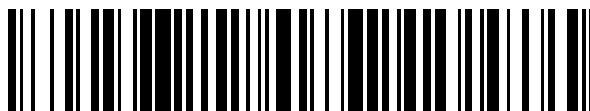


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 780 393**

51 Int. Cl.:

G06F 21/36

(2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.04.2013** **PCT/US2013/037973**

87 Fecha y número de publicación internacional: **31.10.2013** **WO13163285**

96 Fecha de presentación y número de la solicitud europea: **24.04.2013** **E 13781105 (5)**

97 Fecha y número de publicación de la concesión europea: **25.12.2019** **EP 2842069**

54 Título: **Sistema de introducción de contraseña resistente al fraude**

30 Prioridad:

25.04.2012 US 201261638223 P

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

25.08.2020

73 Titular/es:

ARCANUM TECHNOLOGY LLC (100.0%)
630 Olympic Drive, Suite C
Athens, GA 30601, US

72 Inventor/es:

FINNAN, BRIAN G.;
BRICE, FRANK P. y
BROWN, WILLIAM B.

74 Agente/Representante:

DURAN-CORRETJER, S.L.P

ES 2 780 393 T3

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

DESCRIPCIÓN

Sistema de introducción de contraseña resistente al fraude

5 REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

ANTECEDENTES

10 En el mundo moderno, los sistemas computarizados son responsables de recoger, transmitir y almacenar una cantidad de información cada vez mayor. Estos sistemas son necesarios, ya que la necesidad de acceder a la información de forma rápida y precisa se ha convertido en un factor crítico en las operaciones diarias de las que dependen los negocios y la economía. Aunque los avances tecnológicos han ayudado a proteger los datos confidenciales frente al acceso no autorizado durante su transmisión y almacenamiento, poco ha cambiado en los medios mediante los cuales los individuos autorizados introducen los datos y acceden a los mismos.

15 Gracias a los avances en cifrado y a sistemas informáticos más potentes, el almacenamiento y la transmisión de datos han alcanzado un nivel de seguridad que nunca antes había conocido la civilización humana. Una vez que un sistema recoge los datos, éstos se pueden almacenar y compartir entre otros sistemas con poca o ninguna probabilidad de revelación no autorizada. Incluso los procedimientos altamente técnicos para adquirir datos almacenados o transmitidos que se han protegido adecuadamente, a través de medios no autorizados son poco prácticos en el mejor de los casos, y no plantean ninguna amenaza significativa para la seguridad de los datos.

20 Existen varias debilidades en los procedimientos usados habitualmente para una introducción de datos segura y una transmisión poco segura, todas las cuales se han explotado para poder acceder a información segura. Estas explotaciones varían desde el uso de múltiples dispositivos electrónicos hasta la simple observación. Los puntos más débiles en la gestión de seguridad de datos normalmente son los propios seres humanos y las interfaces humano-máquina (Human-Machine Interface, HMI), a través de las cuales se almacenan los datos y se accede a los mismos.

25 Los individuos siempre deberían proteger cualquier información confidencial para evitar que otros adquieran la información. Dichas medidas incluyen: abstenerse de tratar información confidencial mientras tiene ajustes no seguros, limitar cualquier transporte de información a procedimientos seguros, evitar prácticas de documentación tales como grabar información usando procedimientos no seguros mediante la escritura o almacenamiento en ordenadores personales, proteger los dispositivos de identificación, tales como placas de identidad y tarjetas frente a la pérdida o el robo, y otros procedimientos considerados por la mayoría como prácticas de sentido común.

30 Muchas HMI se diseñan con medidas preparadas para ayudar a evitar la revelación no prevista de información segura. Desafortunadamente, se ha demostrado que muchas de estas medidas son insuficientes, ya que estas interfaces han llegado a ser cada vez más prolíficas en la sociedad. Una práctica de este tipo es ocultar los valores, una vez introducidos, enmascarándolos con un carácter genérico, tal como un asterisco. Aunque esto esconde activamente de los observadores los datos finales proporcionados al sistema, no hace nada para ocultar la acción de seleccionar los valores individuales al introducir los datos. Otra práctica menos común es el reposicionamiento de las teclas virtuales en los dispositivos de visualización gráfica entre usos. Este diseño ayuda a garantizar que la observación de la introducción de datos desde cierta distancia no revelará la información introducida a través de los movimientos del individuo que usa la interfaz. Sin embargo, una vez más, esto no proporciona protección frente a la observación cercana.

35 Uno de los usos más comunes del acceso a datos seguro en la sociedad actual se centra en el uso de cajeros automáticos (Automated Teller Machine, ATM) y en transacciones con tarjetas de débito. A pesar de los procedimientos para proteger el acceso a cuentas financieras, solo en Estados Unidos se roban anualmente millones de dólares mediante fraude de tarjetas de débito y crédito. En el caso de cajeros automáticos y transacciones de débito, la única información requerida para acceder a la cuenta es el número de cuenta y su número de identificación personal (Personal Identification Number, PIN) asociado. De estos dos elementos, solo el PIN es secreto y está controlado por el titular de la cuenta.

40 El PIN, un número de cuatro dígitos, solo permite diez mil combinaciones posibles. Adicionalmente, algunas combinaciones del PIN se prefieren estadísticamente sobre otras, debido a su facilidad para recordarlas, su asociación con patrones físicos en el teclado numérico usado durante la introducción del PIN, y la asociación de números con grupos de letras, permitiendo traducir el PIN a palabras. Estos PIN usados habitualmente se pueden explotar para aumentar la probabilidad de adivinar correctamente el PIN correspondiente a una cuenta determinada.

45 Se pueden usar varios procedimientos para obtener un número de cuenta y el PIN asociado. "Mirar por encima del hombro" (Shoulder Surfing) es el acto de observar a un individuo mientras introduce su PIN con el objetivo de obtener el PIN del individuo para su uso futuro. Un esquema similar implica el uso de un dispositivo de clonación, que se acopla sobre la posición de entrada de la tarjeta y está diseñado para parecer una parte del cajero automático, junto con una cámara colocada estratégicamente. Cuando un individuo introduce su tarjeta en el cajero

automático, el dispositivo de clonación también lee el número de cuenta codificado en la tarjeta. A continuación, la cámara graba el PIN cuando el individuo se lo proporciona al sistema, recogiendo así tanto el número de cuenta como el PIN asociado.

5 Las transacciones de débito que se producen en un punto de venta en muchos casos se almacenan en sistemas locales y, a continuación, se procesan como un grupo periódicamente o al final de día laborable. Dicho almacenamiento de números de cuenta y PIN puede ser un objetivo en un intento de adquirir la información, especialmente porque se almacenan en grandes cantidades.

10 Otros puntos habituales de debilidad son la supervisión de líneas de datos, las violaciones de centros de datos y las tarjetas perdidas, robadas o fraudulentas. La supervisión de líneas de datos puede ser una debilidad de seguridad si los datos no se cifran adecuadamente antes de su transmisión, o si el cifrado se ve comprometido; sin embargo, una implementación y un mantenimiento adecuados pueden evitar que esto sea un problema. Las tarjetas perdidas, robadas o fraudulentas y las violaciones de centros de datos solo ponen en riesgo los números de cuenta, no sus PIN asociados.

La presente invención aborda todas estas debilidades y, además, ofrece medidas mejoradas de protección en áreas que no se consideran riesgos inmediatos.

20 En consecuencia, se puede ver que existe una necesidad de una mejor manera de evitar el fraude de contraseñas. La presente invención está dirigida, principalmente, a la provisión de soluciones para éste y otros problemas. La Patente WO2006064241 A2 da a conocer un procedimiento de validación de un usuario, que comprende las etapas de almacenar datos de usuario representativos de un código de validación para el usuario que comprende una combinación de símbolos seleccionados de un conjunto de símbolos, presentar una imagen visualizada que incluye una pluralidad de áreas designables en las que dicho conjunto de símbolos se distribuye entre dichas áreas designables de tal manera que cada área designable contiene una pluralidad de dichos símbolos, variar la imagen entre presentaciones consecutivas, de tal manera que la distribución de dichos símbolos entre dichas áreas designables cambia entre presentaciones consecutivas, validar un usuario en una rutina de validación detectando la designación por un usuario de una combinación de dichas áreas designables en una imagen presentada, y determinar si la combinación de áreas designables designadas contiene la combinación de símbolos que forma el código de validación para dicho usuario.

La Patente US2004230843 A1 da a conocer una selección de una secuencia de imágenes y su conversión en elementos de un alfabeto concatenados para formar un valor de texto sin cifrar de la contraseña. Ventajosamente, se aplica una función hash criptográfica una o varias veces al valor de texto sin cifrar de la contraseña para formar un valor criptográficamente protegido de la contraseña.

CARACTERÍSTICAS DE LA INVENCION

40 La invención se define mediante las reivindicaciones independientes adjuntas. En las reivindicaciones dependientes se definen otras realizaciones. Según una realización de la presente invención, se da a conocer un procedimiento para introducir y verificar una contraseña. El procedimiento general para la introducción de contraseña incluye: presentar a un cliente una disposición de interfaz predeterminada; introducir una contraseña por el cliente mediante la selección de teclas asociadas con propiedades correspondientes a las requeridas para una verificación de contraseña correcta; verificar la contraseña introducida tras la finalización de la introducción de la contraseña; permitir o denegar el acceso deseado en función de los resultados de la verificación de la contraseña.

En otro aspecto, la invención se refiere a un procedimiento para la autenticación de contraseñas de usuario. El procedimiento incluye acceder a una base de datos de información de usuarios con parámetros de opciones de entrada de usuario predefinidos y generar una disposición aleatoria de opciones de entrada a partir de los parámetros de opciones de entrada de usuario predefinidos. El procedimiento incluye manifestar la disposición aleatoria de opciones de entrada en una interfaz de visualización interactiva y recibir una selección de las opciones de entrada de la interfaz de visualización interactiva. El procedimiento también incluye comparar la selección recibida de opciones de la interfaz de visualización interactiva con los parámetros de opciones de entrada de usuario predefinidos.

En otro aspecto, la invención se refiere a un procedimiento para la creación de contraseñas de usuario. El procedimiento incluye recibir una contraseña seleccionada con una disposición de entradas que tiene dos o más propiedades diferentes de un grupo que comprende números, caracteres, símbolos, colores, patrones, sonidos, texturas, topología, localización, orientación o posición relativa con respecto a la interfaz. La contraseña se recibe en una interfaz de usuario. El procedimiento también incluye almacenar la contraseña seleccionada en una base de datos de usuarios.

En otro aspecto, la invención se refiere a un sistema para la validación de contraseñas. El sistema incluye una pantalla de interfaz de usuario con una pluralidad de teclas. Cada tecla tiene por lo menos dos opciones de propiedades dinámicas diferentes. El sistema tiene una base de datos en comunicación con la interfaz de usuario. La

base de datos está configurada para recibir información de opciones de propiedades seleccionadas de la pantalla de interfaz de usuario. La base de datos está configurada para enviar información de opciones de propiedades variables a la pantalla de interfaz de usuario.

- 5 Según una realización más concreta de la presente invención, la disposición de la interfaz predeterminada usada durante la introducción de la contraseña incluye una pluralidad de teclas virtuales manifestadas en una configuración definida mediante un dispositivo.
- 10 Según una realización más concreta de la presente invención, el dispositivo usado durante la introducción de la contraseña puede incluir parcialmente una interfaz gráfica.
- 15 Según un aspecto más concreto de la presente invención, cada una de las teclas virtuales presentadas durante la introducción de la contraseña está asociada con una pluralidad de propiedades, siendo una propiedad una combinación de una representación en la interfaz y un valor de interpretación. La representación en la interfaz es la manifestación de la propiedad mediante el dispositivo que proporciona la interfaz humana. El valor de interpretación es la identidad de la propiedad, mediante la cual se identifica por el sistema.
- 20 Según otro aspecto de la presente invención, las propiedades asociadas con las teclas virtuales se definen en conjuntos de propiedades (siendo un conjunto de propiedades un grupo de propiedades). Durante la introducción de la contraseña, cada tecla virtual se asocia con una única propiedad de cada uno de la pluralidad de conjuntos de propiedades.
- 25 Según otro aspecto de la presente invención, después de completarse la introducción de la contraseña, los valores de interpretación de las propiedades asociadas con las teclas virtuales seleccionadas se comparan con los valores de interpretación de la contraseña registrada anteriormente como válida durante el proceso de creación de la contraseña.
- 30 Según otra realización más concreta de la presente invención, después de completarse la introducción de la contraseña, los conjuntos de propiedades a partir de los cuales se originan las propiedades asociadas con las teclas virtuales seleccionadas se comparan con los conjuntos de propiedades de la contraseña registrada anteriormente como válida durante el proceso de creación de la contraseña.
- 35 Según otro aspecto de la presente invención, las asociaciones de propiedades con cada una de las teclas virtuales se reasignan de una manera generalmente aleatoria después de cada uso de la interfaz de introducción de la contraseña.
- 40 Según un aspecto más concreto de la presente invención, el proceso mediante el cual se llevan a cabo las asociaciones de propiedades con cada una de las teclas virtuales incluye: a) el cálculo de un número, que es el número óptimamente seguro de conjuntos de propiedades a agrupar; b) la selección, de una manera generalmente aleatoria, de un número de conjuntos de propiedades igual al valor calculado previamente; c) la reasociación de las propiedades de los conjuntos de propiedades seleccionados de forma colectiva como un grupo con la pluralidad de teclas virtuales de una manera generalmente aleatoria; d) la manifestación de la interfaz actualizada mediante el dispositivo.
- 45 Según una realización más concreta de la presente invención, uno de los conjuntos de propiedades usados durante la introducción de la contraseña puede ser estático, excluyéndose, por tanto, de la reasignación de propiedades generalmente aleatoria.
- 50 Según otra realización de la presente invención, se da a conocer un procedimiento para la creación de contraseñas. El procedimiento general para la creación de contraseñas incluye: a) presentar a un cliente una disposición de interfaz predeterminada; b) introducir una contraseña deseada por el cliente mediante la selección de teclas virtuales que están asociadas con propiedades; c) indicar por el cliente que la introducción de la contraseña se ha completado; d) registrar la contraseña introducida por el sistema para su uso futuro para intentar acceder.
- 55 Según una realización más concreta de la presente invención, la disposición de la interfaz predeterminada usada durante la creación de la contraseña está formada por una pluralidad de teclas virtuales manifestadas en una configuración definida mediante un dispositivo.
- 60 Según una realización más concreta de la presente invención, el dispositivo usado durante la creación de la contraseña puede incluir parcialmente una interfaz gráfica.
- 65 Según una realización más concreta de la presente invención, cada una de las teclas virtuales presentadas durante la creación de la contraseña está asociada con una única propiedad, siendo la propiedad una combinación de una representación en la interfaz y un valor de interpretación. La representación en la interfaz es la manifestación de la propiedad mediante el dispositivo que proporciona la interfaz humana. El valor de interpretación es la identidad de la propiedad, mediante la cual se identifica por el sistema.

Según otra realización más concreta de la presente invención, cada una de las teclas virtuales presentadas durante la creación de la contraseña está asociada con una pluralidad de propiedades, siendo una propiedad una combinación de una representación en la interfaz y un valor de interpretación. La representación en la interfaz es la manifestación de la propiedad mediante el dispositivo que proporciona la interfaz humana. El valor de interpretación es la identidad de la propiedad, mediante la cual se identifica por el sistema.

Según otro aspecto de la realización concreta de la presente invención, la selección de una tecla virtual provoca la manifestación de una pluralidad de teclas virtuales igual al número de propiedades asociadas con la tecla virtual seleccionada, estando asociada cada una de las teclas virtuales manifestadas con una de las propiedades asociadas con la tecla virtual seleccionada. La propiedad deseada a incluir en la creación de la contraseña se elige entonces seleccionando la tecla virtual manifestada asociada con la propiedad deseada.

Según otro aspecto de la presente invención, después de completarse la creación de la contraseña, los valores de interpretación de las propiedades asociadas con las teclas virtuales seleccionadas se registran para su uso futuro para intentar acceder mediante el proceso de introducción de la contraseña.

Según otra realización más concreta de la presente invención, después de completarse la creación de la contraseña, el conjunto de propiedades del cual se ha elegido cada una de las propiedades se registra como un patrón de propiedades, además del registro de los valores de interpretación.

Según otra realización de la presente invención, se da a conocer un procedimiento para crear contraseñas seguras. El procedimiento general para la creación de contraseñas seguras incluye: presentar a un cliente una disposición de interfaz predeterminada; introducir la contraseña deseada por el cliente mediante la selección de teclas virtuales que están asociadas con propiedades; indicar por el cliente que la introducción de la contraseña se ha completado; reasociar las propiedades de los conjuntos de propiedades seleccionados entre la pluralidad de teclas virtuales de una manera generalmente aleatoria a través del uso de un algoritmo de dispersión de propiedades que garantiza que las propiedades asociadas inicialmente como un grupo con cualquier tecla virtual determinada no se asocian como un grupo con cualquier tecla virtual después de la reasociación; manifestar la interfaz actualizada mediante el dispositivo; reintroducir la contraseña deseada como una confirmación por el cliente mediante la selección de teclas virtuales que se han reasociado con propiedades; verificar que la introducción de la contraseña inicial y la introducción de la confirmación de contraseña tienen en común las mismas propiedades para cada posición de la contraseña deseada; registrar la contraseña introducida por el sistema para su uso futuro para intentar acceder.

Según otra realización más concreta de la presente invención, se describen procedimientos para la conversión de contraseñas en PIN tradicionales, tanto para la creación de contraseñas como para la entrada de acceso a cuentas a usar con los sistemas bancarios actuales.

Una ventaja de la presente invención es que la revelación de la contraseña a través de cualquier medio de observación requiere múltiples observaciones del proceso de introducción de la contraseña para la misma contraseña. Múltiples observaciones no garantizan la revelación de la contraseña, ya que la probabilidad del proceso de reasociación de propiedades entre intentos de introducción de la contraseña generalmente es aleatorio. La probabilidad de revelación de la contraseña es inversamente proporcional al número de conjuntos de propiedades utilizados, el número de teclas virtuales definidas para la configuración de la interfaz, el número de propiedades únicas definidas en cada uno de los conjuntos de propiedades y la longitud de la contraseña.

Otra ventaja de la presente invención es que todos los esquemas de contraseña/PIN existentes se admiten de forma inherente, sin requerir que las contraseñas/PIN existentes se descarten y/o restablezcan. Otras ventajas y beneficios más de la presente invención se harán evidentes para los expertos en la materia después de leer y comprender la presente memoria descriptiva.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención puede tomar forma en varios componentes y disposiciones de componentes, y/o en varias etapas y disposiciones de etapas. Los dibujos tienen solo fines de ilustración de las realizaciones preferentes, y no deben interpretarse como limitativos de la invención.

La **figura 1** ilustra una realización ejemplar de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de la contraseña, que tiene similitudes con los teclados numéricos usados habitualmente.

La **figura 2** ilustra una realización ejemplar de una disposición de teclas físicas o virtuales que se puede usar durante el proceso de creación de una contraseña para su uso con la disposición de teclas virtuales de introducción de contraseña mostrada en la **figura 1**.

La **figura 3** ilustra el diagrama de flujo de un primer proceso lógico de alto nivel de ejemplo para la creación de una contraseña que acompaña al uso de una disposición de teclas similar a la mostrada en la **figura 2**.

La **figura 3a** ilustra el diagrama de flujo de un proceso lógico de alto nivel alternativo para la creación de una

contraseña y el patrón de propiedades asociado que acompaña al uso de una disposición de teclas similar a la mostrada en la **figura 2**.

La **figura 4** ilustra una segunda realización ejemplar de una disposición de teclas virtuales que utiliza conjuntos de propiedades que se pueden usar durante el proceso de creación de una contraseña para su uso con la disposición de teclas virtuales de introducción de contraseña mostrada en la **figura 1**.

La **figura 5** ilustra el diagrama de flujo de un segundo proceso lógico de alto nivel de ejemplo para la creación de una contraseña que acompaña al uso de una disposición de teclas similar a la mostrada en la **figura 4**.

La **figura 5a** ilustra el diagrama de flujo de un proceso lógico de alto nivel alternativo para la creación de una contraseña y el patrón de propiedades asociado que acompaña al uso de una disposición de teclas similar a la mostrada en la **figura 4**.

La **figura 6** ilustra el diagrama de flujo de un tercer proceso lógico de alto nivel de ejemplo para la creación de una contraseña que acomoda el uso de disposiciones de teclas similares a las mostradas en la **figura 2** y en la **figura 4**.

La **figura 6a** ilustra el diagrama de flujo de un proceso lógico de alto nivel alternativo para la creación de una contraseña y el patrón de propiedades asociado que acomoda el uso de disposiciones de teclas similares a las mostradas en la **figura 2** y en la **figura 4**.

La **figura 7** ilustra un ejemplo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 1**.

La **figura 8** ilustra el diagrama de flujo de un cuarto proceso lógico de alto nivel de ejemplo para la introducción y la verificación de una contraseña.

La **figura 8a** ilustra el diagrama de flujo de un proceso lógico de alto nivel alternativo al mostrado en la **figura 8**, que muestra la introducción y la verificación de una contraseña para una realización que permite que un dispositivo utilizado para la introducción de contraseña tenga conocimiento previo de un patrón de propiedades asociado con una contraseña válida.

La **figura 8b** ilustra el diagrama de flujo de un proceso lógico de alto nivel alternativo al mostrado en la **figura 8**, que muestra la introducción y la verificación de una contraseña para una realización que permite que un dispositivo utilizado para la validación de contraseñas tenga conocimiento de un patrón de propiedades asociado con una contraseña válida.

La **figura 9** ilustra un primer ejemplo alternativo de una disposición de teclas virtuales después de una segunda reasociación de las propiedades con las teclas virtuales mostradas en la **figura 1**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 10** ilustra un segundo ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 1**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña, que tiene bloqueado el conjunto de propiedades de números.

La **figura 11** ilustra un tercer ejemplo alternativo de una disposición de teclas virtuales después de una segunda reasociación de las propiedades con las teclas virtuales mostradas en la **figura 1**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de la contraseña, que tiene bloqueado el conjunto de propiedades de números.

La **figura 12** ilustra un cuarto ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, siendo la forma de las teclas virtuales un conjunto de propiedades.

La **figura 13** ilustra un quinto ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 12**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 14** ilustra un sexto ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, estando orientadas las formas de las teclas virtuales de forma diferente.

La **figura 15** ilustra un séptimo ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 14**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 16** ilustra un octavo ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene conjuntos de propiedades independientes del idioma.

La **figura 17** ilustra un noveno ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 16**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 18** ilustra un décimo ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene un conjunto de propiedades numéricas con más de un dígito.

La **figura 19** ilustra un undécimo ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 18**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 20** ilustra un duodécimo ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene un conjunto de propiedades que está asociado con la proximidad de las teclas, en lugar de con la identidad de las teclas.

La **figura 21** ilustra un décimo tercer ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 20**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña.

La **figura 22** ilustra un décimo cuarto ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene teclas que se pueden pulsar físicamente que se asocian a través de la proximidad de las teclas.

La **figura 23** ilustra un décimo quinto ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 22**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña, que tiene teclas que se pueden pulsar físicamente que se asocian a través de la proximidad.

La **figura 24** ilustra un décimo sexto ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene teclas que se pueden pulsar físicamente que se asocian a través de su posicionamiento relativo.

La **figura 25** ilustra un décimo séptimo ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene teclas que se pueden pulsar físicamente que son capaces de modificar individualmente su aspecto físico.

La **figura 26** ilustra un décimo octavo ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades con las teclas virtuales mostradas en la **figura 25**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña, que tiene teclas que se pueden pulsar físicamente que son capaces de modificar individualmente su aspecto físico.

La **figura 27** ilustra un décimo noveno ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene una interfaz capaz de producir braille.

La **figura 28** ilustra un vigésimo ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene una interfaz capaz de producir braille.

La **figura 29** ilustra un vigésimo primer ejemplo alternativo de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene una interfaz capaz de producir braille.

La **figura 30** ilustra un vigésimo segundo ejemplo alternativo de una disposición de teclas virtuales después de una reasociación de las propiedades mostradas en la **figura 29**, que utiliza conjuntos de propiedades para su uso durante el proceso de introducción de contraseña, que tiene una interfaz capaz de producir braille.

La **figura 31** ilustra una vigésimo tercera realización ejemplar de una disposición de teclas virtuales que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña, que tiene conjuntos de propiedades con propiedades vacías.

