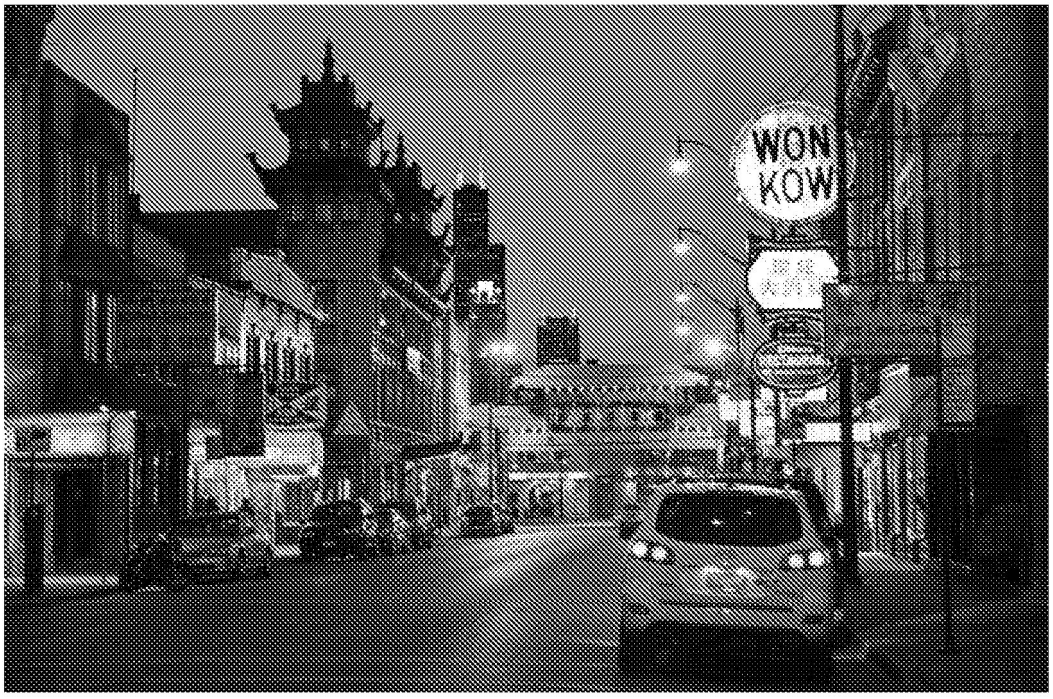
9. Dispositivo según la reivindicación 7, en el que el procesador (320) también recibe una entrada de usuario para la selección de la imagen inicial, usando también el procesador (320) la imagen inicial seleccionada para la generación del valor secreto.

10. Dispositivo según la reivindicación 7, en el que el procesador también integra continuamente las variantes en la imagen inicial para generar la imagen modificada.

11. Dispositivo según la reivindicación 7, en el que una entrada de usuario comprende la selección de un elemento gráfico y el procesador también está adaptado para proporcionar al menos una variante en respuesta.

12. Dispositivo según la reivindicación 11, en el que el procesador también está adaptado para proporcionar todas las variantes del elemento gráfico seleccionado en respuesta a una entrada de usuario para seleccionar una variante.

13. Dispositivo según la reivindicación 7, en el que el procesador también está adaptado para proporcionar además el elemento gráfico visualizado originalmente.