La **figura 32** ilustra el diagrama de flujo de un proceso lógico de alto nivel como un ejemplo que se puede usar en la etapa de asociación de propiedades con teclas virtuales mostrada en las etapas 805, 805a y 805b de las **figuras 8, 8a y 8b**, respectivamente.

La **figura 33** ilustra el diagrama de flujo de un proceso lógico de alto nivel como un ejemplo que se puede usar en la selección de conjuntos de propiedades a agrupar durante la etapa de reorganización de propiedades mostrada en las etapas 815, 815a y 815b de las **figuras 8, 8a y 8b**, respectivamente.

La **figura 34** ilustra el diagrama de flujo de un proceso lógico de alto nivel como un ejemplo que se puede usar en la etapa de reorganización de propiedades entre teclas virtuales mostrada en las etapas 820, 820a y 820b de las **figuras 8, 8a y 8b**, respectivamente.

La **figura 35** ilustra el diagrama de flujo de un proceso lógico de alto nivel como un ejemplo que se puede usar en el cálculo del número de conjuntos de propiedades a utilizar durante la reorganización de las asociaciones de las propiedades con las teclas. Este proceso es una observación más detallada de las etapas 810, 810a y 810b de las **figuras 8, 8a y 8b**, respectivamente.

La **figura 36a** ilustra parcialmente un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de un algoritmo de dispersión de propiedades que se puede utilizar en realizaciones del sistema de contraseñas que implementan un procedimiento de creación de contraseñas seguras.

La **figura 36b** ilustra el resto del ejemplo de diagrama de flujo del proceso lógico de alto nivel de un algoritmo de dispersión de propiedades iniciado en la **figura 36a**.

La **figura 37** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina de inicialización de valores estáticos de propiedades, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 38** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para obtener las propiedades no estáticas de las teclas, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 39** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para obtener teclas seleccionadas, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 40** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para obtener las propiedades no estáticas máximas de las teclas, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b** y la rutina de obtención de las teclas seleccionadas representada en la **figura 39**.

La **figura 41** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para actualizar los valores estáticos de las propiedades, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 42** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para obtener las teclas, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 43** ilustra un ejemplo de diagrama de flujo de un proceso lógico de alto nivel de una rutina para intercambiar las propiedades de las teclas, a ejecutar como una subrutina conjuntamente con el algoritmo de dispersión de propiedades representado en la **figura 36a** y en la **figura 36b**.

La **figura 44** ilustra un ejemplo de conjuntos de propiedades configurados para utilizarse en realizaciones del sistema de contraseñas que se integran con los sistemas bancarios actuales, tal como se describe en la **figura 45** y en la **figura 46**. Estos conjuntos de propiedades también se usan en la **figura 48** y en la **figura 49** para representar un ejemplo de una realización que implementa un procedimiento de creación de contraseñas seguras.

La **figura 45** ilustra un procedimiento mediante el cual una contraseña se puede crear y convertir en un PIN tradicional a utilizar por un sistema bancario actual.

La **figura 46** ilustra un procedimiento mediante el cual una contraseña se puede introducir para el acceso a una cuenta y convertir en un PIN tradicional a utilizar por un sistema bancario actual.

La **figura 47** ilustra una realización ejemplar adicional de una disposición de teclas virtuales basada en los conjuntos de propiedades representados en la **figura 44** que utiliza conjuntos de propiedades para su uso durante el proceso de introducción y verificación de contraseña.

La **figura 48** ilustra un ejemplo de la disposición de teclas virtuales que utiliza los conjuntos de propiedades representados en la **figura 44**, después de la ejecución del algoritmo de dispersión de propiedades mostrado en la **figura 36a** y en la **figura 36b**, aplicado a las teclas virtuales mostradas en la **figura 47**.

La **figura 49** ilustra el diagrama de flujo de un ejemplo del proceso lógico de alto nivel para la creación segura de una contraseña que acompaña al uso de una disposición de teclas similar a la mostrada en la **figura 47** y en la **figura 48**.

La **figura 50** es un diagrama esquemático de un sistema de introducción de contraseñas resistente al fraude que funciona con las realizaciones mostradas en las **figuras 1-49**, según una realización de ejemplo.

DESCRIPCIÓN DETALLADA

Se debe comprender que la presente invención no se limita a los dispositivos, procedimientos, condiciones o parámetros concretos descritos y/o mostrados en la presente memoria, y que la terminología usada en la presente memoria tiene como fin describir realizaciones particulares solo a modo de ejemplo. Por tanto, la terminología pretende ser interpretada de manera amplia y no pretende ser limitativa de la invención reivindicada. Por ejemplo, como se usan en la memoria descriptiva, incluyendo las reivindicaciones adjuntas, las formas singulares "un" y "uno" incluyen el plural, el término "o" significa "y/o", y la referencia a un valor numérico particular incluye por lo menos ese valor particular, salvo que el contexto indique claramente lo contrario. Además, cualquier procedimiento descrito en la presente memoria no pretende limitarse a la secuencia de etapas descrita, sino que puede llevarse a cabo en otras secuencias, salvo que se indique expresamente lo contrario en la presente memoria.

A continuación, se pretende dar a conocer una descripción detallada de ejemplos de la invención, y no deben tomarse como limitativos de la propia invención. En cambio, muchas variaciones pueden caer dentro del alcance de la invención, que se define en las reivindicaciones que siguen a la descripción.

La **figura 1** es una realización ejemplar de la presente invención con el fin de introducir contraseñas. El ejemplo representa un dispositivo **100** que tiene las capacidades para manifestar una disposición de teclas virtuales **110**, en este caso mediante una interfaz gráfica **105**. Para los fines de la presente invención, un dispositivo puede ser cualquier ordenador, sistema o periférico conectado capaz de modificar dinámicamente su interfaz, y presentar a los usuarios del sistema diferentes configuraciones de la interfaz a través de las cuales los usuarios pueden proporcionar una contraseña. Ejemplos de un dispositivo de este tipo incluyen, de forma no limitativa: dispositivos portátiles usados durante la recogida de datos, teléfonos móviles y dispositivos inteligentes, cajeros automáticos, ordenadores personales, sistemas de crédito/débito usados en surtidores de combustible y líneas de cajas, terminales con acceso de seguridad física, etc. Cada una de las teclas virtuales **110** de esta realización está asociada con seis conjuntos de propiedades; sin embargo, se puede emplear cualquier pluralidad de conjuntos de propiedades. Los conjuntos de propiedades usados en el ejemplo mostrado en la **figura 1** son: forma **115**, número **120**, caracteres latinos de la A a la H **125**, caracteres latinos de la I a la Q **130**, caracteres latinos de la R a la Z **135** y color **140** (representado como un patrón). Los conjuntos de propiedades pueden incluir grupos de cualesquiera propiedades, permitiendo que una tecla virtual **110** se pueda distinguir de otra dentro de las capacidades del dispositivo **100**. Como es muy evidente en la **figura 1**, cada conjunto de propiedades incluye una pluralidad de propiedades distinguibles, generalmente menor o igual al número de teclas virtuales **110** utilizadas por la interfaz. Cada propiedad se define como una combinación de una representación en la interfaz **105**, que se manifiesta mediante el dispositivo **100**, y un valor de interpretación, que se usa en la identificación de la propiedad por el sistema.

Es posible que una propiedad esté asociada con más de una tecla virtual. Por ejemplo, las teclas virtuales asociadas

con las propiedades de números "1" y "9" en la **figura 1** comparten una asociación con la propiedad de caracteres latinos "A". Además, la tecla virtual asociada con la propiedad de números "0" comparte una asociación con las propiedades de caracteres latinos "E", "O" y "T" con varias teclas virtuales diferentes. En esta realización particular, estas cuatro propiedades se repiten, porque son las letras usadas de forma más habitual en inglés. Para evitar la confusión de los usuarios del sistema, cualquier representación en la interfaz de las propiedades compartidas también comparte el mismo valor de interpretación.

También es posible que un conjunto de propiedades contenga menos propiedades que el número de teclas virtuales utilizadas por la configuración de la interfaz, como se muestra en la realización representada en la **figura 31**. Se observa que la esquina superior derecha de la tecla virtual asociada con la propiedad de números "9" no muestra ninguna propiedad donde de otro modo debería situarse el conjunto de propiedades de caracteres latinos de la A a la H **3125**. Además, la tecla virtual asociada con la propiedad de números "0" no está asociada con ninguno de los tres conjuntos de propiedades de caracteres latinos. Después de reorganizar las propiedades asociadas entre las teclas virtuales, estos valores de propiedades vacíos se tratan igual que si contuviesen una representación en la interfaz. Sin embargo, cuando se elige una tecla virtual durante la introducción de contraseña, las propiedades faltantes se omiten de la selección registrada.

Cuando se usa la introducción de contraseña, las propiedades asociadas con las teclas virtuales se reorganizan en un proceso generalmente aleatorio representado en la **figura 8**. Este proceso comienza con la disposición representada en la **figura 1**, y puede dar lugar a la disposición representada en la **figura 7**. El sistema asocia **805** un elemento de cada conjunto de propiedades con cada tecla virtual de una manera generalmente aleatoria, para lo cual se representa un ejemplo en la **figura 32**, que da lugar a la disposición representada en la **figura 1**. A continuación, se calcula **810** un número óptimamente seguro de conjuntos de propiedades a agrupar, para lo cual se representa un ejemplo en la **figura 35**, basándose en el número de conjuntos de propiedades utilizados. En el caso de este ejemplo, que tiene seis conjuntos de propiedades, el número calculado es tres. A continuación, se selecciona **815** un número de conjuntos de propiedades igual al valor calculado anteriormente de una manera generalmente aleatoria, para lo cual se representa un ejemplo en la **figura 33**. En el ejemplo actual, se selecciona el número de conjuntos de propiedades **120** y **720**, los caracteres latinos de la R a la Z **135** y **735** y el color **140** y **740**. A continuación, las propiedades de los conjuntos de propiedades seleccionados se reasocian colectivamente **820** como un grupo entre la pluralidad de teclas virtuales de una manera generalmente aleatoria, para lo cual se representa un ejemplo en la **figura 34**. Finalmente, el dispositivo manifiesta **825** la interfaz actualizada mostrada en la **figura 7**.

La disposición representada en la **figura 9** representa los resultados de este proceso, habiéndose ejecutado una vez más usando la disposición representada en la **figura 7** como punto de inicio. En el caso de la disposición representada en la **figura 9**, los conjuntos de propiedades seleccionados aleatoriamente son la forma **715** y **915**, el número **720** y **920** y los caracteres latinos de la A a la H **725** y **925**.

En la **figura 8** también se describe un proceso de introducción de contraseñas. En cualquier momento durante la introducción de la contraseña, un usuario puede elegir cancelar **830** el proceso, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección **835** de una de las teclas virtuales por un usuario, no es obvio para un observador cuál de las propiedades se está eligiendo, ya que puede ser cualquiera de la pluralidad de propiedades asociadas con la tecla virtual seleccionada. En este momento, el sistema registra o almacena **840** todos los valores de interpretación de las propiedades asociadas con la tecla virtual seleccionada para la posición actual en la contraseña. Este proceso se repite hasta que se completa **845** la introducción de la contraseña, momento en el cual el sistema lleva a cabo una comparación **850** entre una contraseña válida, que se ha creado anteriormente, y la contraseña proporcionada por el usuario. Esta comparación determina **855** si la validación es una coincidencia correcta. Si la contraseña introducida no coincide con la contraseña válida, se deniega **860** el acceso al sistema. Si la comparación es igual, se proporciona al usuario **865** cualquier acceso que el sistema esté diseñado para conceder.

Otra realización ejemplar de la invención permite que uno de los conjuntos de propiedades se haga estático, en cuyo caso el conjunto de propiedades se excluye de la selección aleatoria de conjuntos de propiedades a reasociar. La **figura 10** muestra un ejemplo de una realización de este tipo después del proceso de reorganización, que comienza con la disposición representada en la **figura 1**. Las propiedades elegidas para reorganizar son la forma **115** y **1015**, los caracteres latinos de la I a la Q **130** y **1030** y el color **140** y **1040**.

La **figura 11** representa los resultados de este proceso de reorganización, habiéndose ejecutado una vez más usando la disposición representada en la **figura 10** como punto de inicio. En el caso de la **figura 11**, los conjuntos de propiedades seleccionados aleatoriamente son los caracteres latinos de la A a la H **1025** y **1125**, los caracteres latinos de la I a la Q **1030** y **1130** y los caracteres latinos de la R a la Z **1035** y **1135**.

La **figura 2** representa una realización ejemplar del proceso de creación de contraseñas, en el que cada tecla está asociada con una única propiedad. En esta realización, las teclas **200** pueden ser virtuales, manifestándose mediante un dispositivo, o las teclas pueden ser componentes físicos de un dispositivo, cuyo objetivo es usarse para la creación de la contraseña. El ejemplo concreto mostrado en la **figura 2** utiliza una fila de teclas para cada

conjunto de propiedades; siendo la fila superior el conjunto de propiedades de forma **215**; siendo la segunda fila el conjunto de propiedades de números **220**; el conjunto de propiedades de caracteres latinos de la A a la H **225** en la tercera fila; el conjunto de propiedades de caracteres latinos de la I a la Q **230** en la cuarta fila; siendo la quinta fila el conjunto de propiedades de caracteres latinos de la R a la Z **235**; y el conjunto de propiedades de colores **240** (representados como patrones) en la última fila.

El proceso mediante el cual esta realización crea la contraseña se resume en la **figura 3**. El sistema manifiesta la interfaz **310**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **320**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **330**, el sistema registra el valor de interpretación de la propiedad asociada con la tecla seleccionada **340** para la posición actual en la contraseña. Este proceso se repite hasta que se completa **350** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **360**.

En la **figura 4** se muestra otra realización ejemplar de la creación de la contraseña. En esta realización, cada tecla virtual está asociada con una pluralidad de propiedades. Después de la selección de una de las teclas virtuales **410**, se manifiesta **455-480** una tecla virtual **450** asociada con cada una de las propiedades asociadas con la tecla seleccionada. La propiedad asociada con una tecla manifestada se añade a la posición actual en la contraseña que se crea cuando se selecciona la tecla virtual manifestada.

El proceso mediante el cual se crea la contraseña para esta realización se describe en la **figura 5**. El sistema manifiesta la interfaz **510**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **520**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **530**, el sistema manifiesta una tecla virtual para cada una de las propiedades asociadas con la tecla seleccionada **540**. Cuando se selecciona **550** una de las teclas virtuales recientemente manifestadas, el sistema registra **560** el valor de interpretación de la propiedad asociada con la tecla seleccionada para la posición actual en la contraseña. Este proceso se repite hasta que se completa **570** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **580**.

La **figura 6** muestra un ejemplo de un proceso mediante el cual las realizaciones ejemplares representadas en la **figura 3** y en la **figura 5** se pueden combinar en un único proceso. El sistema manifiesta la interfaz **605**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **610**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **615**, el sistema comprueba el número de propiedades asociadas con la tecla virtual seleccionada **620**. Si la tecla virtual está asociada con múltiples propiedades, el sistema manifiesta una tecla virtual para cada una de las propiedades asociadas con la tecla seleccionada **625**; a continuación, cuando se selecciona **630** una de las teclas virtuales recientemente manifestadas, el sistema registra el valor de interpretación de la propiedad asociada con la tecla seleccionada **635** para la posición actual en la contraseña. Si la tecla virtual seleccionada inicialmente está asociada con una única propiedad, el sistema registra **640** el valor de interpretación de la propiedad asociada con la tecla seleccionada para la posición actual en la contraseña. Este proceso se repite hasta que se completa **645** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **650**.

Otra realización ejemplar de la creación de la contraseña da a conocer un medio seguro de establecer la contraseña que haría extremadamente difícil que un observador determinase la nueva contraseña, incluso si el observador tiene una visión óptima mientras se está introduciendo la contraseña. Las **figuras 36a-43** dan a conocer un algoritmo de dispersión de propiedades que reorganizará las propiedades asociadas con las teclas virtuales de una manera generalmente aleatoria, de tal manera que la configuración resultante de propiedades asociadas en cualquier tecla virtual incluirá como mucho una única propiedad que estaba asociada con una tecla virtual inmediatamente antes de la ejecución del algoritmo. Un ejemplo de la configuración mostrada en la **figura 48** es un resultado posible después de la ejecución del algoritmo, habiéndose ejecutado a partir de la configuración inicial mostrada en la **figura 47**. La comparación de cualquier tecla virtual en la **figura 47** con cualquier tecla virtual en la **figura 48** mostrará que las teclas virtuales comparadas comparten como mucho una única propiedad, incluyendo la posición de la tecla en la interfaz. Cuando un usuario del sistema elige crear una nueva contraseña, se ejecutará un proceso similar al representado en la **figura 49**. En esta realización, cada tecla virtual está asociada con una pluralidad de propiedades **4905**. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **4910**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **4915**, el sistema registra el valor de interpretación de todas las propiedades asociadas con la tecla seleccionada **4920** para la posición actual en la contraseña. Este proceso se repite hasta que se completa **4925** la introducción de la contraseña, momento en el cual el sistema ejecuta el algoritmo de dispersión de propiedades **4935** mostrado en las **figuras 36a-43**, después del cual se visualiza la configuración resultante y se indica al usuario que confirme la contraseña introducida anteriormente. Después de

que el proceso de introducción de la contraseña se repite para la confirmación **4390**, se realiza una comparación entre las propiedades asociadas con cada tecla seleccionada inicialmente y la tecla seleccionada durante la confirmación para cada posición de la contraseña introducida **4940**. El algoritmo de dispersión de propiedades garantiza que no pueda haber más de una propiedad en común entre las teclas para cada comparación. Si el usuario seleccionó correctamente las teclas con una propiedad común para cada posición de la contraseña durante la confirmación **4945**, el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **4950**. Por el contrario, si, durante la confirmación, el usuario no seleccionó teclas con las mismas propiedades en la misma secuencia que durante la introducción de la contraseña inicial, el proceso de creación de la contraseña se cancela y el usuario debe iniciar el proceso de nuevo desde el principio. Esta realización depende de la condición de que el número de propiedades asociadas con cada tecla sea menor o igual que el número total de teclas usadas por la interfaz implementada por la realización.

Un ejemplo de un algoritmo de dispersión de propiedades se representa en las **figuras 36a-36b**. Una lista que comprende todas las teclas virtuales se almacena en la memoria del sistema como la variable Teclas **3602**, a continuación, se calcula la variable PP como $\text{Techo}(\log_{10}(\text{número de Teclas en la variable de tipo lista Teclas}+1))$ **3604** y la variable CP se calcula como $\text{Techo}(\log_{10}((\text{número de Teclas en la variable de tipo lista Teclas}+1)/2))$ **3606**. A continuación, se inicializan **3608** los valores estáticos de las propiedades siguiendo el proceso Inicializar Valores Estáticos de las Propiedades mostrado en la **figura 37**, y se asigna el valor uno a la variable K **3610**. La variable NSP se ajusta a una lista de conjuntos de propiedades **3612** usando el proceso Obtener Propiedades No Estáticas de las Teclas representado en la **figura 38** y, a continuación, la lista de teclas seleccionadas creada siguiendo el proceso Obtener Teclas Seleccionadas mostrado en la **figura 39** se asigna a la variable Seleccionado **3614**. A continuación, se asigna a la variable Bucle un valor booleano de FALSO **3616**, así como a la variable Salto **3618**, y se asigna el valor uno a la variable S **3620**. Si la variable K es mayor que uno y Salto es igual a FALSO **3622**, entonces los valores estáticos de las propiedades se actualizan **3624** usando el proceso Actualizar Valores Estáticos de las Propiedades mostrado en la **figura 41**, la variable de tipo lista de conjuntos de propiedades NSP se ordena en orden ascendente basándose en el valor Estático de cada propiedad y en el conjunto de propiedades al que pertenece cada propiedad de la tecla en la posición igual a la variable K en la variable de tipo lista Teclas **3626**, y si el número de teclas en la variable de tipo lista Seleccionado **3628** es cero, la lista creada usando el proceso Obtener Teclas Seleccionadas representado en la **figura 39** se asigna a la variable de tipo lista Seleccionado **3630**. Las variables de tipo lista Reorganizar y Alternar se ajustan **3632** entonces a la lista creada siguiendo el proceso Obtener Teclas mostrado en la **figura 42**, y se asigna el valor booleano FALSO a la variable EstablecerSalto **3634**.

Este proceso continúa en la **figura 36b**, en la que, si el número de teclas en la variable de tipo lista Reorganizar no es igual cero **3636**, entonces la variable R se ajusta a una tecla que se selecciona aleatoriamente de la variable de tipo lista Reorganizar **3638**, las propiedades de las teclas almacenadas en las variables R y K se intercambian **3640** como se representa en el proceso Intercambiar Teclas de la **figura 43**, y la tecla asignada a la variable R se elimina de la variable de tipo lista Seleccionado **3642**; por el contrario, si el número de teclas en la variable de tipo lista Reorganizar es igual a cero **3636**, entonces, si la variable Bucle no es igual a VERDADERO **3644**, y el número de conjuntos de propiedades en la variable de tipo lista NSP no es igual a la variable S o la variable K no es menor que el número de teclas en la variable de tipo lista Teclas menos uno **3650**, entonces la variable EstablecerSalto se ajusta al valor booleano VERDADERO **3654**. Si la variable EstablecerSalto es igual a FALSO y la variable Salto es igual a VERDADERO **3656**, la ejecución vuelve a la novena etapa del proceso, en la cual la variable Salto se ajusta a FALSO **3618**, y continúa desde allí. Sin embargo, si el valor de la variable Bucle es VERDADERO **3644**, entonces la variable R se ajusta a una tecla que se selecciona aleatoriamente de la variable de tipo lista Alternar **3646**, y las propiedades de las teclas almacenadas en las variables R y K se intercambian **3648**, como se representa en el proceso Intercambiar Teclas de la **figura 43**, o, si la variable Bucle no es igual a VERDADERO **3644**, pero la variable S es igual al número de conjuntos de propiedades en la variable de tipo lista NSP y la variable K es menor que el número de teclas en la variable de tipo lista Teclas menos uno **3650**, entonces la variable Bucle se ajusta al valor booleano VERDADERO **3652**. En este punto, la ejecución también vuelve a la novena etapa del proceso, en la que la variable Salto se ajusta a FALSO **3618**, y continúa desde allí. Si la variable EstablecerSalto no es igual a FALSO o la variable Salto no es igual a VERDADERO **3656**, la variable Salto se ajusta al valor de la variable EstablecerSalto **3658** y la variable S se incrementa en uno **3660**. Si el número de conjuntos de propiedades en la variable de tipo lista NSP es mayor que cero **3662**, entonces la ejecución vuelve a la undécima etapa **3622** del proceso, en la que la variable K se compara con el valor de uno y la variable Salto se compara con el valor booleano de FALSO, y continúa desde allí; por el contrario, si el número de conjuntos de propiedades en la variable de tipo lista NSP no es mayor que cero **3662**, la variable K se incrementa en uno **3664**. A continuación, si la variable K no es igual al número de teclas en la variable de tipo lista Teclas **3666**, la tecla asignada a la variable K se elimina de la variable de tipo lista Seleccionado **3668** y la ejecución vuelve a la sexta etapa del proceso, en la cual la variable NSP se ajusta a una lista de conjuntos de propiedades **3612** usando el proceso Obtener Propiedades No Estáticas de las Teclas representado en la **figura 38**, y continúa desde allí; de otro modo, el proceso se ha completado y finaliza.

El proceso para Inicializar Valores Estáticos de las Propiedades, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las **figuras 36a-36b**, se representa en la **figura 37**. Se asigna a la variable Impar un valor booleano de VERDADERO si el número de teclas en la variable de tipo lista Teclas es impar, y FALSO si el número de teclas en la variable de tipo lista Teclas es par **3705**. A continuación, se asignan a la

- variable de tipo lista Seleccionado valores equivalentes a la variable de tipo lista Teclas **3710**, y la variable P se ajusta al valor de uno **3715**, así como la variable K **3720**, después de lo cual el valor de uno se asigna al valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades que pertenecen a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas **3725**, y la variable K se incrementa en uno **3730**. Si la
- 5 variable K no es mayor que el número de teclas en la variable de tipo lista Teclas **3735**, entonces la ejecución vuelve a la quinta etapa del proceso, en la que el valor de uno se asigna al valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades que pertenecen a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas **3725**, y continúa desde allí; por el contrario, si la variable K es mayor que el número de
- 10 teclas en la variable de tipo lista Teclas **3735**, entonces, si la variable Impar es VERDADERO **3740**, la variable R se ajusta a una tecla que se selecciona aleatoriamente de la variable de tipo lista Seleccionado **3745**, el valor de cero se asigna al valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades que pertenecen a la tecla igual a la variable R **3750**, y la tecla se elimina de la variable de tipo lista Seleccionado que es igual a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas **3755**. Entonces, la variable P se incrementa en uno **3760**. Si la variable P no es mayor que el número de conjuntos de propiedades usados por las
- 15 teclas en la interfaz **3765**, entonces la ejecución vuelve a la cuarta etapa del proceso, en la que se asigna a la variable K un valor de uno **3720**, y continúa desde allí; por el contrario, si la variable P es mayor que el número de conjuntos de propiedades usados por las teclas en la interfaz **3765**, el proceso se ha completado y vuelve al proceso de referencia.
- 20 El proceso para Obtener Propiedades No Estáticas de las Teclas, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las **figuras 36a-36b**, se representa en la **figura 38**. Se asigna un valor de uno a la variable P **3810**, y la variable de tipo lista NSP se ajusta a una lista vacía **3820**. Si el valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas no es menor que uno **3830**, entonces el conjunto de
- 25 propiedades, al que pertenece la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas, se añade a la variable de tipo lista NSP **3840**. Entonces, la variable P se incrementa en uno **3850**. Si la variable P no es mayor que el número de conjuntos de propiedades usados por las teclas en la interfaz **3860**, entonces la ejecución vuelve a la tercera etapa del proceso, en la que el valor Estático de la propiedad en la posición igual a la variable P en la lista de
- 30 propiedades pertenecientes a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas se compara con el valor de uno **3830**, y continúa desde allí; por el contrario, si la variable P es mayor que el número de conjuntos de propiedades usados por las teclas en la interfaz **3860**, el proceso se ha completado y vuelve al proceso de referencia.
- 35 El proceso para Obtener Teclas Seleccionadas, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las **figuras 36a-36b**, se representa en la **figura 39**. El valor de la variable K+1 se asigna a la variable X **3910**, y la variable Max se ajusta a un valor **3920**, que se calcula a través del proceso Obtener Propiedades No Estáticas Máximas de las Teclas mostrado en la **figura 42**. A continuación, la variable de tipo lista Seleccionado se ajusta a una lista vacía **3930**, y un valor igual al número de propiedades asociadas con la tecla en la posición igual a la variable X en la variable de tipo lista Teclas que tienen un valor estático que es mayor o igual
- 40 que uno se asigna a la variable N **3940**. Si la variable N es igual a la variable Max **3950**, entonces la tecla en la posición igual a la variable X en la variable de tipo lista Teclas se añade a la variable de tipo lista Seleccionado **3960**. Entonces, la variable X se incrementa en uno **3970**. Si la variable X no es mayor que el número de teclas en la variable de tipo lista Teclas **3980**, entonces la ejecución vuelve a la cuarta etapa del proceso, en la que un valor igual
- 45 al número de propiedades asociadas con la tecla en la posición igual a la variable X en la variable de tipo lista Teclas que tienen un valor estático que es mayor o igual que uno se asigna a la variable N **3940**, y continúa desde allí; por el contrario, si la variable X es mayor que el número de teclas en la variable de tipo lista Teclas **3980**, el proceso se ha completado y vuelve al proceso de referencia.
- 50 El proceso para Obtener Propiedades No Estáticas Máximas de las Teclas, al que se hace referencia en el diagrama del proceso Obtener Teclas Seleccionadas mostrado en la **figura 39**, se representa en la **figura 40**. La variable Y se ajusta a un valor igual al de la variable X **4010**, y se asigna un valor de cero a la variable Max **4020**, entonces un valor igual al número de propiedades asociadas con la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas que tienen un valor estático que es mayor o igual que uno se asigna a la variable N **4030**. Si la variable N
- 55 es mayor que la variable Max **4040**, entonces la variable Max se ajusta al valor de la variable N **4050**. Entonces, la variable Y se incrementa en uno **4060**. Si la variable Y no es mayor que el número de teclas en la variable de tipo lista Teclas, y la variable N no es igual al número de conjuntos de propiedades usadas por las teclas en la interfaz **4070**, entonces la ejecución vuelve a la tercera etapa del proceso, en la que un valor igual al número de propiedades asociadas con la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas que tienen
- 60 un valor estático que es mayor o igual que uno se asigna a la variable N **4030**, y continúa desde allí; por el contrario, si la variable Y es mayor que el número de teclas en la variable de tipo lista Teclas, o si la variable N es igual al número de conjuntos de propiedades usadas por las teclas en la interfaz **4070**, el proceso se ha completado y vuelve al proceso de referencia.
- 65 El proceso para Actualizar Valores Estáticos de las Propiedades, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las **figuras 36a-36b**, se representa en la **figura 41**. Se asigna un

valor de uno a las variables P **4104** y X **4112**, se asigna un valor booleano de VERDADERO a las variables Recuento **4108** y Preferente **4116**, y se asigna un valor de uno a la variable Y **4120**. Si la variable Recuento es igual a cero **4124**, entonces un valor igual al número de propiedades asociadas con la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas que tienen un valor estático que es mayor o igual que uno se asigna a la variable N **4128**, si el valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas no es menor que uno **4132**, entonces si la variable N es igual a la variable Max **4136**, entonces la variable Preferente se incrementa en uno **4140**; independientemente de si el valor de N es igual a la variable Max, la variable Recuento se incrementa en uno **4144**, e independientemente de si el valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas es menor que uno **4132** o no, la variable Y se incrementa en uno **4148**, y si el valor de la variable Y no es mayor que el número de teclas en la variable de tipo lista Teclas **4152**, entonces la ejecución vuelve a la séptima etapa del proceso, en la que un valor igual al número de propiedades asociadas con la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas que tienen un valor estático que es mayor o igual que uno se asigna a la variable N **4128**, y continúa desde allí; por el contrario, si el valor de Recuento no es igual a cero **4124**, entonces se asigna a la variable Ajustar un valor igual a $(\text{Recuento}/2 + \text{Preferente} * 10^{CP}) / 10^{(CP+PP)}$ **4156**, se asigna al valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas un valor igual a Suelo (el valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas) + Ajustar **4160**, la variable Y se incrementa en uno **4164**, si el valor de la variable Y no es mayor que el número de teclas en la variable de tipo lista Teclas **4168**, entonces la ejecución vuelve a la octava etapa del proceso, en la que se asigna al valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas un valor igual a Suelo (el valor Estático de la propiedad en la posición igual a la variable P en la lista de propiedades pertenecientes a la tecla en la posición igual a la variable Y en la variable de tipo lista Teclas) + Ajustar **4160**, y continúa desde allí; por el contrario, si el valor de la variable Y es mayor que el número de teclas en la variable de tipo lista Teclas **4168**, entonces se asigna un valor de cero a la variable Recuento **4172**. En ambos casos, tanto si el valor inicial de la variable Recuento es igual a cero **4124** o no, si el valor de la variable Y es mayor que el número de teclas en la variable de tipo lista Teclas **4152**, **4168**, entonces, si, en ese punto del proceso, el valor de la variable Recuento no es igual a cero **4176**, entonces la ejecución vuelve a la quinta etapa del proceso, en la que se asigna a la variable Y un valor de uno **4120**, y continúa desde allí; por el contrario, si el valor de la variable Recuento es igual a cero **4176**, el valor de la variable P se incrementa en uno **4180**, y si la variable N no es mayor que el número de conjuntos de propiedades usados por las teclas en la interfaz **4084**, se asigna a la variable Preferente el valor cero **4188**, y la ejecución también vuelve a la quinta etapa del proceso, en la que se asigna a la variable Y un valor de uno **4120**, y continúa desde allí; por el contrario, si la variable N es mayor que el número de conjuntos de propiedades usados por las teclas en la interfaz **4084**, el proceso se ha completado y vuelve al proceso de referencia.

El proceso para Obtener Teclas, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las figuras **36a-36b**, se representa en la **figura 42**. Se asigna a la variable X **4205** un valor igual al valor de la variable K+1, se asignan a las variables de tipo lista Reorganizar y Alternar valores de listas vacías **4210**, **4215**, y se asigna a la variable A la propiedad perteneciente al conjunto de propiedades asignado a la variable S en la variable de tipo lista NSP, que está asociada con la tecla en la posición igual a la variable X en la variable de tipo lista Teclas **4220**. Si el valor Estático de la propiedad asignada a la variable A no es mayor que uno **4225**, entonces si la tecla en la posición igual a la variable X en la variable de tipo lista Teclas existe en la variable de tipo lista Seleccionado **4230**, la tecla en la posición igual a la variable X en la variable de tipo lista Teclas se añade a la variable de tipo lista Reorganizar **4235**; por el contrario, si la tecla en la posición igual a la variable X en la variable de tipo lista Teclas no existe en la variable de tipo lista Seleccionado **4230**, la tecla en la posición igual a la variable X en la variable de tipo lista Teclas se añade a la variable de tipo lista Alternar **4240**, e independientemente de si el valor Estático de la propiedad asignada a la variable A es mayor que uno **4225** o no, la variable X se incrementa en uno **4245**. Si el valor de la variable X no es mayor que el número de teclas en la variable de tipo lista Teclas **4250**, la ejecución vuelve a la cuarta etapa del proceso, en la que se asigna a la variable A la propiedad perteneciente al conjunto de propiedades asignado a la variable S en la variable de tipo lista NSP, que está asociada con la tecla en la posición igual a la variable X en la variable de tipo lista Teclas **4120**, y continúa desde allí; por el contrario, si el valor de la variable X es mayor que el número de teclas en la variable de tipo lista Teclas **4250**, el proceso se ha completado y vuelve al proceso de referencia.

El proceso para Intercambiar Propiedades de las Teclas, al que se hace referencia en el diagrama del proceso Dispersión de Propiedades mostrado en las figuras **36a-36b**, se representa en la **figura 43**. La propiedad perteneciente al conjunto de propiedades asignado a la variable S en la variable de tipo lista NSP que está asociada con la tecla en la posición igual a la variable K en la variable de tipo lista Teclas se asigna a la variable P1 **4310**, y la propiedad perteneciente al conjunto de propiedades asignado a la variable S en la variable de tipo lista NSP que está asociada con la tecla en la posición igual a la variable R en la variable de tipo lista Teclas se asigna a la variable P2 **4320**. A continuación, la propiedad asignada a la variable P1 se asocia a la tecla en la posición igual a la variable R en la variable de tipo lista Teclas **4330**, y la propiedad asignada a la variable P2 se asocia a la tecla en la posición igual a la variable K en la variable de tipo lista Teclas **4340**. A continuación, se asignan a los valores

Estático de las propiedades asignadas a las variables P1 y P2 un valor de uno negativo **4350, 4360**. Finalmente, el conjunto de propiedades asignado a la variable S se elimina de la lista de propiedades NSP **4370**. El proceso se ha completado y vuelve al proceso de referencia.

5 Son posibles varios procedimientos para la validación de la contraseña. El sistema puede iterar a través de cada una de las propiedades asociadas con cada una de las teclas virtuales seleccionadas en secuencia, comparar el valor de interpretación de cada propiedad en cada posición en la contraseña introducida con el valor de interpretación de la propiedad en la misma posición en la contraseña almacenada. Una coincidencia para todas las posiciones indicará una contraseña válida.

10 El cifrado de la contraseña se puede implementar identificando todas las combinaciones posibles de la contraseña basándose en las propiedades de cada tecla virtual seleccionada para cada posición en la contraseña introducida. Entonces, cada una de estas combinaciones podría cifrarse y compararse con el valor cifrado de la contraseña almacenada, que se cifró anteriormente en el momento en que se creó. Una coincidencia correcta para cualquiera de las combinaciones indica una contraseña válida.

15 El proceso de validación de la contraseña se puede aumentar añadiendo el uso de un patrón de propiedades. La **figura 3a** describe una realización del proceso de creación de la contraseña que captura el patrón de propiedades, además de la contraseña. El sistema manifiesta la interfaz **310a**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **320a**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **330a**, el sistema registra el valor de interpretación de la propiedad **340a**, así como el identificador del conjunto de propiedades **350a** asociado con la tecla seleccionada para la posición actual en la contraseña. Este proceso se repite hasta que se completa **360a** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **370a**. El sistema también almacena el identificador del conjunto de propiedades a partir del cual se elige cada propiedad durante la creación de la contraseña como el patrón de propiedades **380a**.

20 Por ejemplo, haciendo referencia a la **figura 2**, se utiliza una fila de teclas para cada conjunto de propiedades; siendo la fila superior el conjunto de propiedades de forma **215**; siendo la segunda fila el conjunto de propiedades de números **220**; el conjunto de propiedades de caracteres latinos de la A a la H **225** en la tercera fila; el conjunto de propiedades de caracteres latinos de la I a la Q **230** en la cuarta fila; siendo la quinta fila el conjunto de propiedades de caracteres latinos de la R a la Z **235**; y el conjunto de propiedades de colores **240** (representados como patrones) en la última fila. Durante la creación de la contraseña, si se elige un número de la segunda fila, un identificador que representa al conjunto de propiedades de números se almacena en el patrón de propiedades para la posición actual en la contraseña. Esto se lleva a cabo para cada propiedad seleccionada, y, una vez que se ha completado la creación de la contraseña, cada posición de la contraseña se identificará mediante un identificador del conjunto de propiedades.

25 La **figura 5a** representa una realización del proceso de creación de la contraseña que captura el patrón de propiedades, además de la contraseña, durante la creación de la contraseña usando teclas virtuales con múltiples asociaciones de propiedades. El sistema manifiesta la interfaz **505a**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **510a**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **515a**, el sistema manifiesta una tecla virtual para cada una de las propiedades asociadas con la tecla seleccionada **520a**. Cuando se selecciona **525a** una de las teclas virtuales recientemente manifestadas, el sistema registra el valor de interpretación **530a**, así como el identificador del conjunto de propiedades **535a** asociado con la tecla seleccionada para la posición actual en la contraseña. Este proceso se repite hasta que se completa **540a** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **545a**. El sistema también almacena el identificador del conjunto de propiedades a partir del cual se elige cada propiedad durante la creación de la contraseña como el patrón de propiedades **550a**.

30 En el ejemplo anterior, que usa la **figura 4** como una interfaz de creación de la contraseña, cada una de las teclas virtuales manifestadas a lo largo de la derecha **450**, después de la selección de una de las teclas virtuales iniciales **410**, representa la propiedad de cada uno de los conjuntos de propiedades usados durante la creación de la contraseña. Cuando se selecciona una de las teclas virtuales específicas de la propiedad **450**, el identificador del conjunto de propiedades para el conjunto de propiedades al que pertenece la propiedad se almacena en el patrón de propiedades para la posición actual en la contraseña. Esto se lleva a cabo para cada propiedad seleccionada. Una vez que se ha completado la creación de la contraseña, cada posición de la contraseña se puede identificar mediante un identificador del conjunto de propiedades.

35 El proceso mostrado en la **figura 6a** describe un escenario en el que los procesos descritos en la **figura 3a** y en la **figura 5a** se pueden combinar para acomodar la creación de la contraseña independientemente del número de

propiedades asociadas con cada tecla virtual. El sistema manifiesta la interfaz **605a**, o bien la interfaz está construida como un componente físico de un dispositivo a usar para la creación de la contraseña. En cualquier momento durante la creación de la contraseña, un usuario puede elegir cancelar el proceso **610a**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas **615a**, el sistema comprueba el número de propiedades asociadas con la tecla virtual seleccionada **620a**. Si la tecla virtual está asociada con múltiples propiedades, el sistema manifiesta una tecla virtual para cada una de las propiedades asociadas con la tecla seleccionada **625a**; a continuación, cuando se selecciona **630a** una de las teclas virtuales recientemente manifestadas, el sistema registra el valor de interpretación de la propiedad asociada con la tecla seleccionada **635a** para la posición actual en la contraseña. Si la tecla virtual seleccionada inicialmente está asociada con una sola propiedad, el sistema registra el valor de interpretación **640a**. Después de que se registra el valor de interpretación, el identificador del conjunto de propiedades **645a** asociado con la tecla seleccionada también se registra para la posición actual en la contraseña. Este proceso se repite hasta que se completa **650a** la creación de la contraseña, momento en el cual el sistema guarda los valores de interpretación como una contraseña válida para su uso futuro durante la introducción de la contraseña **655a**. El sistema también almacena el identificador del conjunto de propiedades a partir del cual se elige cada propiedad durante la creación de la contraseña como el patrón de propiedades **660a**.

La **figura 8a** es un ejemplo de un proceso mediante el cual la introducción de la contraseña podría utilizar un patrón de propiedades. El sistema asocia un elemento de cada conjunto de propiedades con cada tecla virtual de una manera generalmente aleatoria **805a**, para lo cual se representa un ejemplo en la **figura 32**. A continuación, se calcula un número óptimamente seguro de conjuntos de propiedades a agrupar basándose en el número de conjuntos de propiedades utilizado **810a**, para lo cual se representa un ejemplo en la **figura 35**. A continuación, se selecciona un número de conjuntos de propiedades igual al valor calculado anteriormente de una manera generalmente aleatoria **815a**, para lo cual se representa un ejemplo en la **figura 33**. Las propiedades en los conjuntos de propiedades seleccionados se reasocian entonces colectivamente como un grupo entre la pluralidad de teclas virtuales, de una manera generalmente aleatoria **820a**, para lo cual se representa un ejemplo en la **figura 34**. La interfaz actualizada se manifiesta entonces mediante el dispositivo **825a** y está preparada para la introducción de la contraseña.

En cualquier momento durante la introducción de la contraseña, un usuario puede elegir cancelar el proceso **830a**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas virtuales por un usuario **835a**, no es obvio para un observador cuál de las propiedades se está eligiendo, ya que puede ser cualquiera de la pluralidad de propiedades asociadas con la tecla virtual seleccionada. En este punto, el sistema registra el valor de interpretación de la propiedad asociada con la tecla virtual seleccionada coincidente con el conjunto de propiedades del patrón de propiedades almacenado **840a** para la posición actual en la contraseña. Este proceso se repite hasta que se ha completado **845a** la introducción de la contraseña, momento en el cual el sistema lleva a cabo una comparación entre una contraseña válida que se ha creado anteriormente y la contraseña proporcionada por el usuario **850a**. Si la contraseña introducida no coincide con la contraseña válida **855a**, se deniega **860a** el acceso al sistema. Si la comparación es igual **855a**, se proporciona al usuario **865a** cualquier acceso que el sistema esté diseñado para conceder.

Una realización en la que el sistema que proporciona la interfaz de introducción de contraseña es independiente del sistema que gestiona y valida las contraseñas puede usar un proceso similar al mostrado en la **figura 8b**. El sistema comienza asociando un elemento de cada conjunto de propiedades con cada tecla virtual de una manera generalmente aleatoria **805b**, para lo cual se representa un ejemplo en la **figura 32**. A continuación, se calcula un número óptimamente seguro de conjuntos de propiedades a agrupar basándose en el número de conjuntos de propiedades utilizado **810b**, para lo cual se representa un ejemplo en la **figura 35**. A continuación, se selecciona un número de conjuntos de propiedades igual al valor calculado anteriormente de una manera generalmente aleatoria **815b**, para lo cual se representa un ejemplo en la **figura 33**. Las propiedades en los conjuntos de propiedades seleccionados se reasocian entonces colectivamente como un grupo entre la pluralidad de teclas virtuales, de una manera generalmente aleatoria **820b**, para lo cual se representa un ejemplo en la **figura 34**. La interfaz actualizada se manifiesta entonces mediante el dispositivo **825b** y está preparada para la introducción de la contraseña.

En cualquier momento durante la introducción de la contraseña, un usuario puede elegir cancelar el proceso **830b**, borrando así cualesquiera propiedades seleccionadas anteriormente y comenzando el proceso de nuevo. Después de la selección de una de las teclas virtuales por un usuario **835b**, no es obvio para un observador cuál de las propiedades se está eligiendo, ya que puede ser cualquiera de la pluralidad de propiedades asociadas con la tecla virtual seleccionada. En este momento, el sistema registra todas las propiedades asociadas con la tecla virtual seleccionada **840b** para la posición actual en la contraseña. Este proceso se repite hasta que se completa **845b** la introducción de la contraseña, momento en el cual el sistema de introducción de la contraseña se pone en contacto con el sistema de validación de contraseña y comparte la información de la contraseña introducida. A continuación, el sistema de validación de contraseña compara el identificador del conjunto de propiedades para cada propiedad seleccionada en cada posición en la contraseña con el identificador del conjunto de propiedades almacenado en el patrón de propiedades para la posición coincidente, eliminando todas las coincidencias fallidas. Esta eliminación deja un único valor para cada posición, que, a continuación, se compara con la contraseña válida, que se creó

anteriormente **850b**. Si la contraseña introducida no coincide con la contraseña válida **855b**, se deniega **860b** el acceso al sistema. Si la comparación es igual **855b**, se proporciona al usuario **865b** cualquier acceso que el sistema esté diseñado para conceder.

El cifrado de la contraseña almacenada se puede beneficiar mucho del uso de los patrones de propiedades. En dichos casos, los valores de interpretación de las propiedades seleccionadas a usar en la validación se pueden determinar eliminando las propiedades para cada posición en la contraseña que no pertenecen al conjunto de propiedades especificado en el patrón de propiedades almacenado para la misma posición, dejando solo un único valor de interpretación para cada posición. A continuación, los valores resultantes podrían cifrarse y compararse con la contraseña almacenada cifrada anteriormente para su validación.

Pueden existir realizaciones en las que se usa una única contraseña para proporcionar acceso a información y/o funcionalidades de un sistema o para controlar el acceso físico a una zona de una instalación. Se pueden implementar realizaciones alternativas en las que las contraseñas son específicas de individuos o grupos de individuos, que requieran, en primer lugar, que los propios usuarios se identifiquen en el sistema antes o durante la introducción de la contraseña. Se pueden crear más realizaciones en las que individuos, grupos y/o puntos de acceso puedan utilizar diferentes conjuntos de propiedades o interfaces a través de las que se introducen las contraseñas.

La **figura 12** representa una realización en la que se utilizan seis teclas virtuales con tres conjuntos de propiedades en un dispositivo **1200** que tiene una pantalla gráfica táctil **1210**. Los conjuntos de propiedades en este ejemplo son: caracteres latinos usados en inglés como vocales **1220**, color **1240** (o patrón) y forma **1230**. En esta realización, la representación en la interfaz de la propiedad de forma se manifiesta como la forma de la propia tecla virtual. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedad de forma **1330**) se muestra en la **figura 13**.

Otra realización se muestra en la **figura 14**. Como en el ejemplo anterior, se puede emplear un dispositivo **1400** con una pantalla gráfica táctil **1410**. Esta realización muestra que no es necesario que todas las teclas virtuales **1420**, **1430** tengan la misma orientación, y que se pueden utilizar caracteres alfabéticos tanto en mayúsculas **1450** como en minúsculas **1470**. Además de éstos, se usa un conjunto de propiedades numéricas **1460** y un conjunto de propiedades de color **1440** (o patrón). Un ejemplo de la interfaz resultante **1510** después de haberse reorganizado (propiedades de caracteres alfabéticos en minúsculas **1570** y de color **1540** (o patrón)) se muestra en la **figura 15**.

Un ejemplo adicional de una realización que no tiene propiedades alfanuméricas se proporciona en la **figura 16**. Una realización de este tipo puede ser útil en implementaciones globales, ya que no hay propiedades que la vinculen específicamente con un idioma o una región. Los conjuntos de propiedades son: forma **1640**, color de la forma **1650** (o patrón de la forma) y color de la tecla **1630** (o patrón de la tecla). Incluso aunque muchas de las formas **1640** son similares, todas ellas se orientan de manera diferente, haciendo, por tanto, que se puedan distinguir. El uso del mismo tipo de propiedad (color) **1650** se proporciona como un ejemplo en esta realización para demostrar la diversidad del uso de los conjuntos de propiedades. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedades de forma **1740** y de color de la forma **1750** (o patrón de la forma)) se muestra en la **figura 17**.

Según una realización alternativa de la invención, las propiedades alfanuméricas no se limitan a ser un único carácter. La **figura 18** muestra una realización ejemplar de una interfaz **1810** que tiene dieciséis teclas virtuales **1820** y tres conjuntos de propiedades. Los conjuntos de propiedades son: números **1830**, conjunto de alfabeto uno **1840** y conjunto de alfabeto dos **1850**. El conjunto de propiedades de números utiliza representaciones en la interfaz que tienen tanto uno como dos dígitos, como un ejemplo que muestra que las combinaciones de valores de la contraseña tradicionales se pueden unificar en propiedades únicas a través del uso de la presente invención. Un experto en la materia puede apreciar que dicho uso de las propiedades no se limita a los números, sino que se puede aplicar también a otros tipos de valores, tales como caracteres alfabéticos. En esta realización, además de los caracteres latinos, los dos conjuntos de propiedades de alfabeto también emplean caracteres especiales usados habitualmente. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedad de números **1930**) se muestra en la **figura 19**.