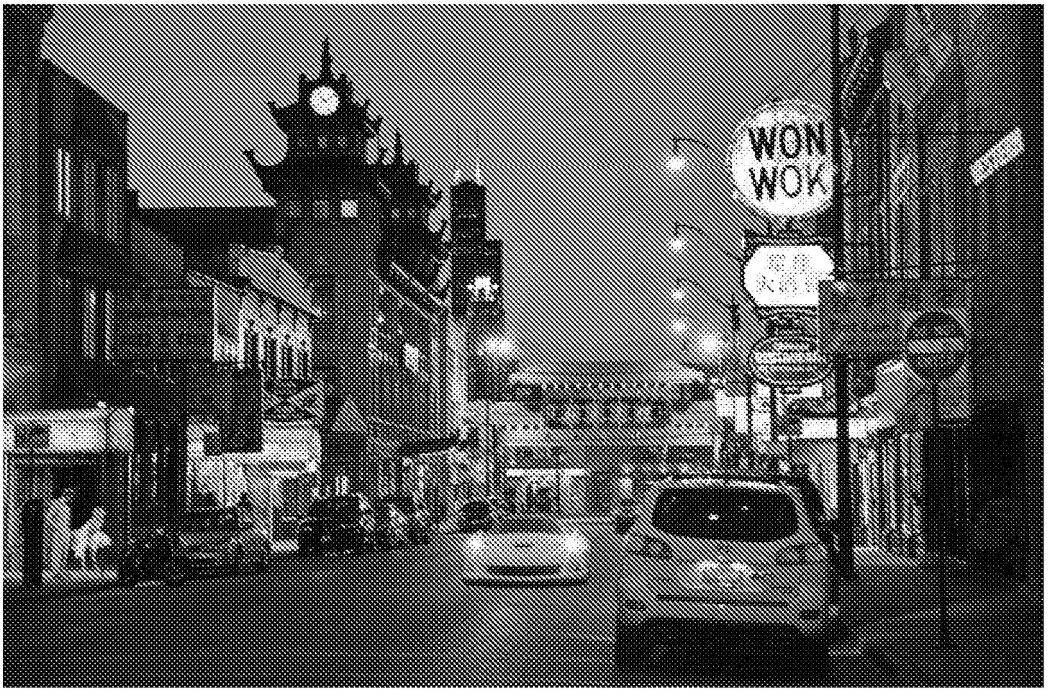


Figura 1

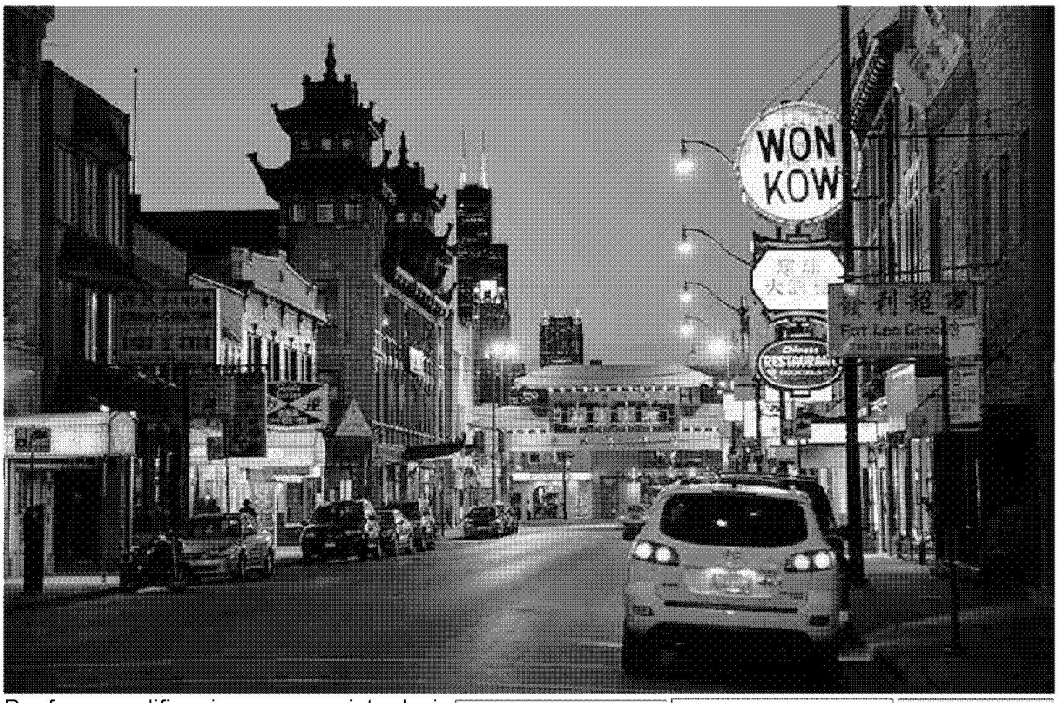


Figura 2