La **figura 20** es un ejemplo de una realización que muestra el uso de conjuntos de propiedades a través de una asociación más abstracta que las realizaciones anteriores. Esta realización utiliza ocho teclas virtuales **2020**, y los siguientes conjuntos de propiedades: punto cardinal **2040**, color (o patrón) de la tecla **2030**, y color (o patrón) de la dirección **2050**. El conjunto de propiedades de color (o patrón) de la tecla **2030** está asociado directamente con cada tecla virtual **2020** como un componente de la manifestación de la propia tecla virtual. Sin embargo, el color (o patrón) de la dirección **2050** está asociado de manera más general con las teclas virtuales **2020** que el color (o patrón) de la tecla **2030**. La representación en la interfaz de la propiedad de color (o patrón) de la dirección **2050** se manifiesta como un componente de la rosa de los vientos en el centro de la interfaz, impartiendo un color (o patrón) a cada punto del diseño. El color (o patrón) de la dirección **2050** de cada punto de la rosa de los vientos está asociado con la tecla virtual a la que apunta. Esta realización también muestra que la representación en la interfaz de las

propiedades no tiene que ser necesariamente uniforme. En este caso, cada una de las propiedades del punto cardinal se representa a través del uso de un tipo de letra diferente. Un experto en la materia puede apreciar que el tipo de letra se puede usar como un conjunto de propiedades adicional; sin embargo, su uso en la realización actual es, preferentemente, decorativo. Un ejemplo de la interfaz resultante **2310** después de haberse reorganizado (propiedades de punto cardinal **2140** y de color (o patrón) de la dirección **2150**) se muestra en la **figura 21**.

En la **figura 22** se muestra una realización adicional que emplea un dispositivo **2200** que tiene una pantalla gráfica **2210** y teclas físicas **2220**. Cada tecla física **2220** está asociada con tres propiedades: forma **2230**, alfabeto **2240** y número **2250**. Las propiedades asociadas con cada tecla son las manifestadas en la misma línea que la tecla y a la izquierda de la tecla. Como con todas las realizaciones dadas a conocer anteriormente, la selección de una tecla indica la selección de una de las propiedades con las que está asociada, sin revelar la propiedad actual seleccionada. Esta realización muestra el uso de la presente invención en dispositivos y sistemas que no tienen pantallas táctiles. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedades de alfabeto **2340** y de números **2350**) se muestra en la **figura 23**.

En la **figura 24** se muestra una realización ejemplar de la presente invención que emplea un dispositivo **2400** que tiene una pantalla gráfica **2405** y teclas físicas **2445**. Esta realización muestra una implementación de la interfaz que funciona con cajeros automáticos y sistemas de débito que no utilizan una pantalla táctil. Las teclas virtuales **2410** que se manifiestan en la pantalla gráfica **2405** están asociadas con las teclas físicas **2445** a través de un posicionamiento relativo común. Por ejemplo: la tecla virtual que tiene la representación en la interfaz de la propiedad de números "3" está asociada con la tecla física "1", la tecla virtual que tiene la representación en la interfaz de la propiedad de números "4" está asociada con la tecla física "6", etc. Es evidente para los expertos en la materia que este tipo de relación de posición permite el uso de la presente invención con cualquier configuración de teclas físicas.

Otra realización de la presente invención utiliza un dispositivo **2500** en el que cada una de una pluralidad de teclas físicas **2520**, existentes en un teclado convencional o numérico **2510**, es capaz de mostrar una imagen directamente en cada tecla, como se muestra en la **figura 25**. Esta realización de ejemplo emplea tres conjuntos de propiedades: número **2530**, imagen **2540** y color **2550** (o patrón). Como con todas las realizaciones anteriores, la selección de una tecla indica el uso de una de las propiedades asociadas en la posición actual de la contraseña. Sin embargo, no se revela la propiedad deseada concreta. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedades de número **2630** y de color **2650** (o patrón)) se muestra en la **figura 26**.

Las propiedades no se limitan a caracteres, números, colores o patrones. Se puede usar cualquier propiedad que se pueda distinguir dentro de las capacidades del dispositivo. Algunos ejemplos adicionales pueden incluir, de forma no limitativa, sonidos, texturas o diferencias más abstractas, tales como la localización o la orientación de una tecla virtual en la interfaz, o la posición relativa de una tecla virtual con respecto a otros componentes de la interfaz.

La **figura 27** muestra la implementación de una realización que utiliza un dispositivo capaz de modificar dinámicamente la topografía de un área superficial **2700**, por ejemplo, una pantalla de braille. Esta realización muestra la presente invención implementada con una interfaz que pueden usar los discapacitados visuales. Cada una de las diez teclas virtuales utilizadas en la **figura 1** se representa a través de la pantalla de braille **2700**. Cada conjunto de propiedades se manifiesta en una fila **2730**, y las propiedades asociadas con cada tecla virtual se manifiestan en una columna **2720**. En este ejemplo particular, cada propiedad se representa mediante dos caracteres, identificando el primero el conjunto de propiedades, e identificando el segundo la propiedad específica. Debido a que algunos caracteres de braille tienen múltiples significados en función de su uso, es necesaria la identificación del conjunto de propiedades. Entre cada columna hay un espacio **2710** para proporcionar una separación definida de una columna a la siguiente. Para seleccionar una propiedad determinada, la pantalla de braille puede ser capaz de detectar presión, en cuyo caso el usuario puede pulsar la propiedad concreta deseada. Si la pantalla no es sensible a la presión, se puede emplear un teclado que proporcione teclas físicas, a través del cual el usuario pueda seleccionar la tecla de número correspondiente a la propiedad de números en la columna de la pantalla de braille que contiene la propiedad deseada.

En la **figura 28** se muestra una versión más concisa de la realización anterior. Esta realización es similar a la realización anterior en que cada conjunto de propiedades se manifiesta en una fila **2830**, y las propiedades asociadas con cada tecla virtual se manifiestan en una columna **2820**. Una diferencia de ejemplo entre esta realización y la anterior es que el conjunto de propiedades que identifica un carácter de braille no está presente en todas las columnas **2820**. En cambio, el conjunto de propiedades que identifican un carácter de braille se lista en una columna independiente específicamente con el fin de identificar el conjunto de propiedades para cada fila **2830**.

En la **figura 29** se representa una realización más concisa del uso de una pantalla de braille. En esta realización, se eliminan los espacios entre las columnas, a excepción de un espacio entre la columna del identificador del conjunto de propiedades y las columnas que contienen las representaciones en la interfaz de las columnas. Esto proporciona una separación definida entre el identificador y las propiedades. Un ejemplo de la interfaz resultante después de haberse reorganizado (propiedades de forma, número y color) se muestra en la **figura 30**. No es un requisito que un conjunto de propiedades se mantenga en la misma fila cuando se reorganizan **3030**. En realidad, es preferible, por

motivos de seguridad, reorganizar los conjuntos de propiedades horizontalmente entre las filas de una manera generalmente aleatoria, para evitar que los observadores sean capaces de determinar de qué conjunto de propiedades se está seleccionando una propiedad.

La **figura 32** es un ejemplo de un proceso mediante el cual el sistema asocia inicialmente un elemento de cada conjunto de propiedades con cada tecla virtual de una manera generalmente aleatoria. Las variables S, Teclas y P se inicializan en **3205** a **3215**. En segundo lugar, se genera aleatoriamente un valor a través del uso de una función de generación de números aleatorios proporcionada por el lenguaje de desarrollo que se utilice para el desarrollo del sistema. A continuación, se usa este número aleatorio para seleccionar una de las teclas K **3220**. En tercer lugar, la tecla seleccionada aleatoriamente K se asocia con la propiedad P del conjunto de propiedades S **3225**. En cuarto lugar, la tecla seleccionada aleatoriamente K se elimina de la lista de todas las teclas K **3230**. Entonces, la variable P se incrementa en uno **3235**. Si el valor de la variable P no es mayor que el número de propiedades en el conjunto S, el proceso establece un bucle hasta la etapa en la que se selecciona aleatoriamente una nueva tecla K; de otro modo, el proceso continúa **3240**. A continuación, la variable S se incrementa en uno **3245**. Si el valor de la variable S no es mayor que el número de conjuntos de propiedades, el proceso establece un bucle hasta la etapa en la que se inicializa la variable Teclas; de otro modo, el proceso finaliza **3250**.

En la **figura 33** se representa un ejemplo del proceso a través del cual se seleccionan conjuntos de propiedades a reorganizar de una manera generalmente aleatoria. En primer lugar, el número de conjuntos de propiedades a agrupar se calcula y se asigna a la variable G **3310**. En segundo lugar, se inicializan las variables Conjuntos y Seleccionado **3320** y **3330**. En tercer lugar, se genera aleatoriamente un valor a través del uso de una función de generación de números aleatorios proporcionada por el lenguaje de desarrollo que se utilice para el desarrollo del sistema. A continuación, se usa este número aleatorio para seleccionar uno de los conjuntos S **3340**. En cuarto lugar, el conjunto seleccionado aleatoriamente S se añade a la lista de conjuntos seleccionados Seleccionado **3350**. A continuación, el conjunto seleccionado aleatoriamente S se elimina de la lista de todos los conjuntos de propiedades no estáticas Conjuntos **3360**. Entonces, la variable G se decrementa en uno **3370**. Si el valor de la variable G es mayor o menor que cero, el proceso establece un bucle hasta la etapa en la que se selecciona aleatoriamente un nuevo conjunto S; de otro modo, el proceso finaliza **3380**.

La **figura 34** representa un ejemplo de un proceso mediante el cual el sistema reorganiza las asociaciones de propiedades con las teclas de una manera generalmente aleatoria. En primer lugar, los conjuntos de propiedades a reorganizar se seleccionan y se ajustan a la variable Seleccionado **3405**. En segundo lugar, se inicializa la variable K **3410**. En tercer lugar, se genera aleatoriamente un valor a través del uso de una función de generación de números aleatorios proporcionada por el lenguaje de desarrollo que se utilice para el desarrollo del sistema. A continuación, se usa este número aleatorio para seleccionar una de las teclas R **3415**. En cuarto lugar, se inicializa la variable S **3420**. En quinto lugar, la variable P se ajusta a la propiedad del conjunto S, que actualmente está asociado con la tecla R **3425**. En sexto lugar, la tecla seleccionada aleatoriamente R se asocia con la propiedad del conjunto S, que actualmente está asociado con la tecla K **3430**. En séptimo lugar, la tecla K se asocia con la propiedad P del conjunto S **3435**. Entonces, la variable S se incrementa en uno **3440**. Si el valor de la variable S no es mayor que el número de conjuntos de propiedades en la lista Seleccionado, el proceso establece un bucle hasta la etapa en la que se inicializa la variable P; de otro modo, el proceso continúa **3445**. A continuación, la variable K se incrementa en uno **3450**. Si el valor de la variable K no es mayor o menor que el número de teclas, el proceso crea un bucle hasta la etapa en la que se selecciona aleatoriamente una nueva tecla R; de otro modo, el proceso finaliza **3455**.

En la **figura 35** se muestra un ejemplo del cálculo del tamaño del grupo de conjuntos de propiedades a usar durante la reorganización de propiedades asociadas con teclas. En su forma más simple, el tamaño del grupo de conjuntos de propiedades es un número entero igual a la mitad del número de conjuntos de propiedades **3510**. Muchos factores del sistema pueden requerir modificaciones de este cálculo, en función de cada implementación concreta.

La integración de un sistema de contraseñas tal como se ha descrito anteriormente con los sistemas bancarios existentes puede presentar muchas dificultades, que deben abordarse antes de poder implementar un sistema bancario basado en contraseña. La **figura 45** y la **figura 46** describen unos medios mediante los cuales se podría implementar un sistema de contraseñas que se integraría con los sistemas bancarios existentes con un esfuerzo mínimo. Estas figuras proporcionan ejemplos visuales basándose en los conjuntos de propiedades definidos en la **figura 44**.

Una realización que tenga la condición de que los valores de interpretación del sistema de las propiedades estén compuestos por el identificador de conjunto del conjunto de propiedades al que pertenecen seguido de un valor decimal de un solo dígito puede convertirse en un PIN tradicional durante la creación de la contraseña a utilizar por los sistemas bancarios actuales siguiendo el procedimiento presentado en la **figura 45**. Después de que el usuario crea la contraseña deseada **4510**, el identificador del conjunto de propiedades de cada propiedad seleccionada, también conocido como el patrón de propiedades, se determina **4520** por el sistema. A continuación, el sistema recorta el identificador del conjunto de propiedades desde la izquierda del valor de interpretación del sistema de cada propiedad **4530**. La parte restante de cada valor de interpretación del sistema es un solo dígito, que, en un sistema de contraseñas que utiliza una contraseña de cuatro propiedades, produce cuatro dígitos decimales que se

pueden utilizar como un PIN tradicional **4540**. El sistema bancario también podría almacenar el patrón de propiedades **4550** en asociación con otra información de la cuenta del usuario.

La **figura 46** da a conocer un procedimiento mediante el cual una contraseña se puede convertir en un PIN tradicional durante la introducción y la validación de la contraseña para su uso con los sistemas bancarios actuales. Como en los sistemas bancarios utilizados actualmente, el usuario presenta al sistema un medio de identificación, por ejemplo, una tarjeta de cajero automático/débito **4610**. A continuación, el usuario introduce una contraseña en la interfaz de contraseña proporcionada **4620**. Después de la recuperación del patrón de propiedades almacenado con la información de la cuenta del usuario **4630**, el sistema selecciona las propiedades correspondientes al patrón de propiedades recuperado **4640**. A continuación, el sistema recorta el identificador del conjunto de propiedades desde la izquierda de cada uno de los valores de interpretación del sistema de las propiedades introducidas **4650**, dando lugar a un solo dígito decimal para cada propiedad, un PIN de cuatro dígitos en el caso de una contraseña de cuatro propiedades, que se utiliza entonces de la misma manera que un PIN tradicional **4660**.

Como se muestra en la **figura 50**, el sistema descrito anteriormente **5000** puede incluir un sistema informático del proveedor de servicios **5002**, uno o más dispositivos de usuario **5020** descritos anteriormente, todo tal como se describe con más detalle a continuación. Uno o varios de los componentes del sistema **5000** pueden incluir uno o varios dispositivos de procesamiento que se pueden configurar para acceder a y leer medios legibles por ordenador asociados que tienen datos y/o instrucciones ejecutables por ordenador almacenados en los mismos para implementar los diversos procedimientos de la invención.

Dispositivos y sistemas de red de ejemplo, incluyendo uno o varios de los sistemas informáticos del proveedor de servicios **5002**, dispositivos de usuario **5020**, pueden incluir o, de otro modo, estar asociados con, hardware y/o software apropiado para transmitir y recibir datos y/o instrucciones ejecutables por ordenador a través de uno o varios enlaces o redes de comunicaciones **5026**. Estos dispositivos y sistemas conectados en red **5002**, **5020** también pueden incluir un número predeterminado de procesadores para procesar datos y ejecutar instrucciones ejecutables por ordenador, así como otros componentes internos y periféricos. Además, estos dispositivos y sistemas en red pueden incluir o estar en comunicación con un número predeterminado de bases de datos apropiadas **5009** que se pueden operar para almacenar datos y/o instrucciones ejecutables por ordenador. La base de datos **5009** puede incluir una amplia variedad de datos diferentes en varias realizaciones, por ejemplo, perfiles de usuario y contraseñas, historial de generación de contraseñas y un grupo de opciones de iconos de contraseñas. Ejecutando las instrucciones ejecutables por ordenador, cada uno de los dispositivos en red puede formar un ordenador de propósito específico en una máquina particular. Como se usa en la presente memoria, el término "medio legible por ordenador" describe cualquier memoria o dispositivo de memoria no transitoria apropiada.

El sistema informático del proveedor de servicios **5002** se puede asociar con un proveedor de servicios que proporciona servicios a clientes o usuarios a través de portales protegidos con contraseña. Para los fines de la presente divulgación, el sistema informático del proveedor de servicios **5002** generalmente se denomina proveedor de servicios. El proveedor de servicios **5002** puede ser cualquier dispositivo controlado por procesador apropiado que facilite la generación de un portal de introducción de contraseña a un dispositivo de usuario apropiado. Por ejemplo, el proveedor de servicios **5002** puede ser un dispositivo informático que incluya ordenadores servidores, ordenadores centrales, ordenadores en red, ordenadores de sobremesa, ordenadores personales, asistentes digitales, asistentes digitales personales, tabletas digitales, aparatos de Internet, circuitos específicos de la aplicación, microcontroladores, miniordenadores, cajeros automáticos y/o cualquier otro dispositivo basado en procesador. La ejecución de las instrucciones implementadas en un ordenador mediante el proveedor de servicios **5002** puede formar un ordenador de propósito específico u otra máquina particular que facilite la operación de un portal de contraseñas a un usuario. Adicionalmente, en algunas realizaciones de la invención, las operaciones y/o el control del proveedor de servicios **5002** se pueden distribuir entre varios componentes de procesamiento.

Además de uno o varios procesadores **5014**, el proveedor de servicios **5002** puede incluir uno o varios dispositivos de memoria **5004**, una o varias interfaces de entrada/salida ("E/S") **5016** y una o varias interfaces de red **5018**. El uno o varios dispositivos de memoria **5004** pueden ser cualesquiera dispositivos de memoria adecuados, por ejemplo, cachés, dispositivos de memoria de solo lectura, dispositivos de memoria de acceso aleatorio, dispositivos de almacenamiento magnético, etc. El uno o varios dispositivos de memoria **5004** pueden almacenar datos, instrucciones ejecutables y/o varios módulos de programa utilizados por el proveedor de servicios, por ejemplo, archivos de datos **5006**, un sistema operativo (OS) **5010**, un sistema de gestión de bases de datos (Database Management System, DBMS) **5012** y/o un módulo anfitrión (host) **5008**. Los archivos de datos **5006** incluyen una amplia variedad de datos diferentes en varias realizaciones, por ejemplo, perfiles de usuario y contraseñas, historial de generación de contraseñas y un grupo de opciones de iconos de contraseñas.

El sistema operativo (OS) **5010** es un módulo de software apropiado que controla al proveedor de servicios **5002**. El OS **5010** también puede facilitar la ejecución de otros módulos de software mediante el uno o varios procesadores **5014**. El OS **5010** puede ser, de forma no limitativa, Microsoft Windows®, Apple OSX™, Linux™, Unix™ o un sistema operativo central. El sistema de gestión de bases de datos ("DBMS") **5012** puede facilitar el mantenimiento de la información almacenada en los dispositivos de memoria **5002** o en una o varias bases de datos apropiadas **5009** asociadas con el proveedor de servicios **5002**. El módulo anfitrión **5008** puede facilitar la recepción

y/o el procesamiento de peticiones y/u otra información que se reciba de un usuario mediante un dispositivo de usuario apropiado **5020**. Por ejemplo, el módulo anfitrión **5008** puede incluir un servidor web u otro programa dedicado que se pueda operar para recibir peticiones y/o información de módulos clientes, por ejemplo, navegadores web, asociados con varios dispositivos de usuario.

5 Es evidente para los expertos en la materia que las representaciones de las realizaciones descritas solo se deben considerar como ejemplos, a través de los cuales se puede implementar la presente invención, y no para limitar la invención. Se puede emplear cualquier configuración de la interfaz concebible dentro de las capacidades de cualquier dispositivo que implemente correctamente la presente invención al mismo tiempo que mantiene su espíritu
10 y su concepto global.

Aunque la invención se ha mostrado y descrito en formas ejemplares, será evidente para los expertos en la materia que se pueden hacer muchas modificaciones, adiciones y eliminaciones en la misma sin salirse del alcance de la invención, definida mediante las siguientes reivindicaciones.

15

REIVINDICACIONES

1. Procedimiento para la autenticación de contraseñas de usuario, que comprende:

- 5 acceder a una base de datos de información de usuarios que comprende una contraseña predefinida que comprende dos o más parámetros de opciones de entrada de usuario, comprendiendo los dos o más parámetros de opciones de entrada de usuario dos o más propiedades diferentes de un grupo que comprende: imágenes, caracteres alfanuméricos, símbolos, colores, patrones, sonidos, texturas, topología, localización, orientación y posición relativa con respecto a una interfaz de visualización interactiva, en el que se asigna a cada propiedad un valor de interpretación del sistema único, en el que las propiedades se organizan en conjuntos de propiedades y se asigna a cada conjunto de propiedades un identificador de conjunto, en el que los identificadores de conjunto de los conjuntos de propiedades de las propiedades en la contraseña predefinida se almacenan como un patrón de propiedades de la contraseña;
- 10 generar una disposición aleatoria de parámetros de opciones de entrada de usuario que comprende las propiedades en los parámetros de opciones de entrada de usuario de la contraseña predefinida, comprendiendo también la disposición aleatoria de parámetros de opciones de entrada de usuario unas propiedades diferentes de dichas propiedades que no son parte de la contraseña, en el que los parámetros de opciones de entrada de usuario que no son parte de la contraseña predefinida también comprenden valores de interpretación del sistema únicos, mediante los cuales la propiedad correspondiente se identifica por un sistema;
- 15 manifestar la disposición aleatoria de parámetros de opciones de entrada de usuario en la interfaz de visualización interactiva, en el que la interfaz de visualización interactiva presenta una disposición de, por lo menos, dos teclas virtuales diferentes colocadas en posiciones en la interfaz de visualización interactiva, y cada tecla virtual presenta una disposición de, por lo menos, dos parámetros de opciones de entrada de usuario diferentes de la disposición aleatoria de parámetros de opciones de usuario;
- 20 recibir de la interfaz de visualización interactiva una selección de las teclas virtuales en el estado en el que se presentaron en la etapa de manifestación, en el que el sistema recibe todos los valores de interpretación del sistema únicos para todos los parámetros de opciones de entrada de usuario presentados en las teclas virtuales seleccionadas, en el que la selección recibida de parámetros de opciones de entrada de usuario incluye los parámetros de opciones de entrada de usuario de la contraseña predefinida y también incluye los parámetros de opciones de entrada de usuario que no son parte de la contraseña predefinida; y
- 25 comparar los valores de interpretación del sistema de todos los parámetros de opciones de entrada de usuario seleccionados recibidos de la interfaz de visualización interactiva con los valores de interpretación del sistema únicos de los parámetros de opciones de entrada de usuario de la contraseña predefinida, y eliminar todas las coincidencias fallidas para cada posición en la contraseña que no pertenezcan al conjunto de propiedades especificado en el patrón de propiedades almacenado para la misma posición, dejando solo un solo valor de interpretación del sistema único coincidente para cada posición, en el que los valores de interpretación del sistema resultantes se comparan entonces con la contraseña predefinida,
- 30 reorganizar de manera aleatoria los parámetros de opciones de entrada de usuario después de comparar los parámetros de opciones de entrada de usuario seleccionados de las teclas virtuales de la interfaz de visualización interactiva con los parámetros de opciones de entrada de usuario de la contraseña predefinida, en el que por lo menos uno de los conjuntos de propiedades es estático, estando excluido, por tanto, de la reorganización aleatoria de los parámetros de opciones de entrada de usuario.

2. Procedimiento, según la reivindicación 1, en el que se asigna a cada propiedad una representación en la interfaz de la propiedad.

3. Sistema para la validación de contraseñas, que comprende:

- 50 una interfaz de visualización interactiva que comprende una pluralidad de teclas en una disposición posicionada en la interfaz de visualización interactiva, estando configurada cada tecla para presentar visualmente por lo menos dos propiedades diferentes de un grupo que comprende imágenes, caracteres alfanuméricos, símbolos, colores, patrones, sonidos, texturas, topología, localización, orientación y posición relativa con respecto a la interfaz de visualización interactiva, en el que se asigna a cada propiedad un valor de interpretación del sistema mediante el cual la propiedad correspondiente se identifica por el sistema;
- 55 una base de datos en comunicación con la interfaz de visualización interactiva, estando configurada la base de datos para enviar información de propiedades variable que representa a las teclas a la interfaz de visualización interactiva, comprendiendo la información de propiedades variable una disposición aleatoria de una contraseña predefinida que comprende dos o más parámetros de opciones de entrada de usuario, comprendiendo los dos o más parámetros de opciones de entrada de usuario dos o más propiedades diferentes de las propiedades, en el que las propiedades se organizan en conjuntos de propiedades, y se asigna a cada conjunto de propiedades un identificador de conjunto, en el que los identificadores de conjunto de los conjuntos de propiedades de las propiedades en la contraseña predefinida se almacenan como un patrón de propiedades de la contraseña, comprendiendo también la información de propiedades variable dichas propiedades diferentes que no son parte de la contraseña, en el que dichas propiedades diferentes que no son parte de la contraseña predefinida también comprenden valores de interpretación del sistema; y
- 60
- 65

- estando configurada la base de datos para recibir valores de interpretación del sistema de propiedades de la interfaz de visualización interactiva de teclas seleccionadas que comprenden los valores de interpretación del sistema asignados a las propiedades de la contraseña y otros valores de interpretación del sistema asignados a propiedades diferentes de los asignados a las propiedades de la contraseña, y estando configurada la base de datos para comparar los valores de interpretación del sistema de las propiedades seleccionadas recibidos de la interfaz de visualización interactiva con los valores de interpretación del sistema de la contraseña predefinida, y para eliminar todas las coincidencias fallidas para cada posición en la contraseña que no pertenezcan al conjunto de propiedades especificado en el patrón de propiedades almacenado para la misma posición, para dejar solo un solo valor de interpretación del sistema coincidente para cada posición, en el que los valores de interpretación del sistema resultantes se comparan entonces con la contraseña predefinida.
- 5
- 10
4. Sistema, según la reivindicación 3, en el que la base de datos está configurada para enviar disposiciones variables de, por lo menos, dos propiedades diferentes después de que la base de datos ha recibido los valores de interpretación del sistema de las propiedades seleccionadas de la interfaz de visualización interactiva.
- 15
5. Sistema, según la reivindicación 3, que comprende, además, un sistema operativo para seleccionar una disposición aleatoria de dichas propiedades de la base de datos y transmitir la disposición aleatoria de propiedades a la interfaz de visualización interactiva.
- 20