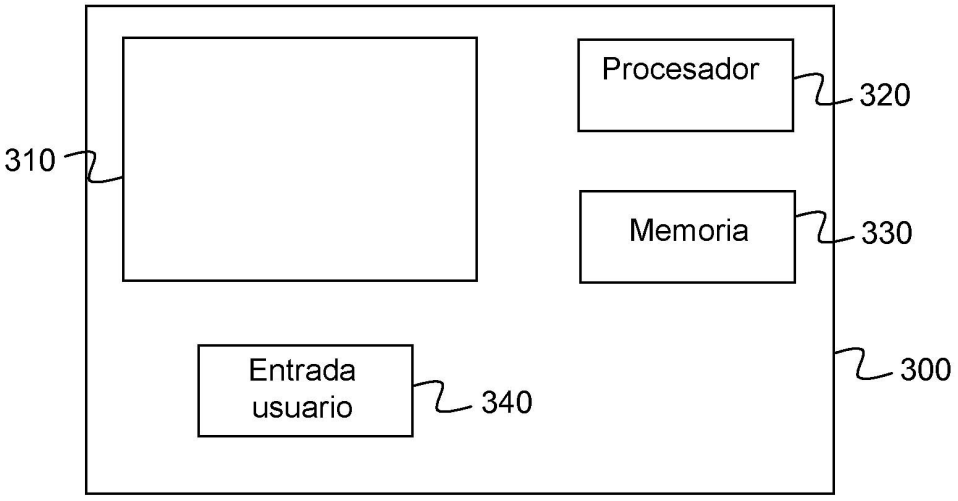


Figura 3

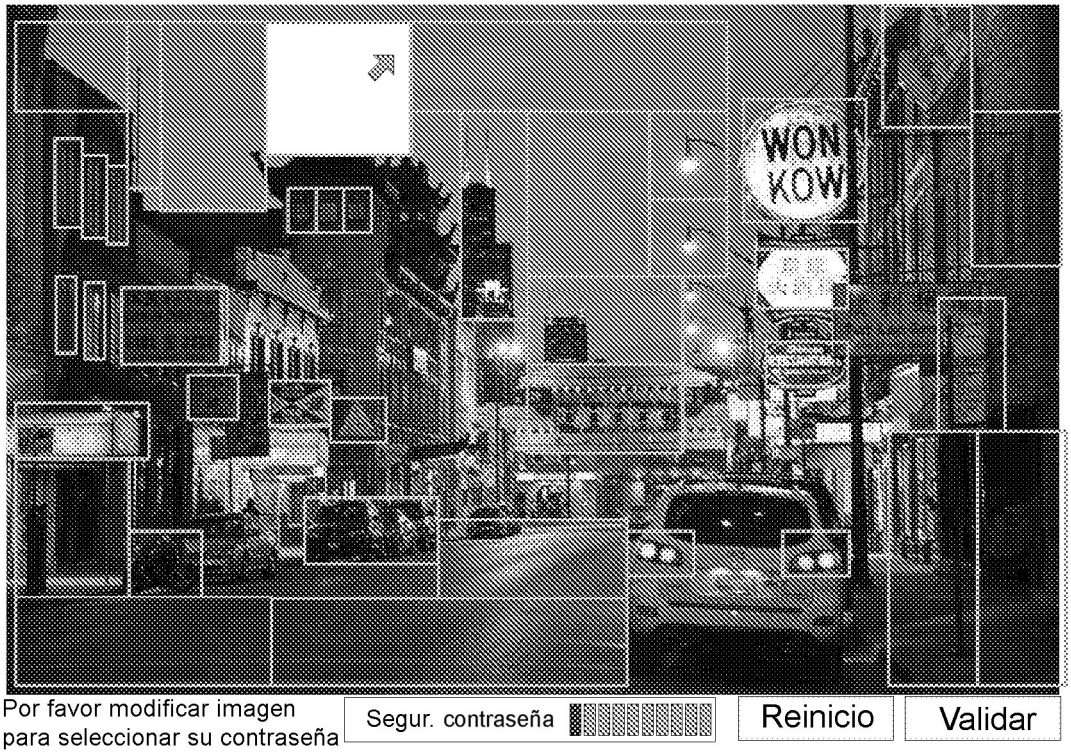


Figura 4

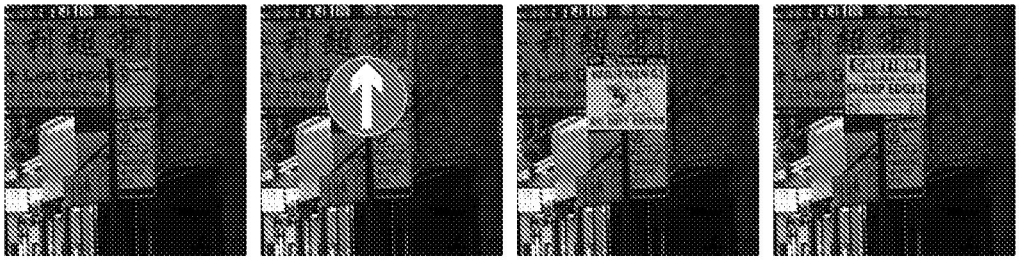