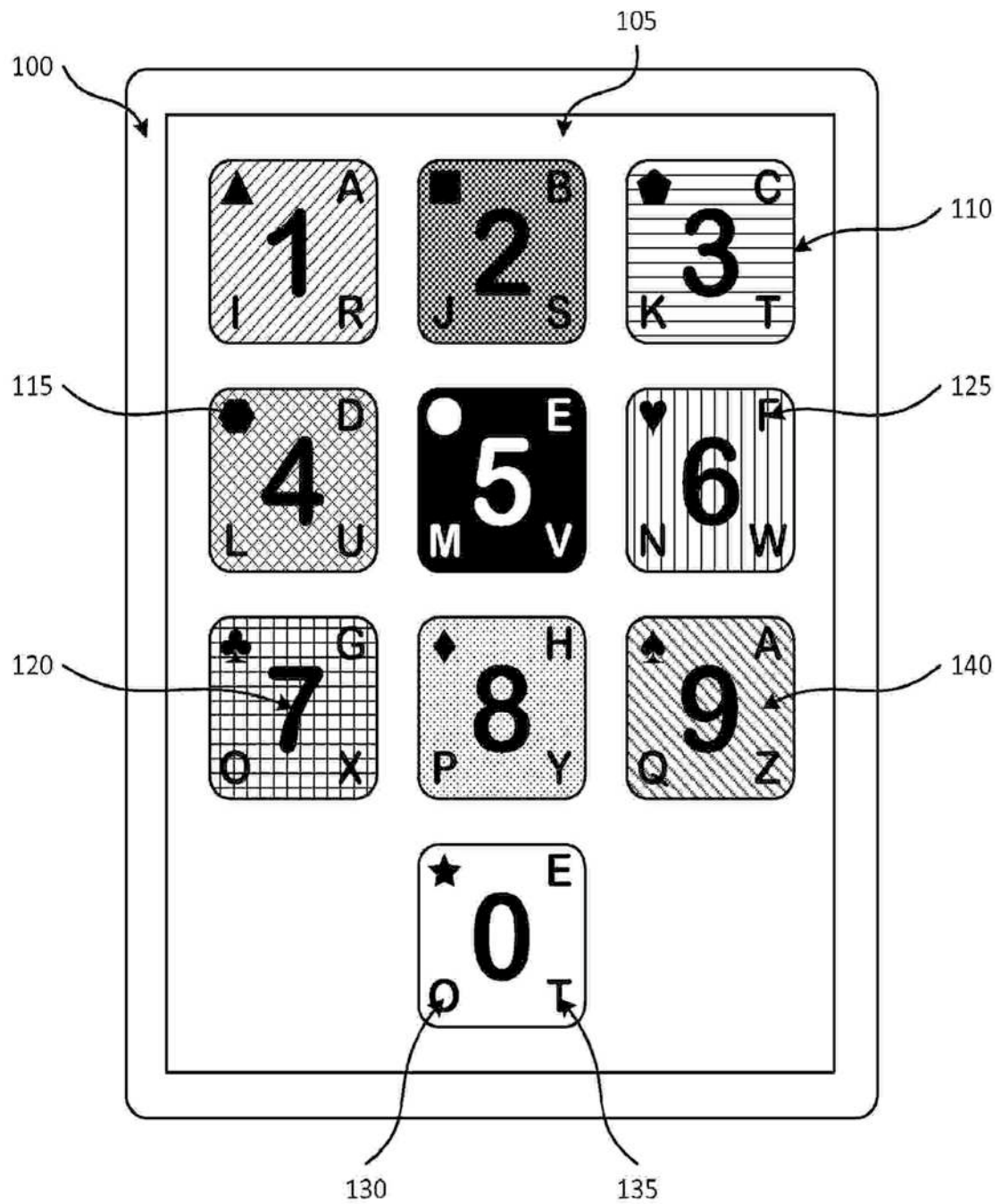


Fig. 1

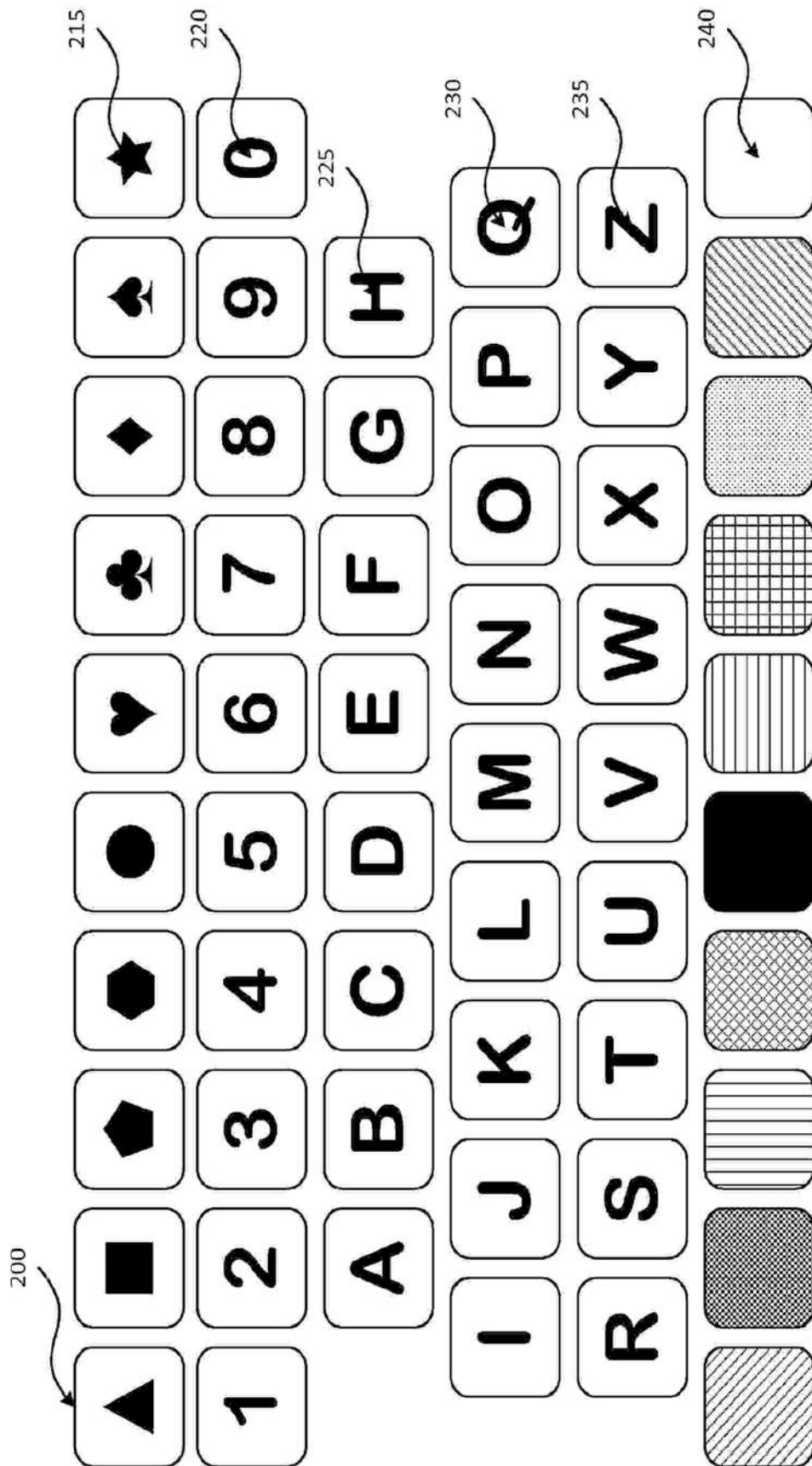


Fig. 2

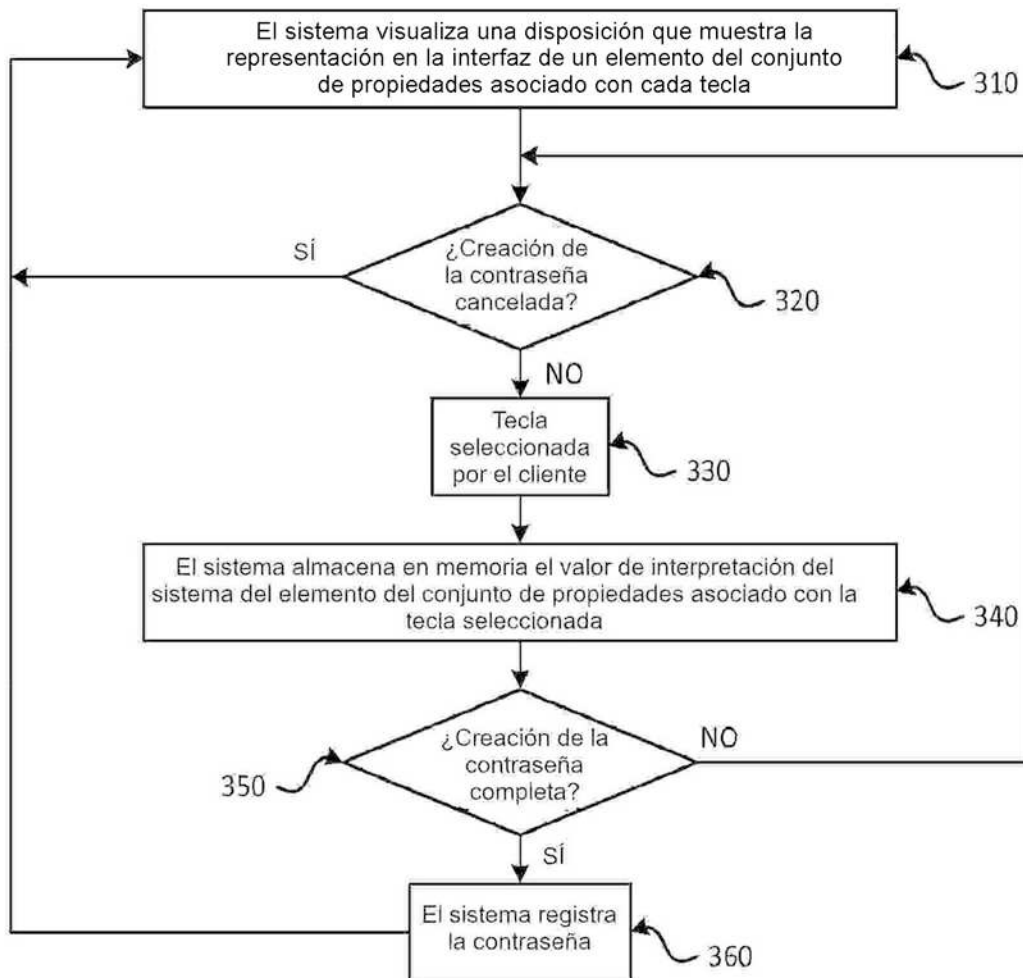


Fig. 3

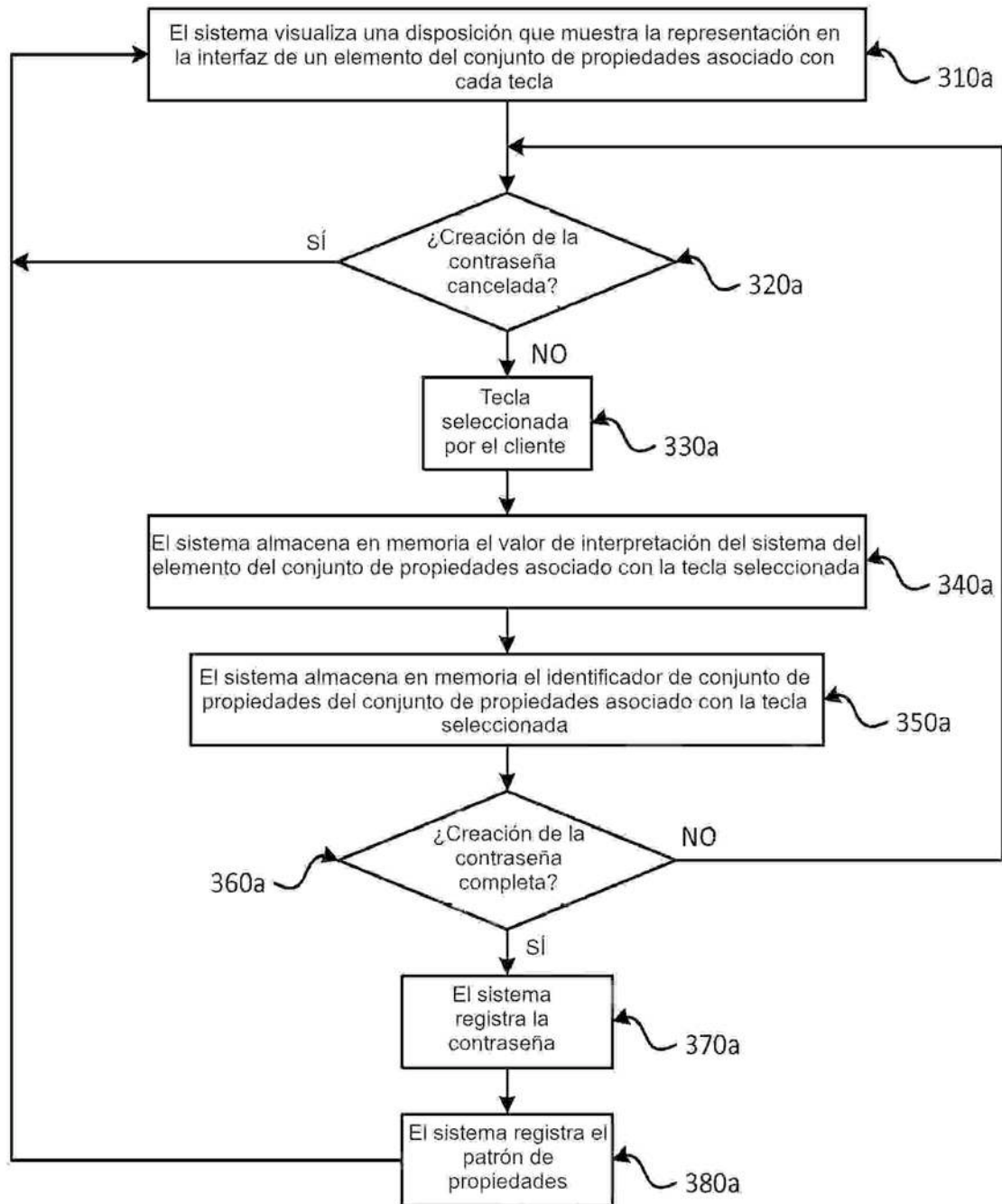


Fig. 3a

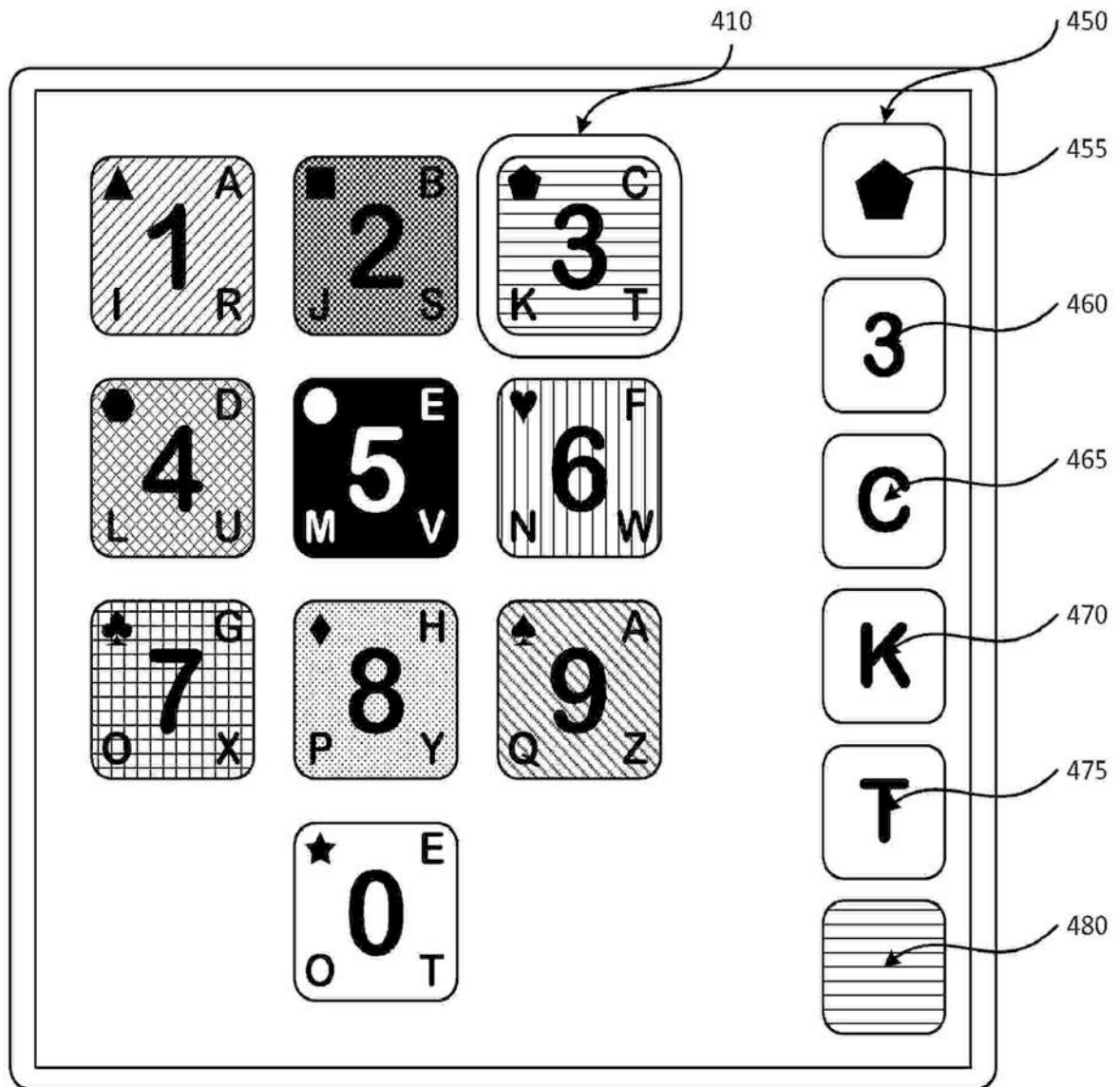


Fig. 4

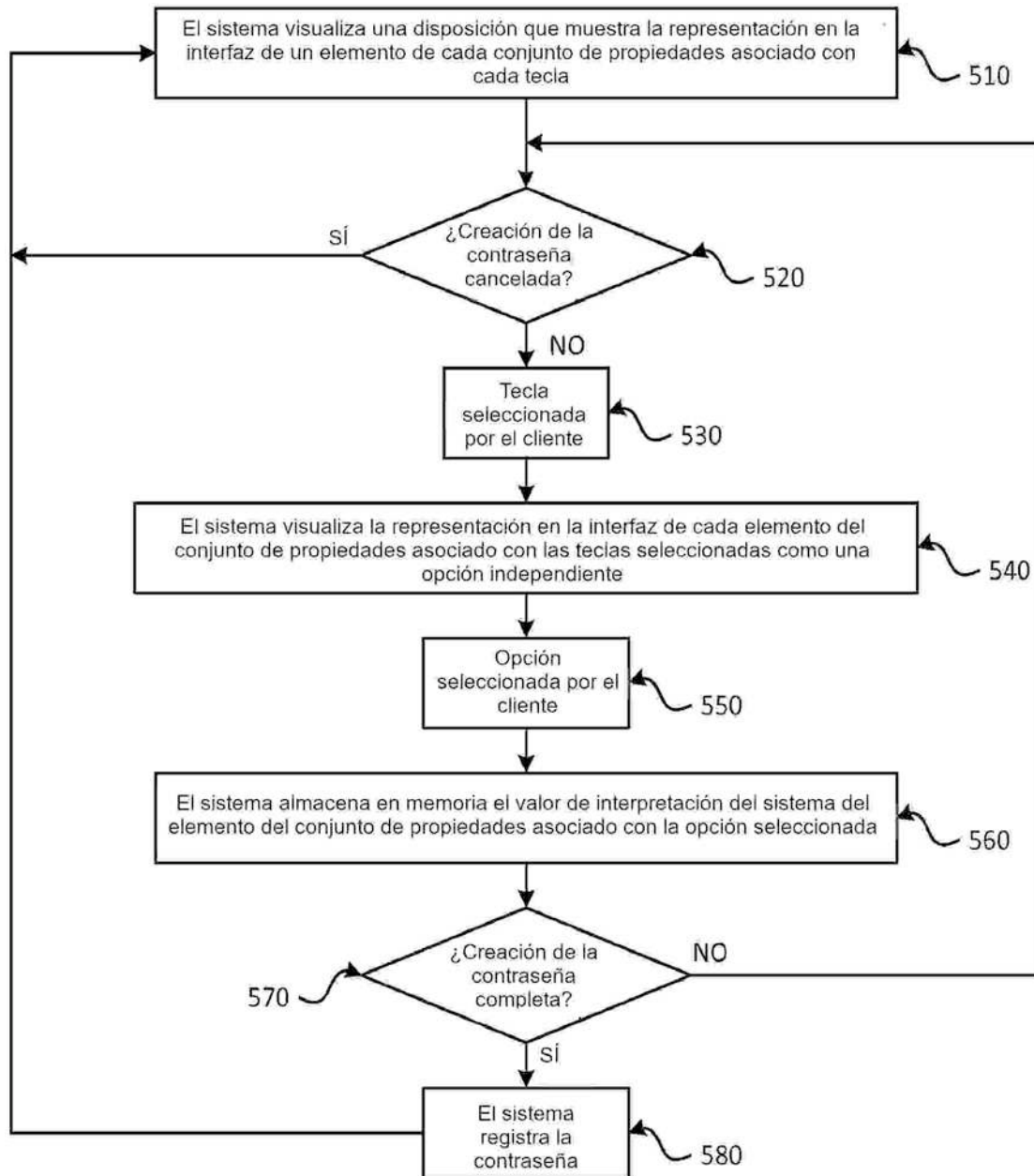


Fig. 5

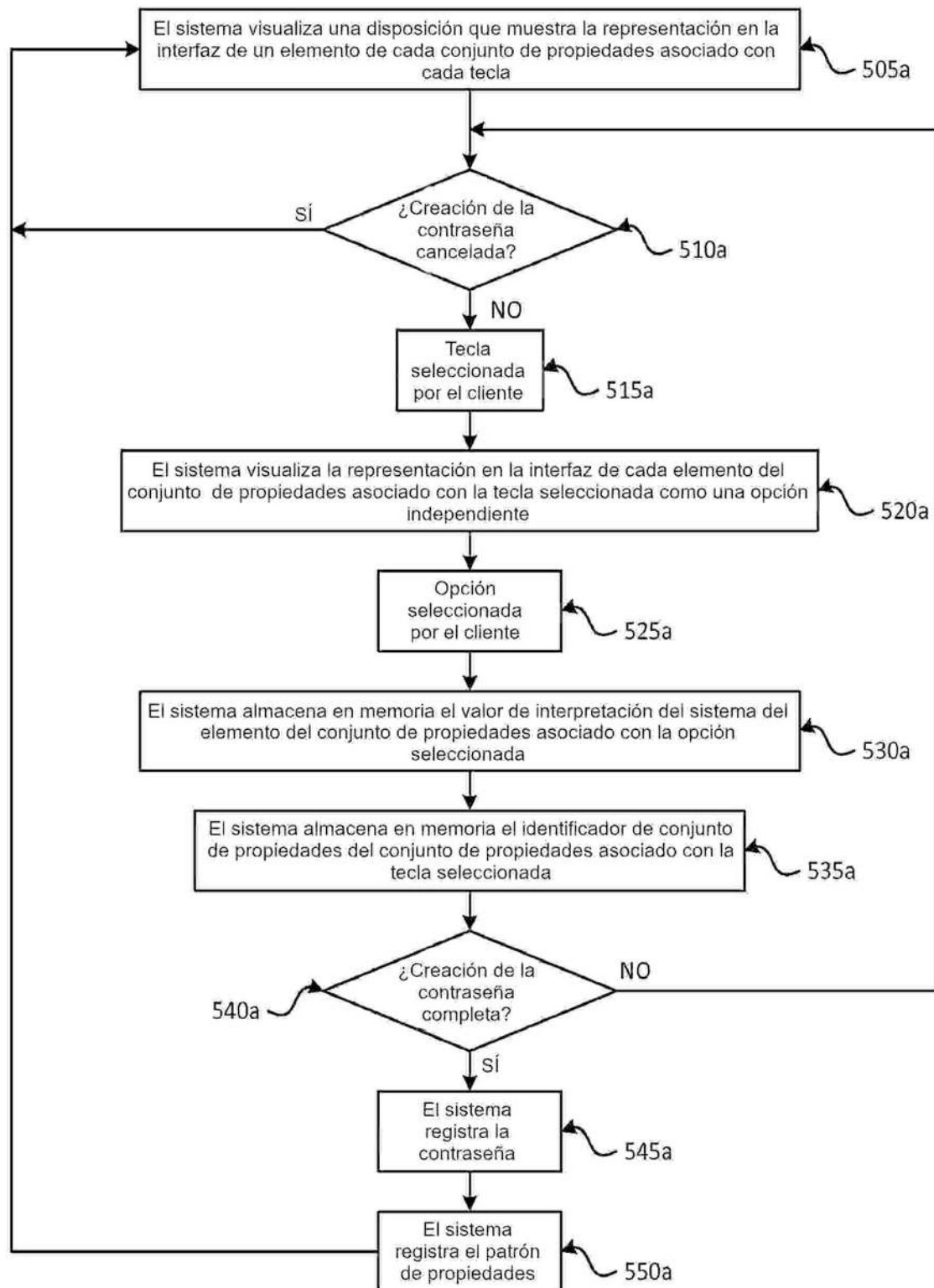


Fig. 5a

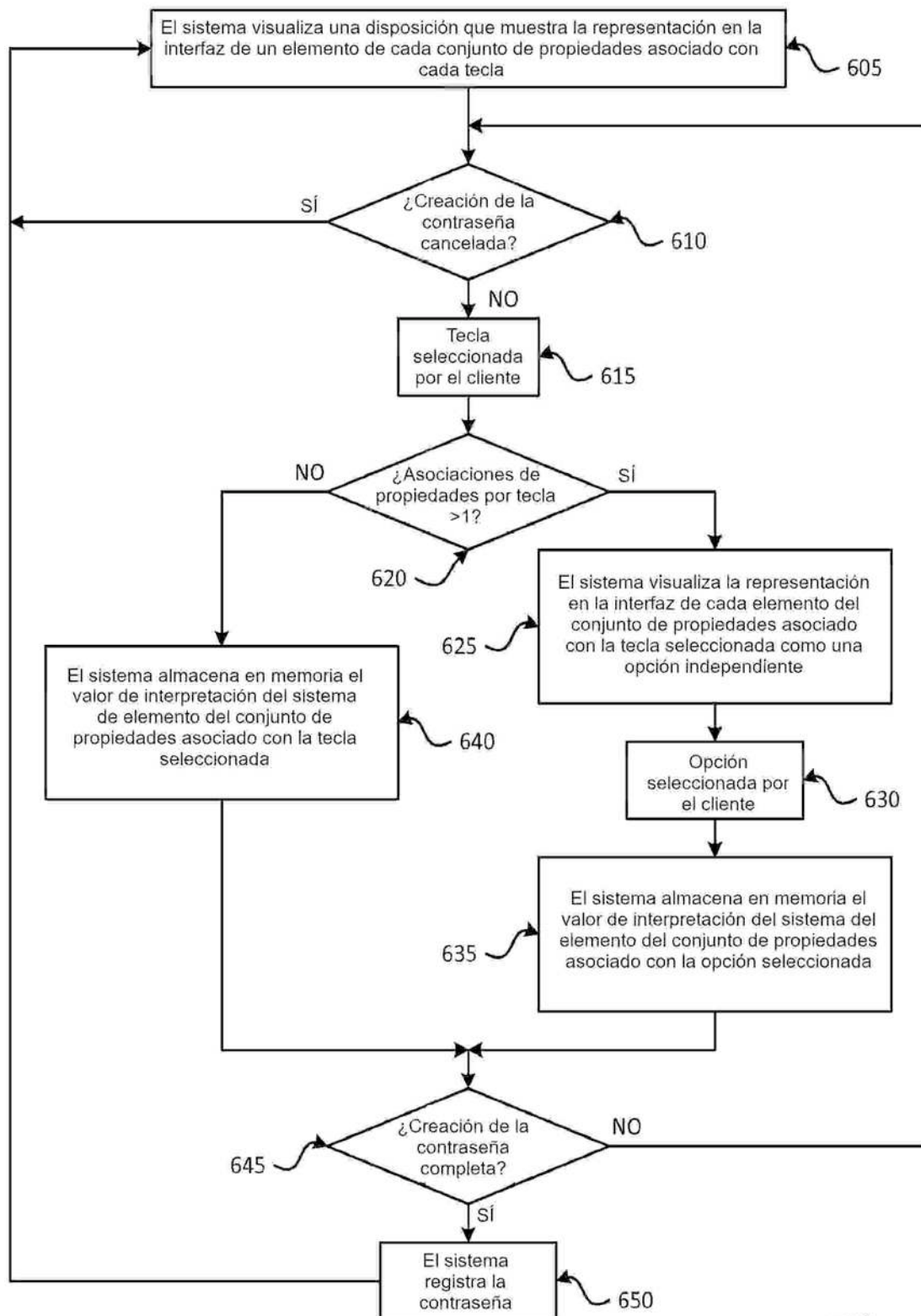
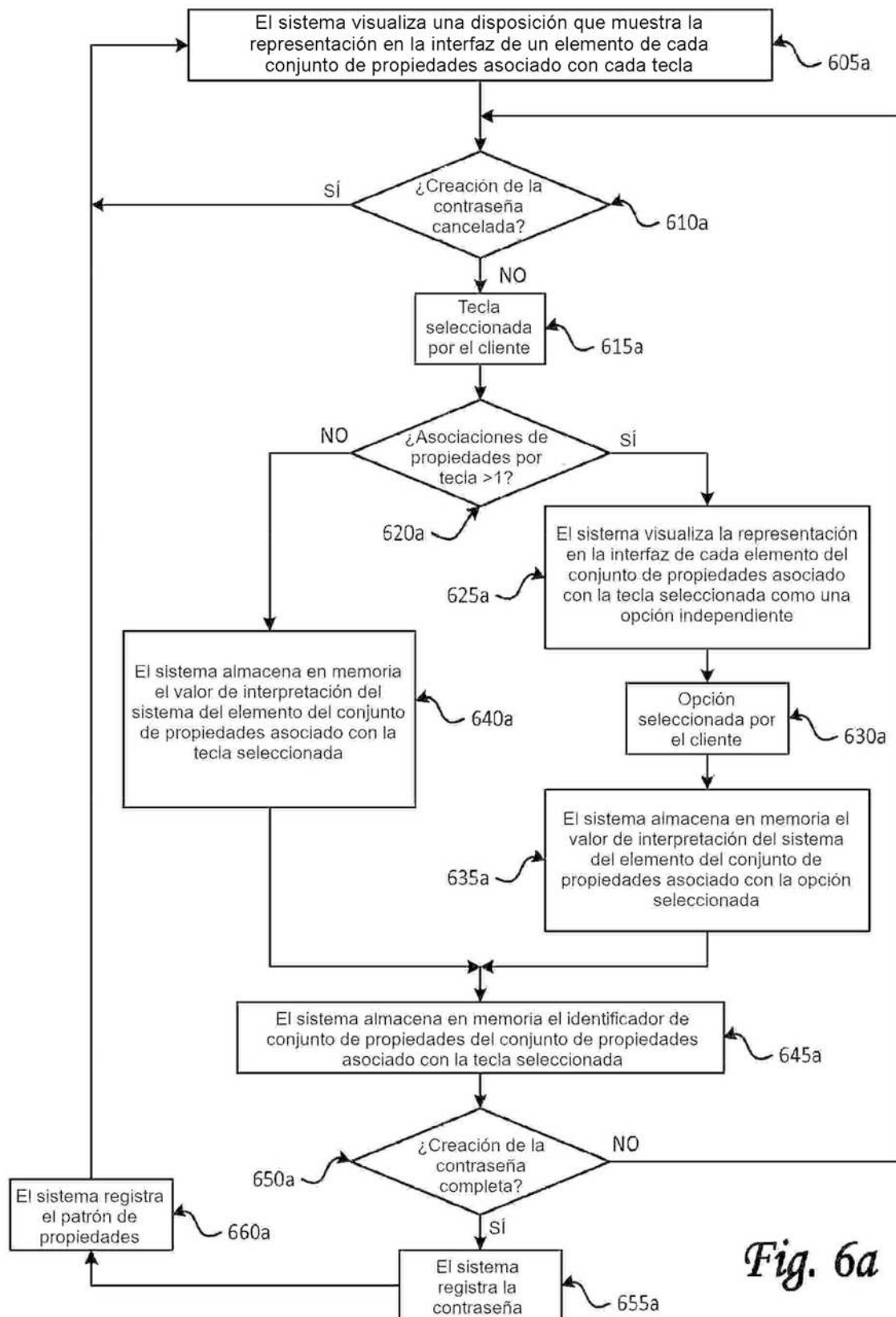


Fig. 6



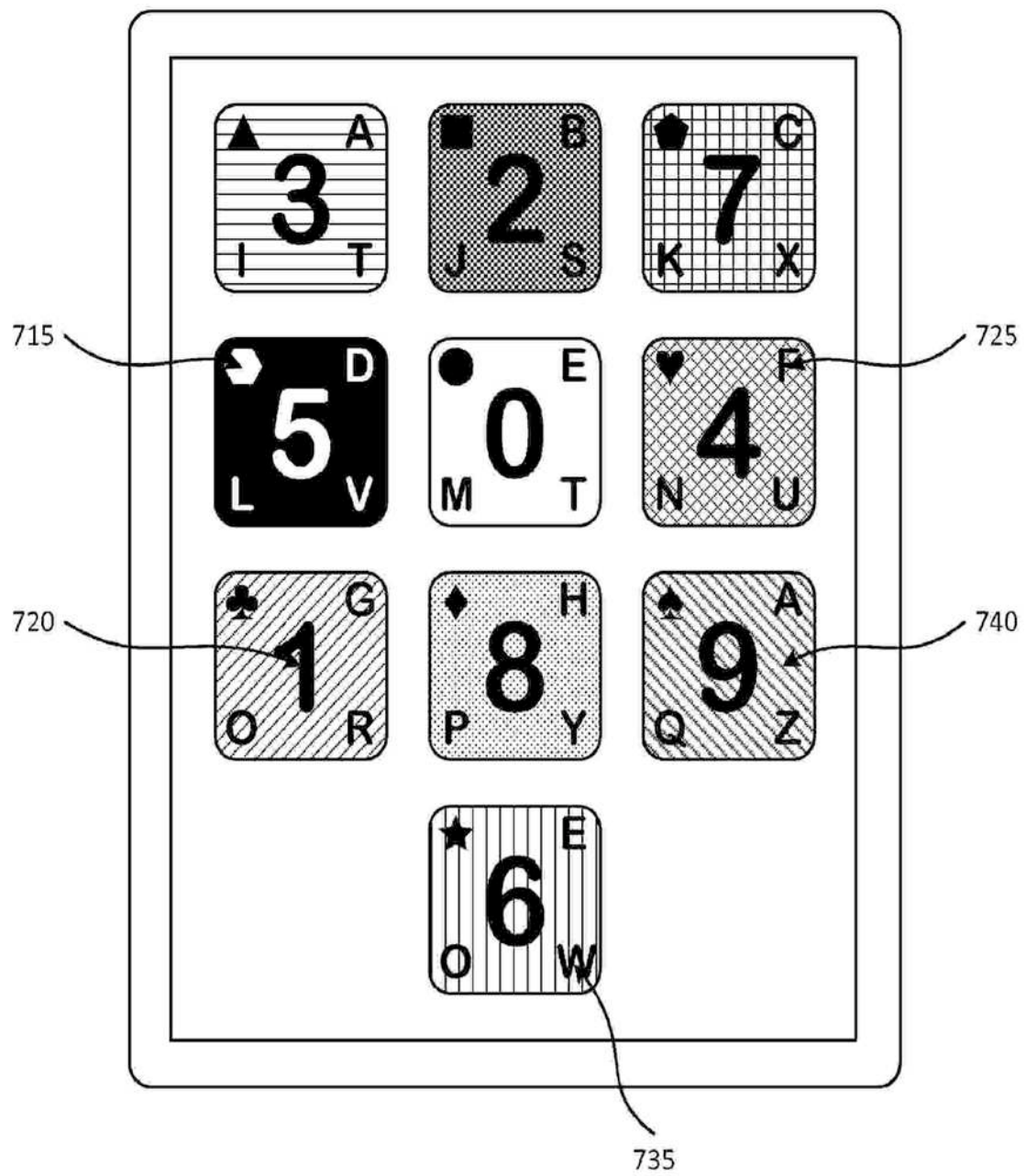
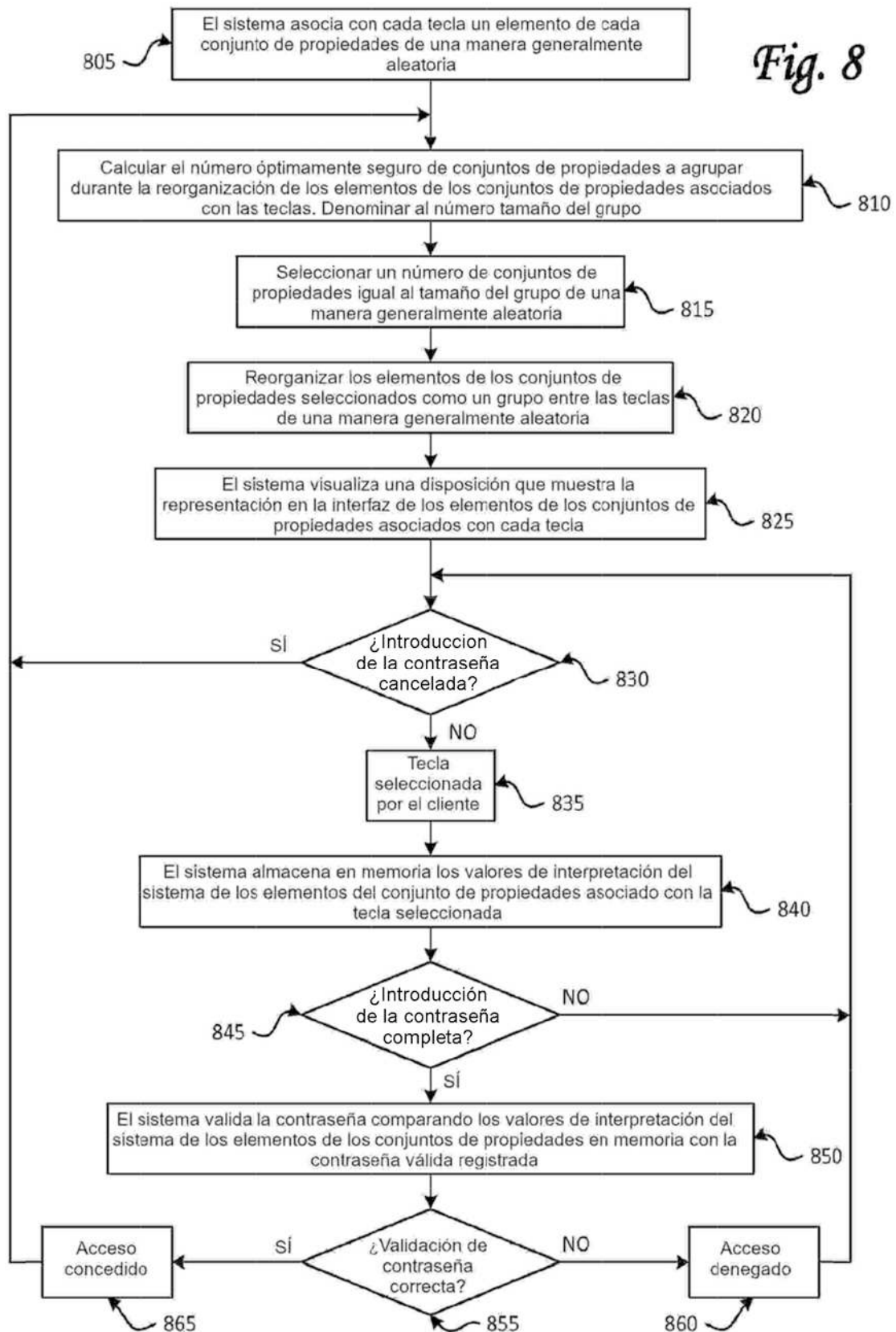
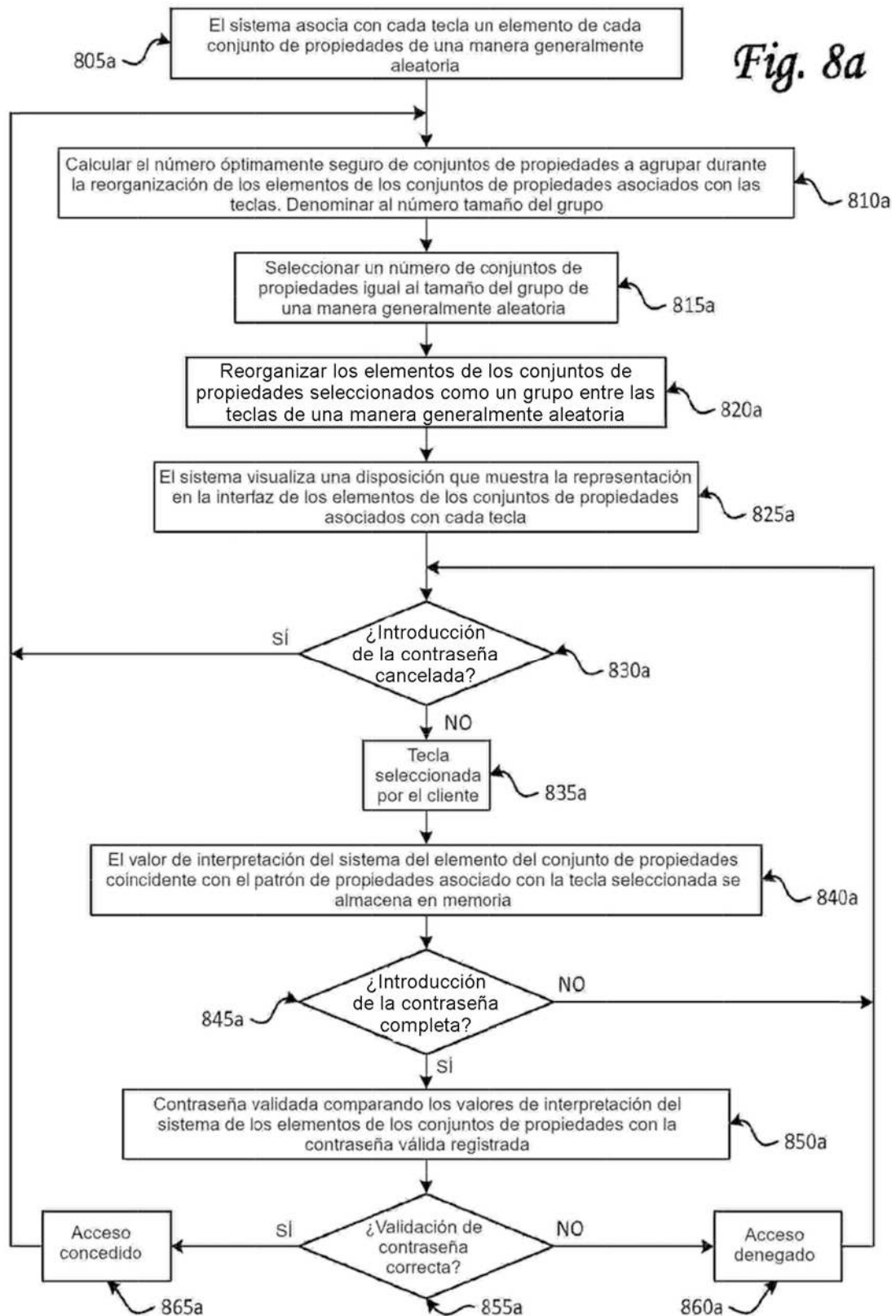
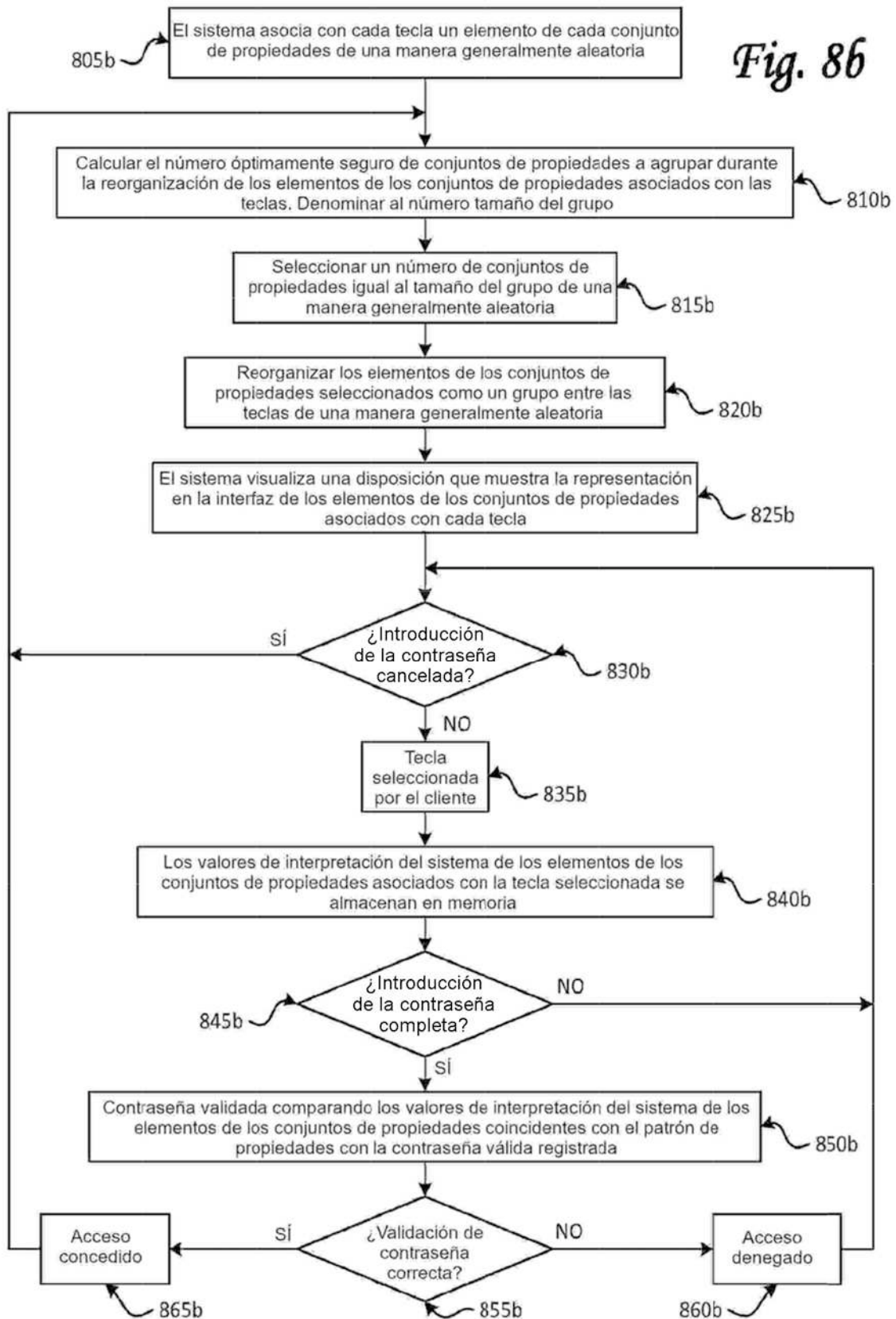


Fig. 7

Fig. 8







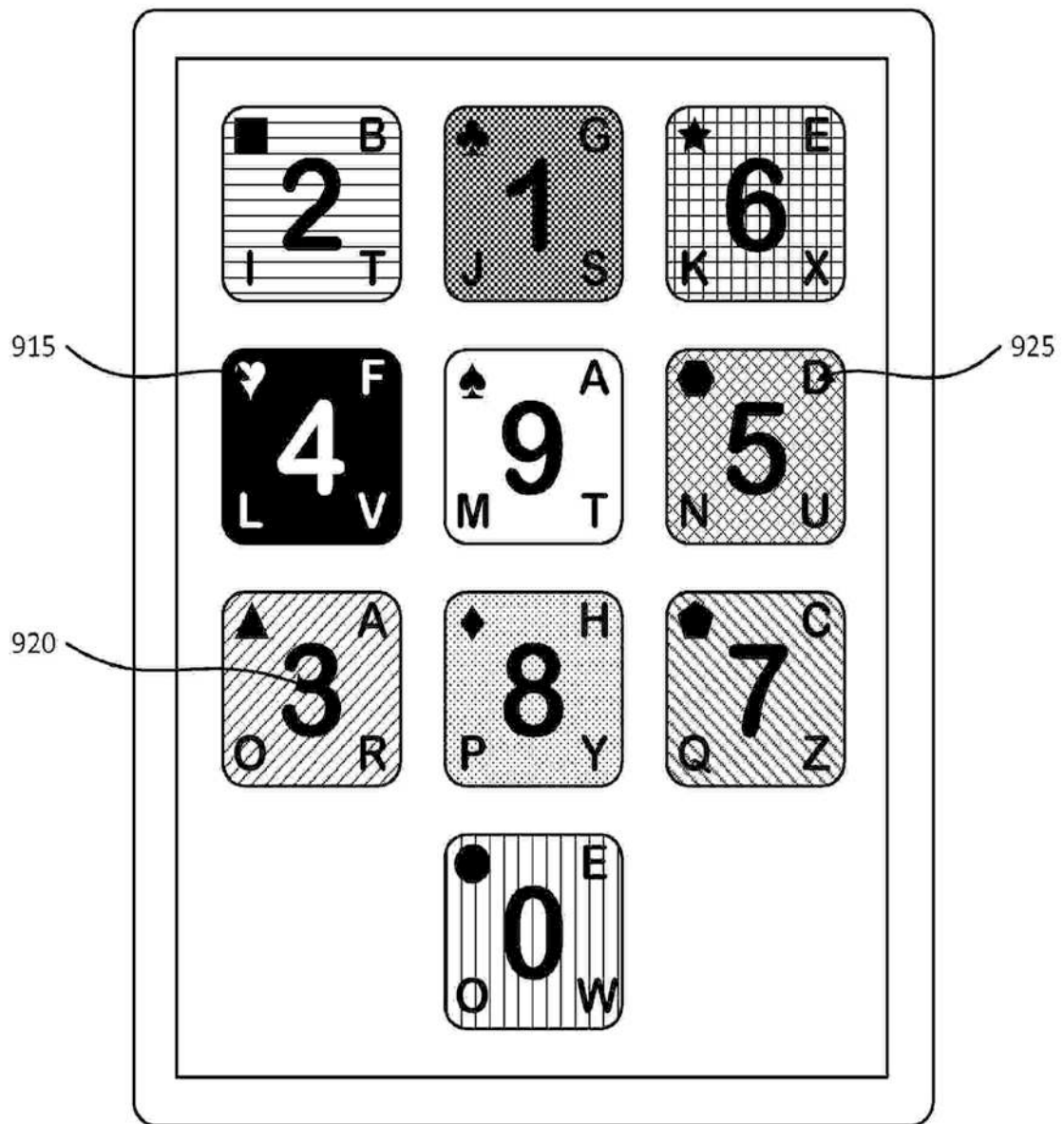


Fig. 9

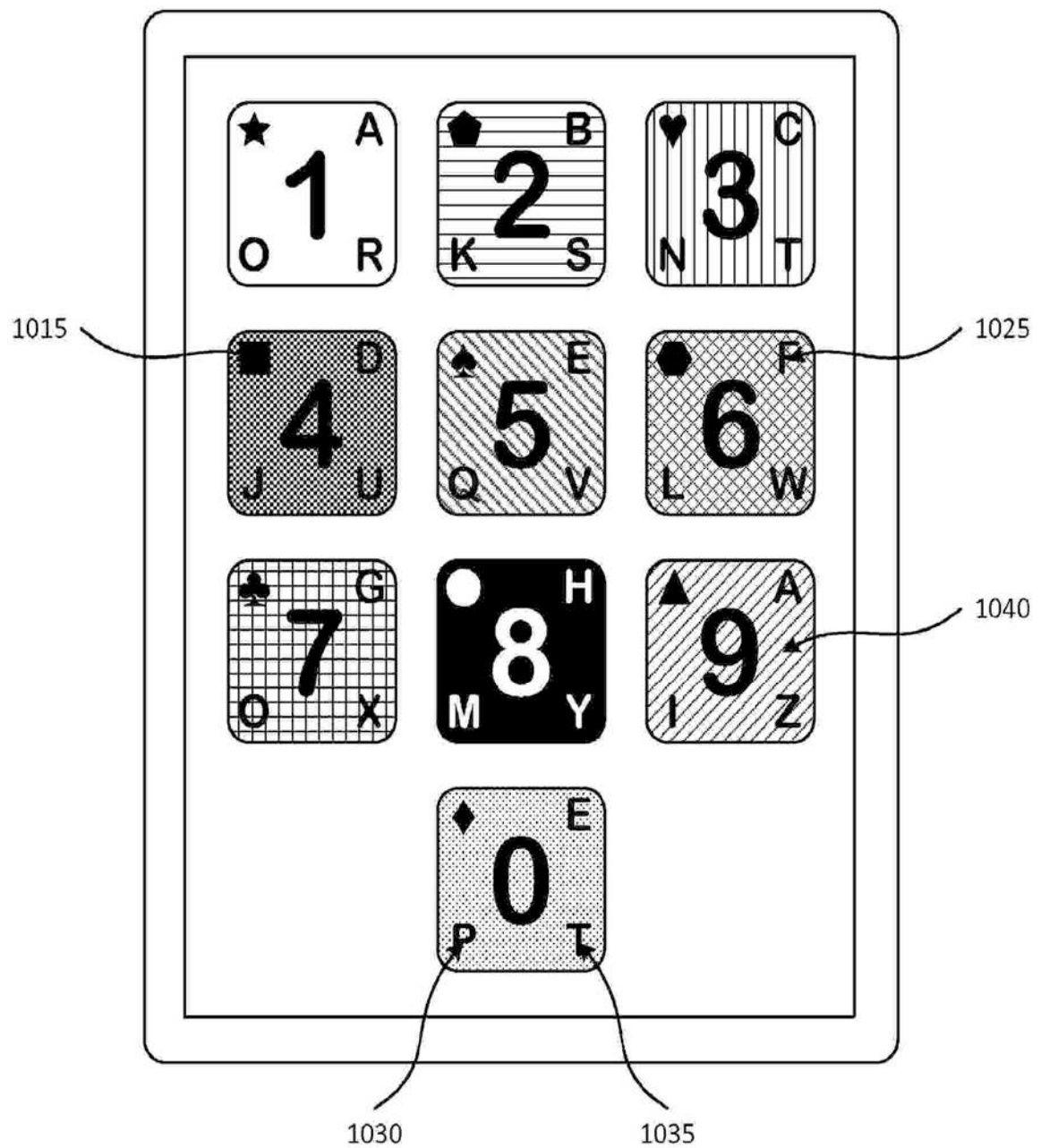


Fig. 10

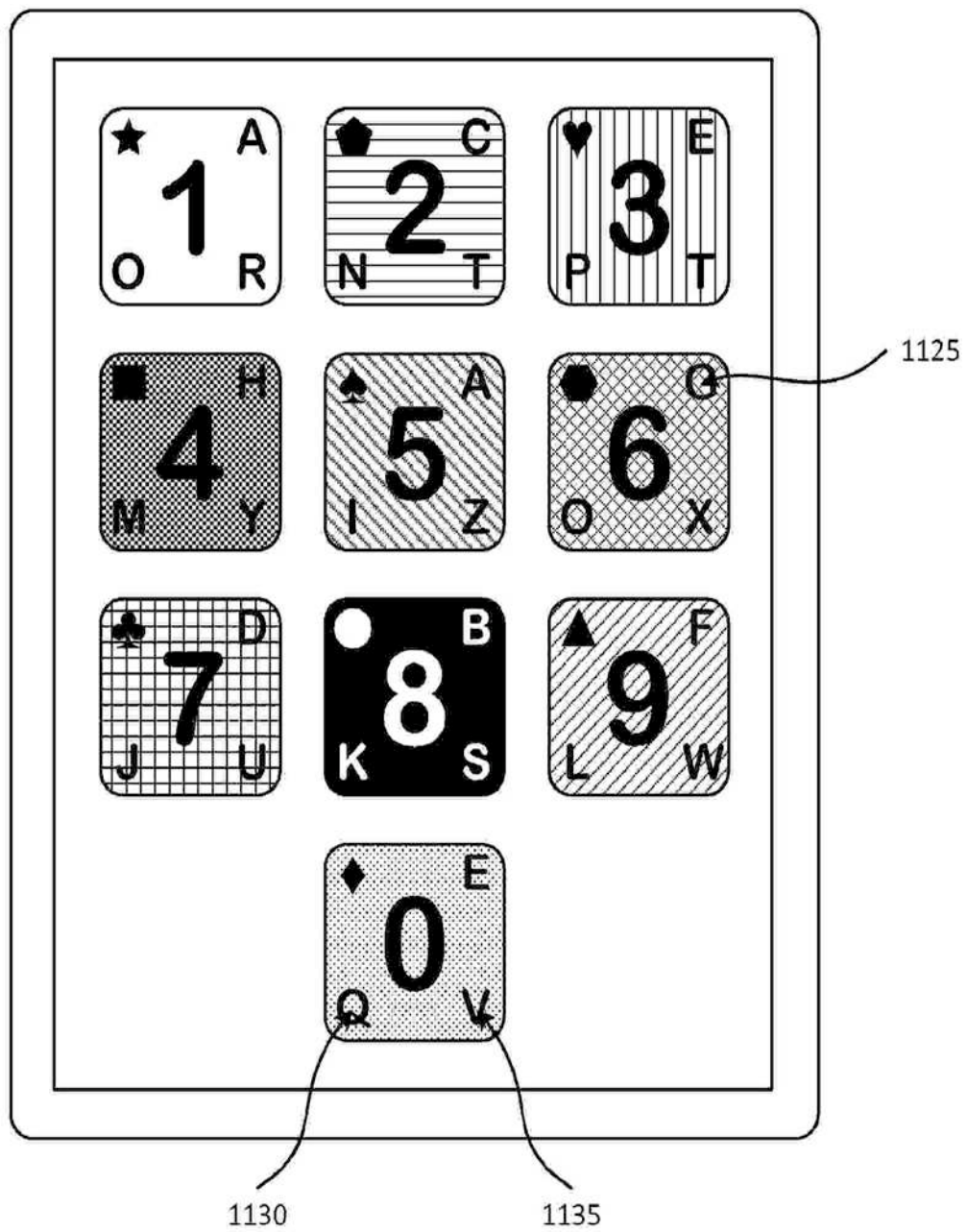


Fig. 11

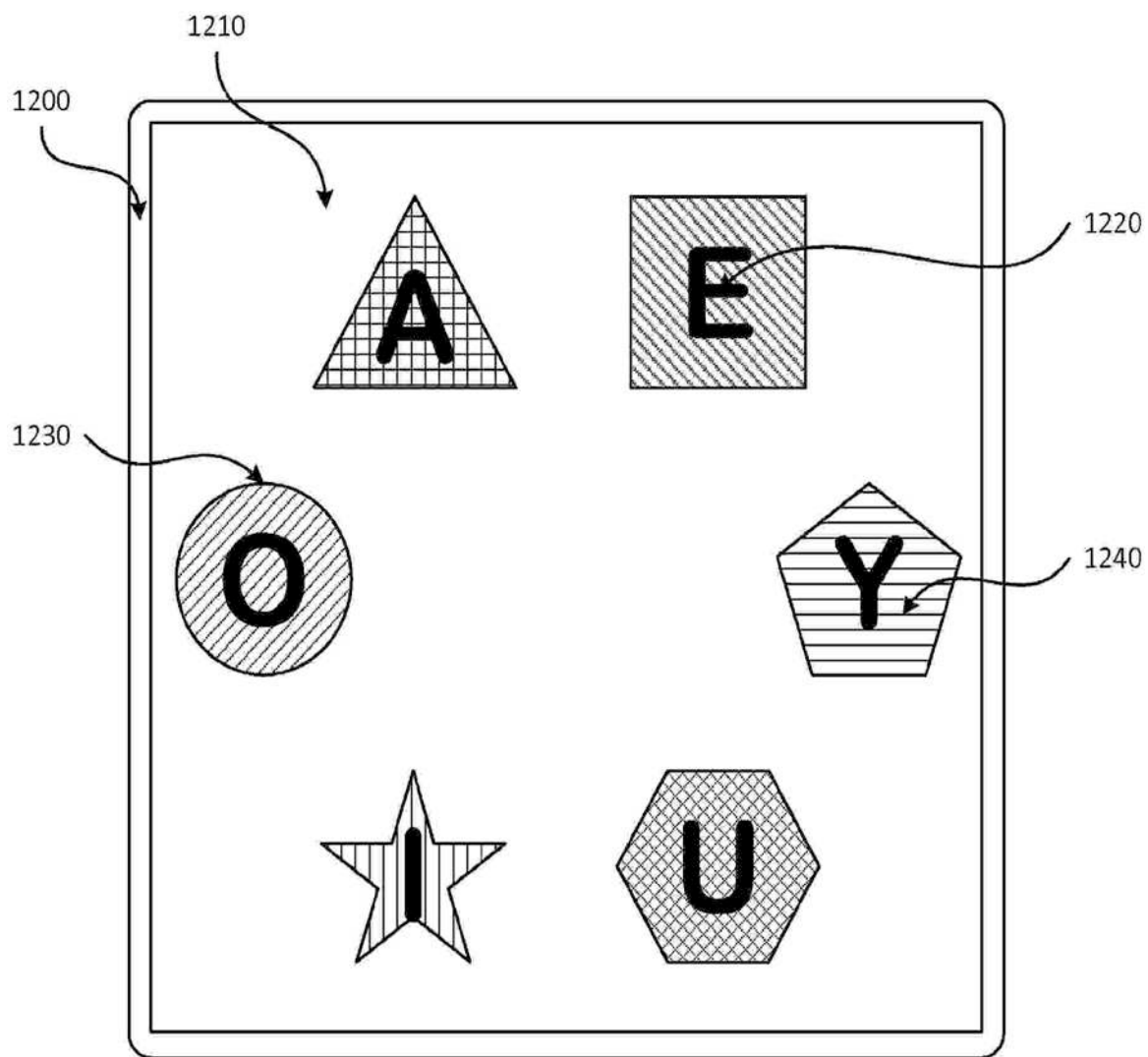


Fig. 12

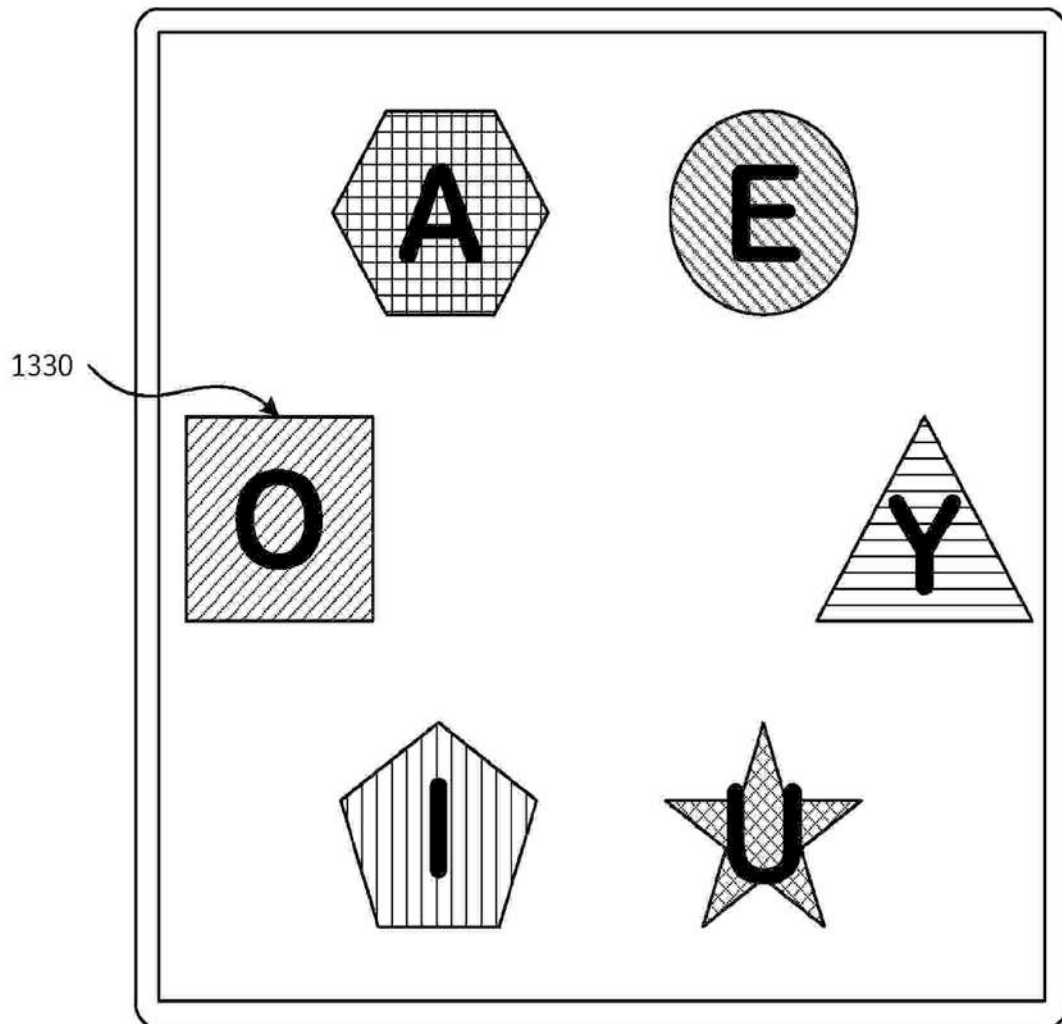


Fig. 13

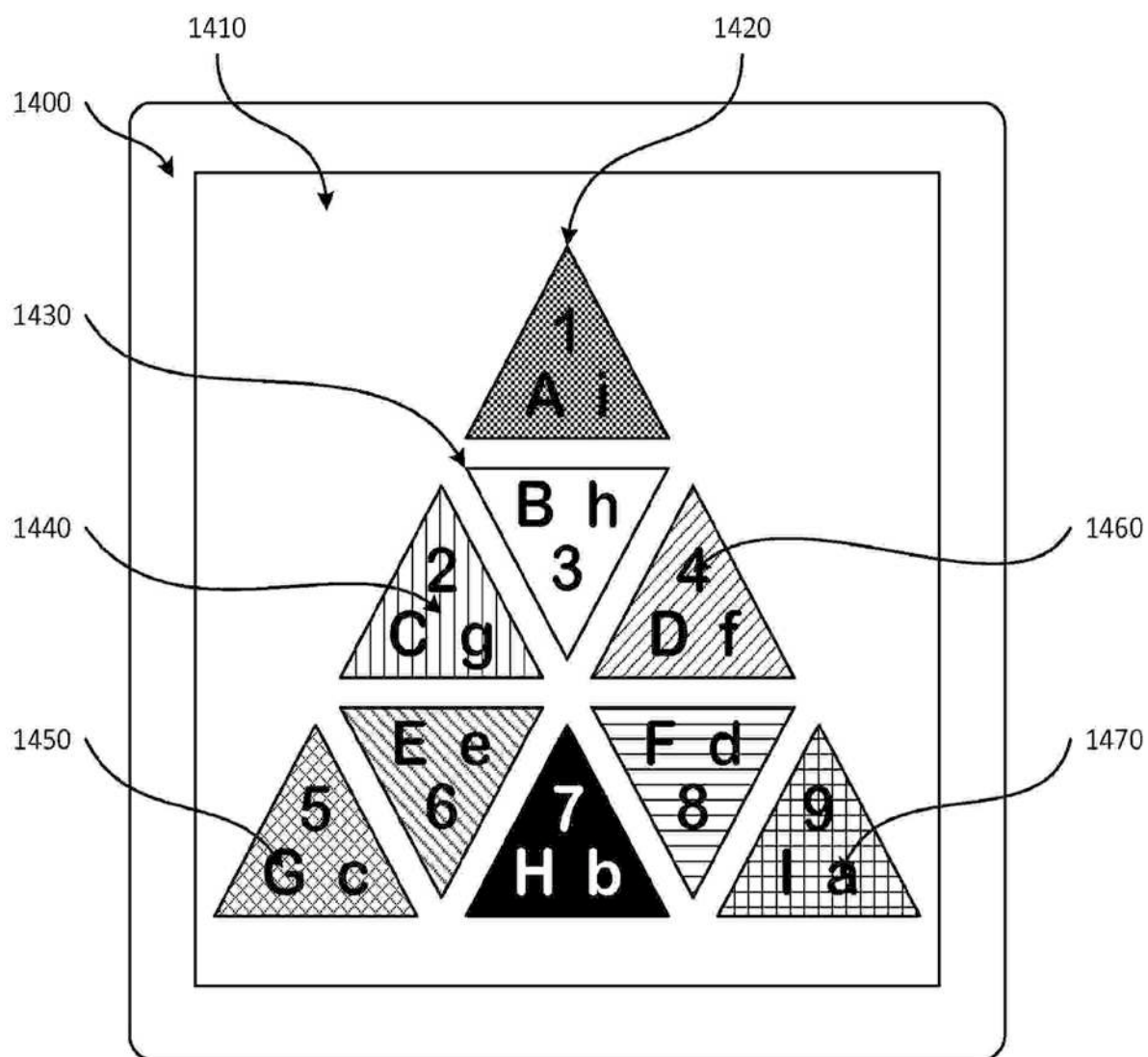


Fig. 14