Figura 5

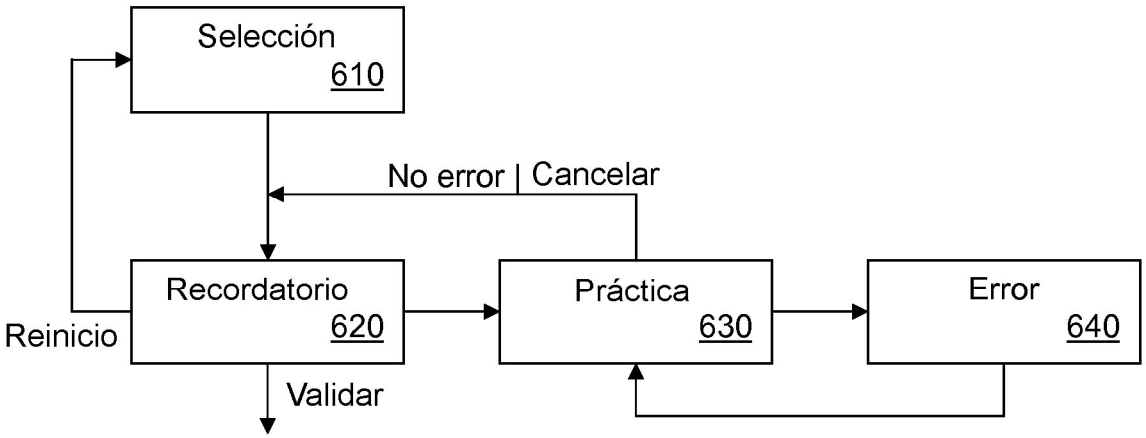
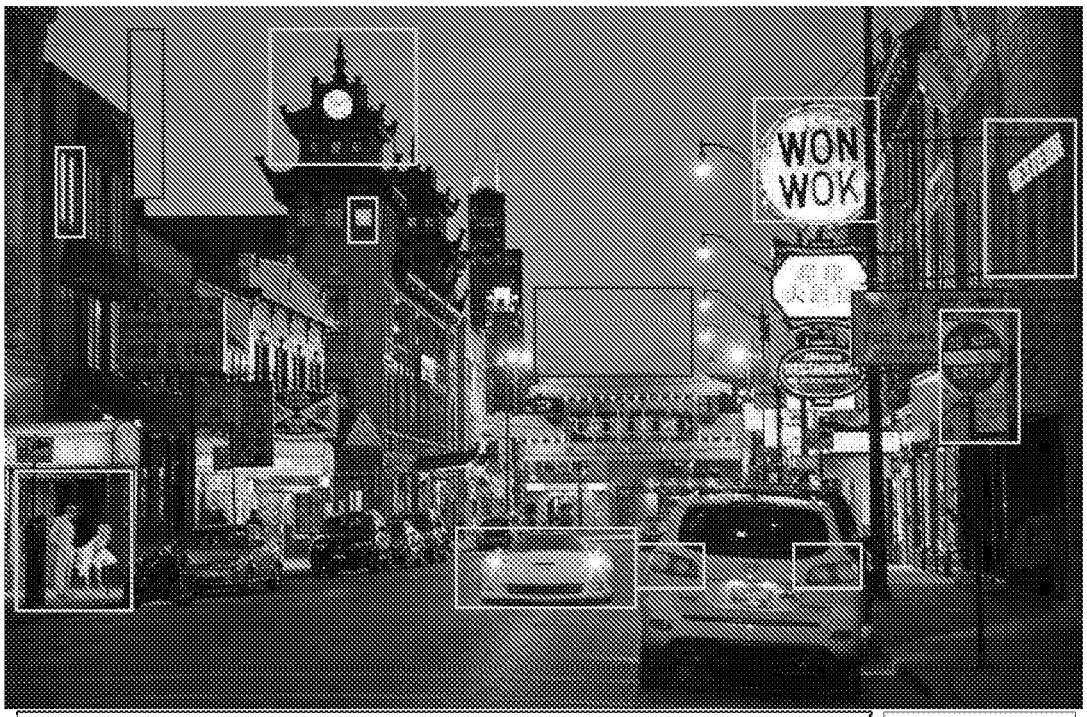


Figura 6

Figura 7



Cometió 2 errores, por favor practicar nuevamente

Practicar nuev.

Figura 8

Figura 9

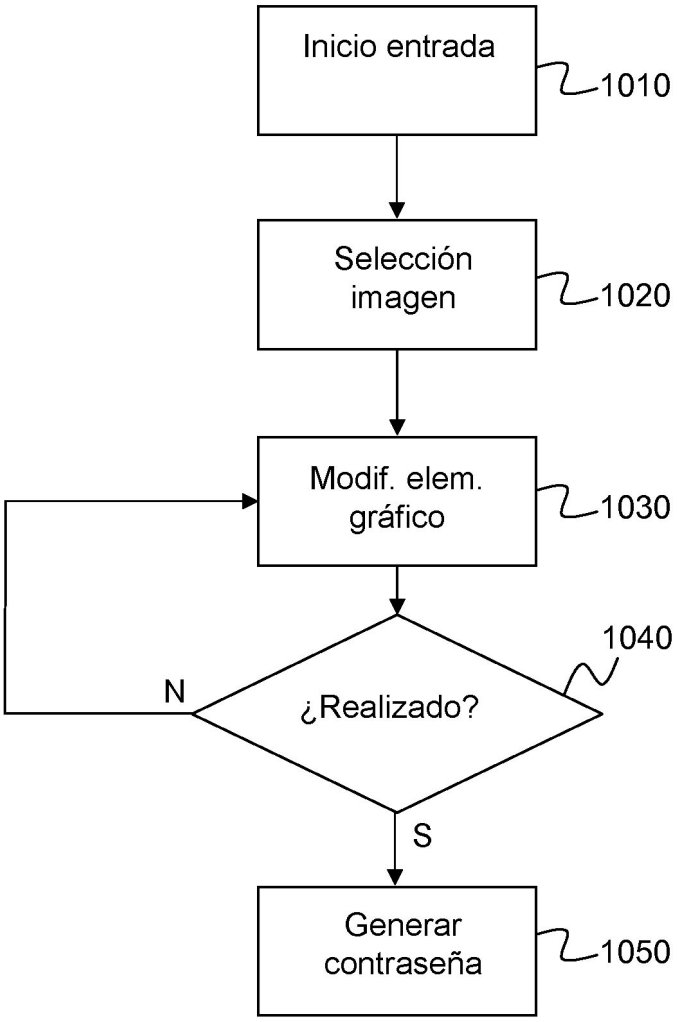

Inicio entrada
1010
Selección imagen
1020
Modif. elem. gráfico
1030
¿Realizado?
1040
N
S
Generar contraseña
1050

Figura 10