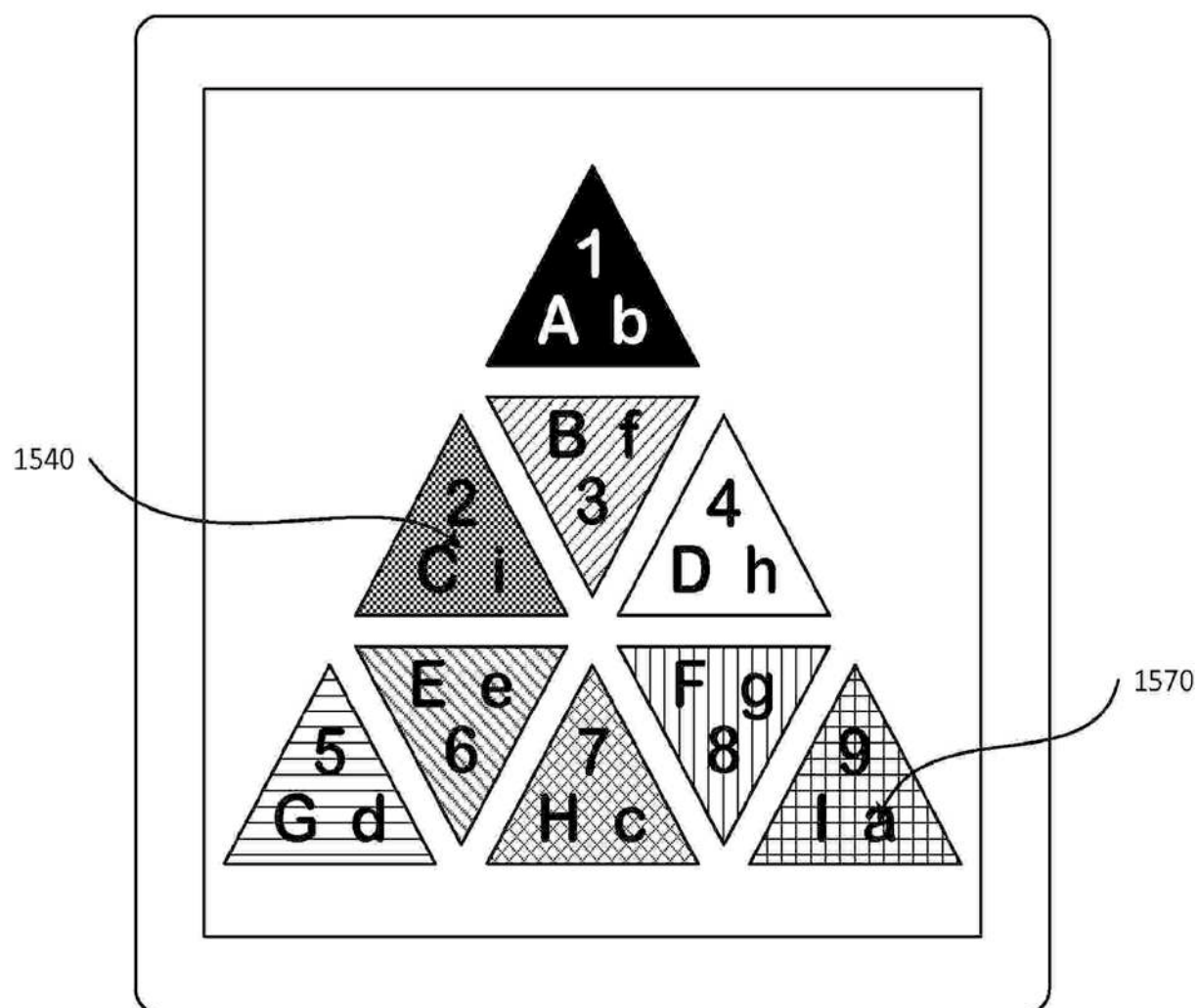


Fig. 15

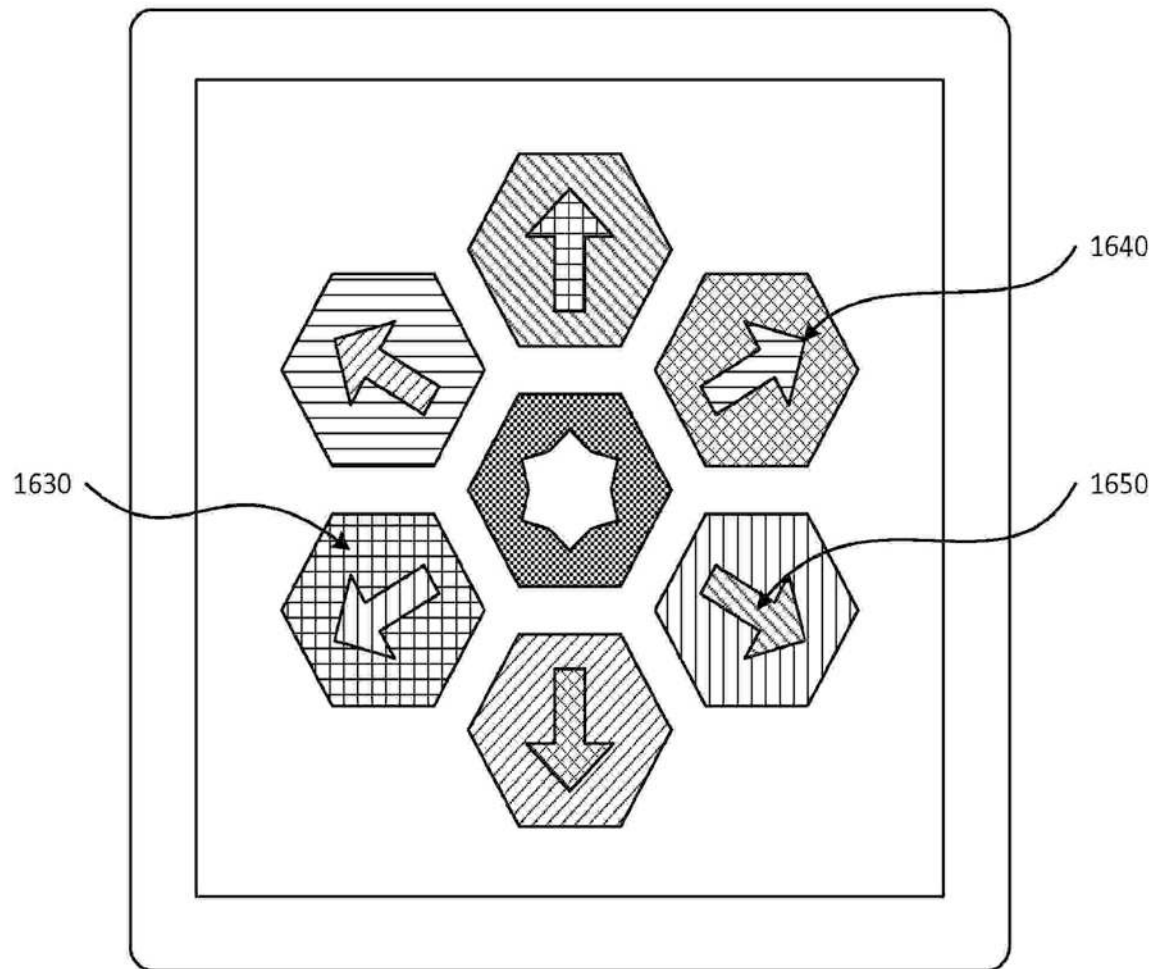


Fig. 16

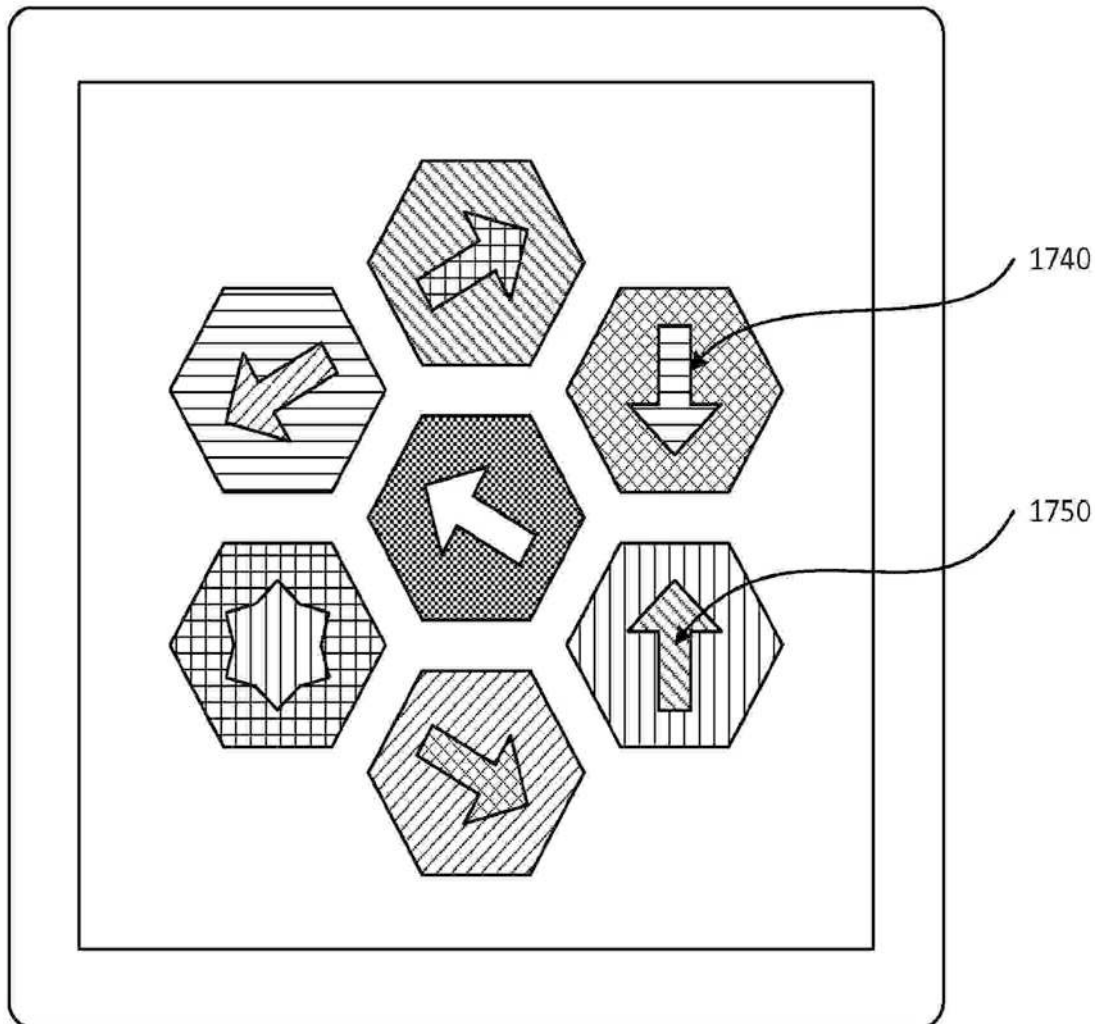


Fig. 17

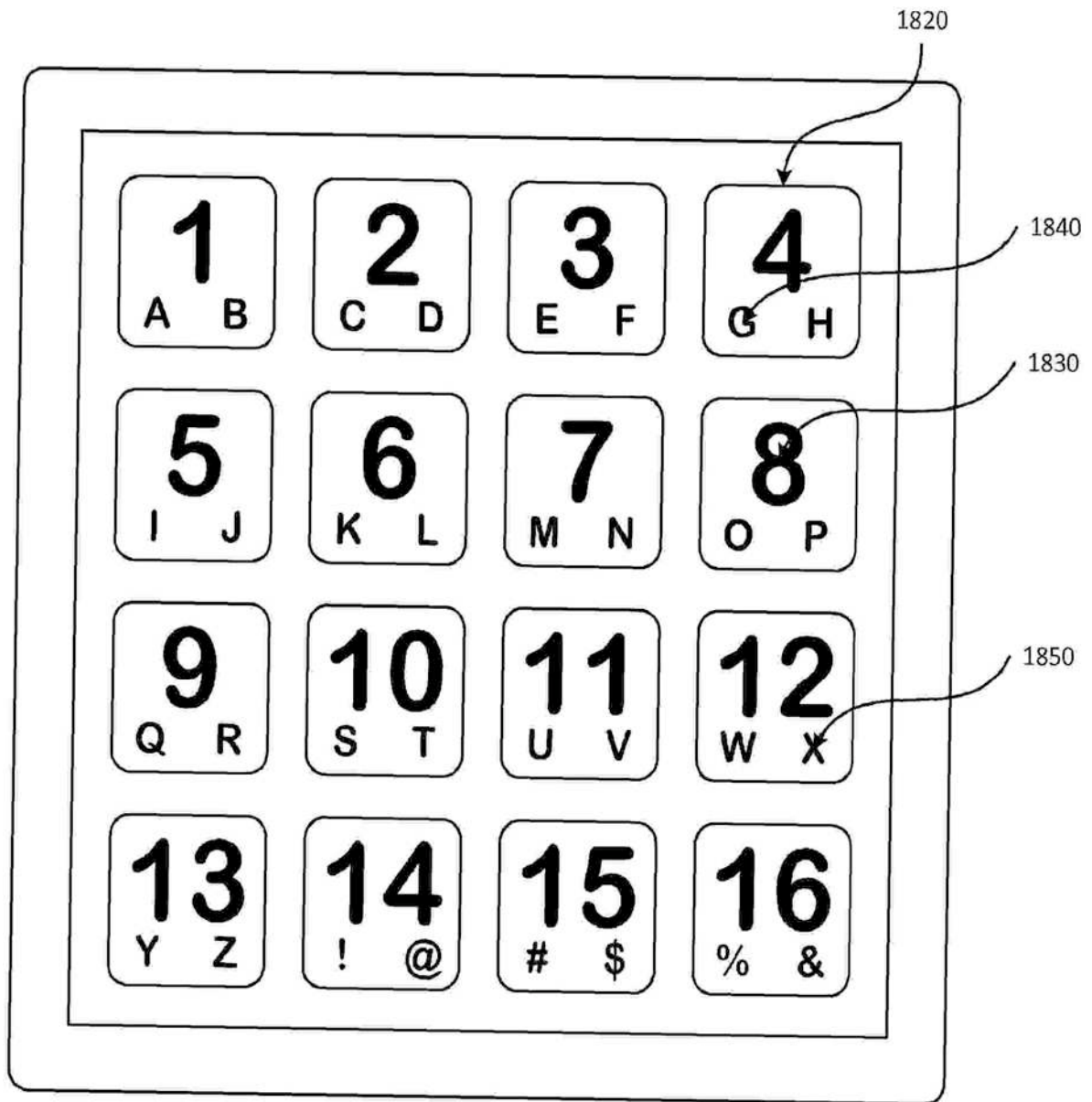


Fig. 18

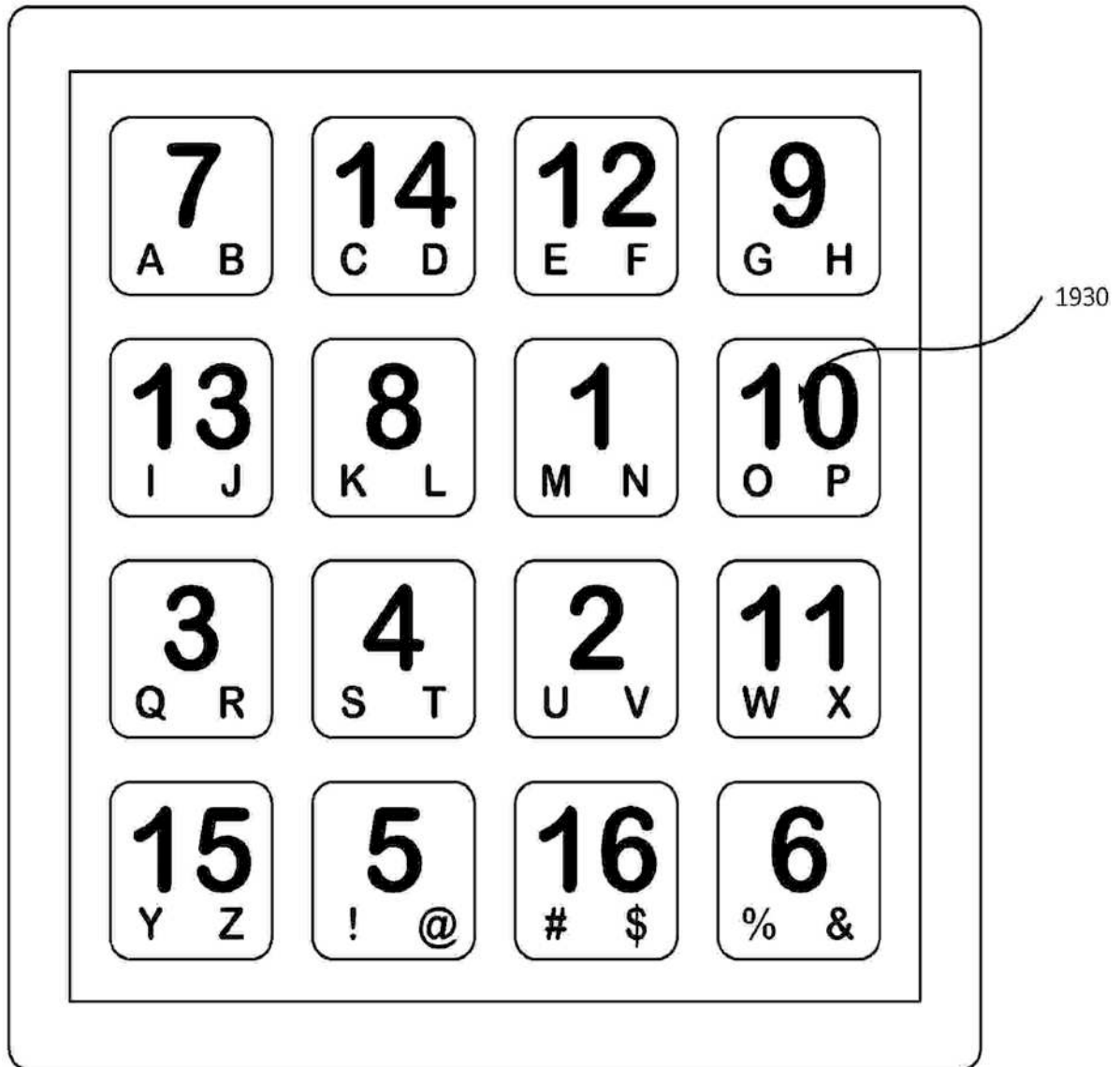


Fig. 19

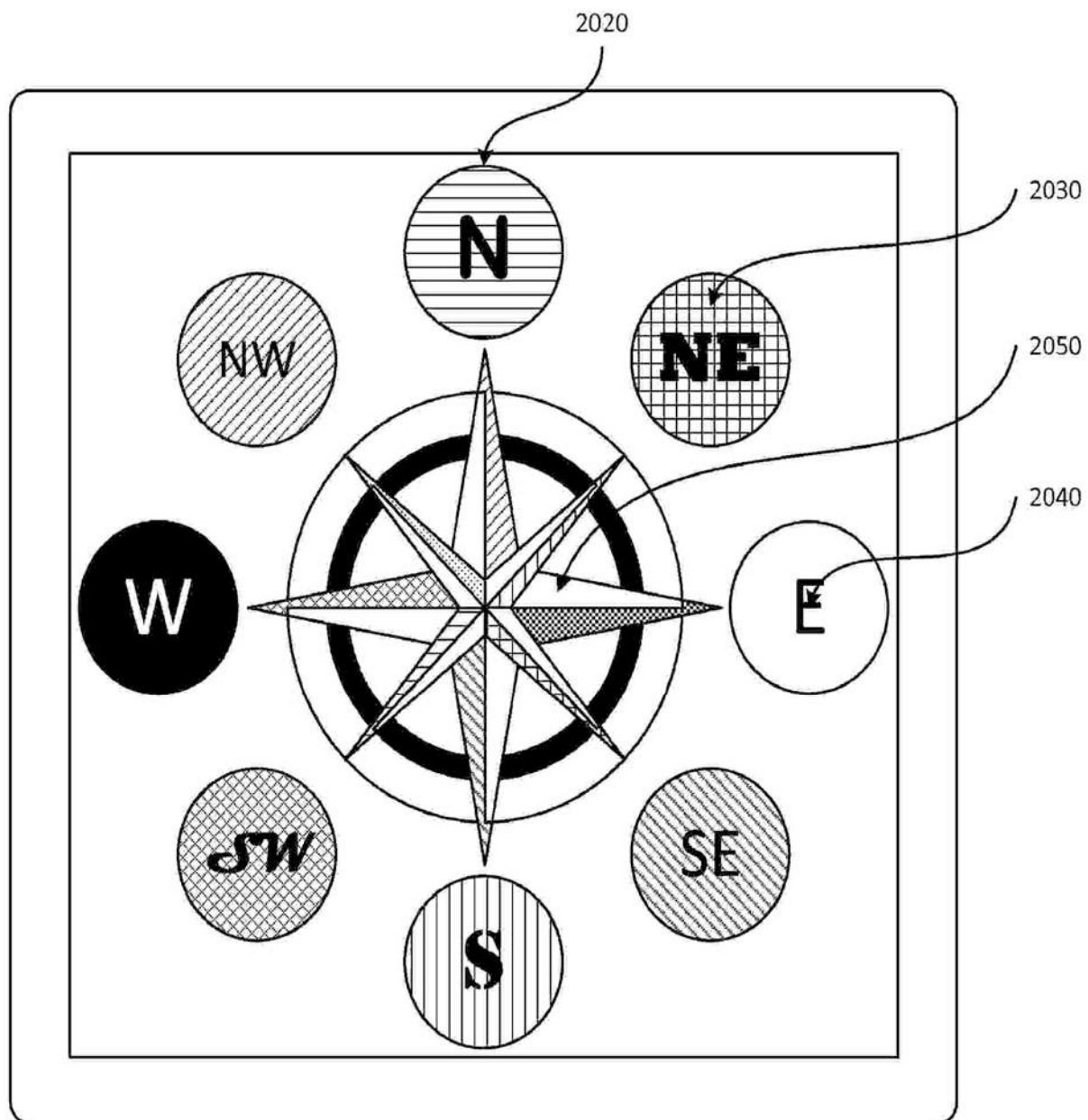


Fig. 20

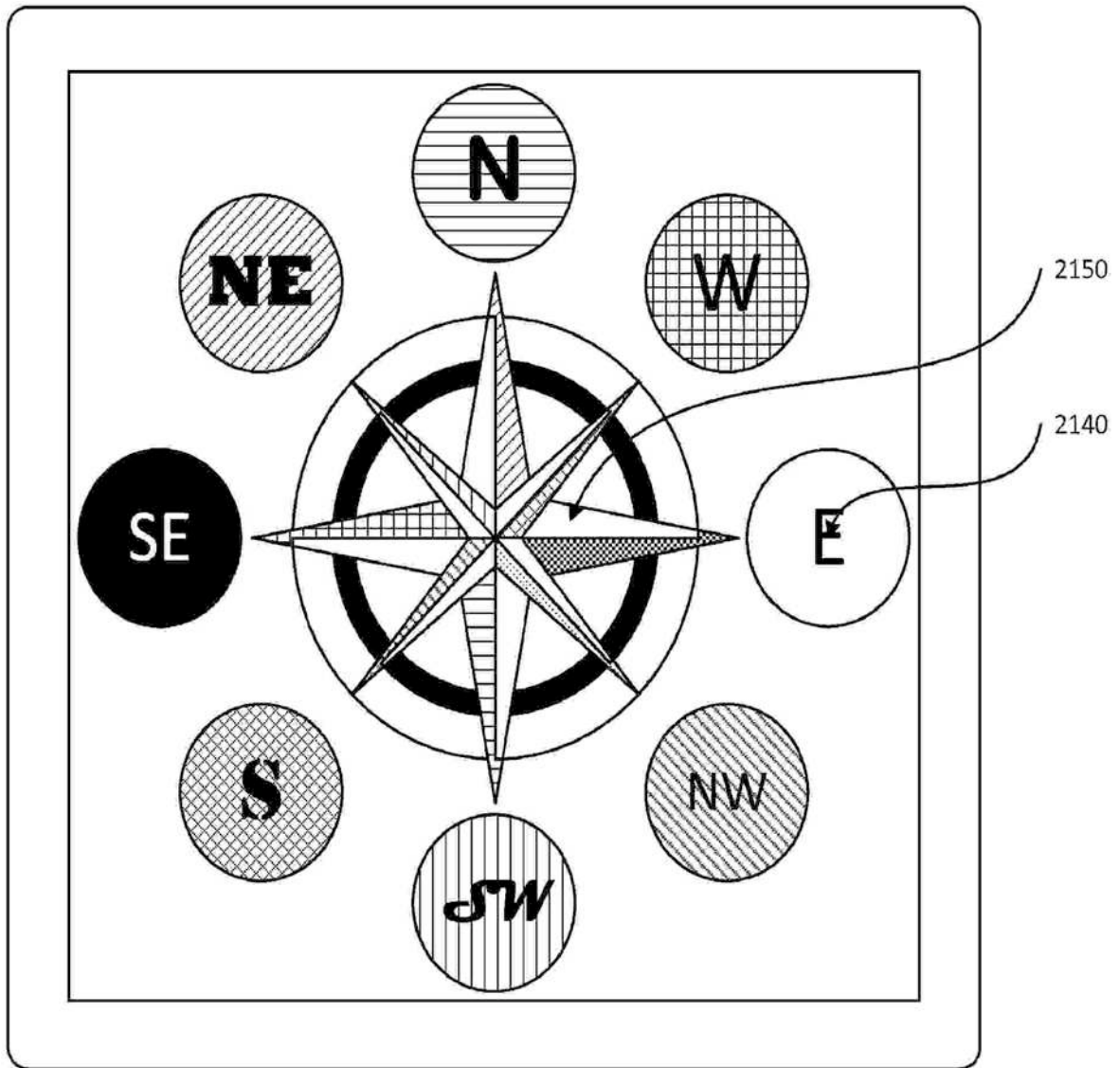


Fig. 21

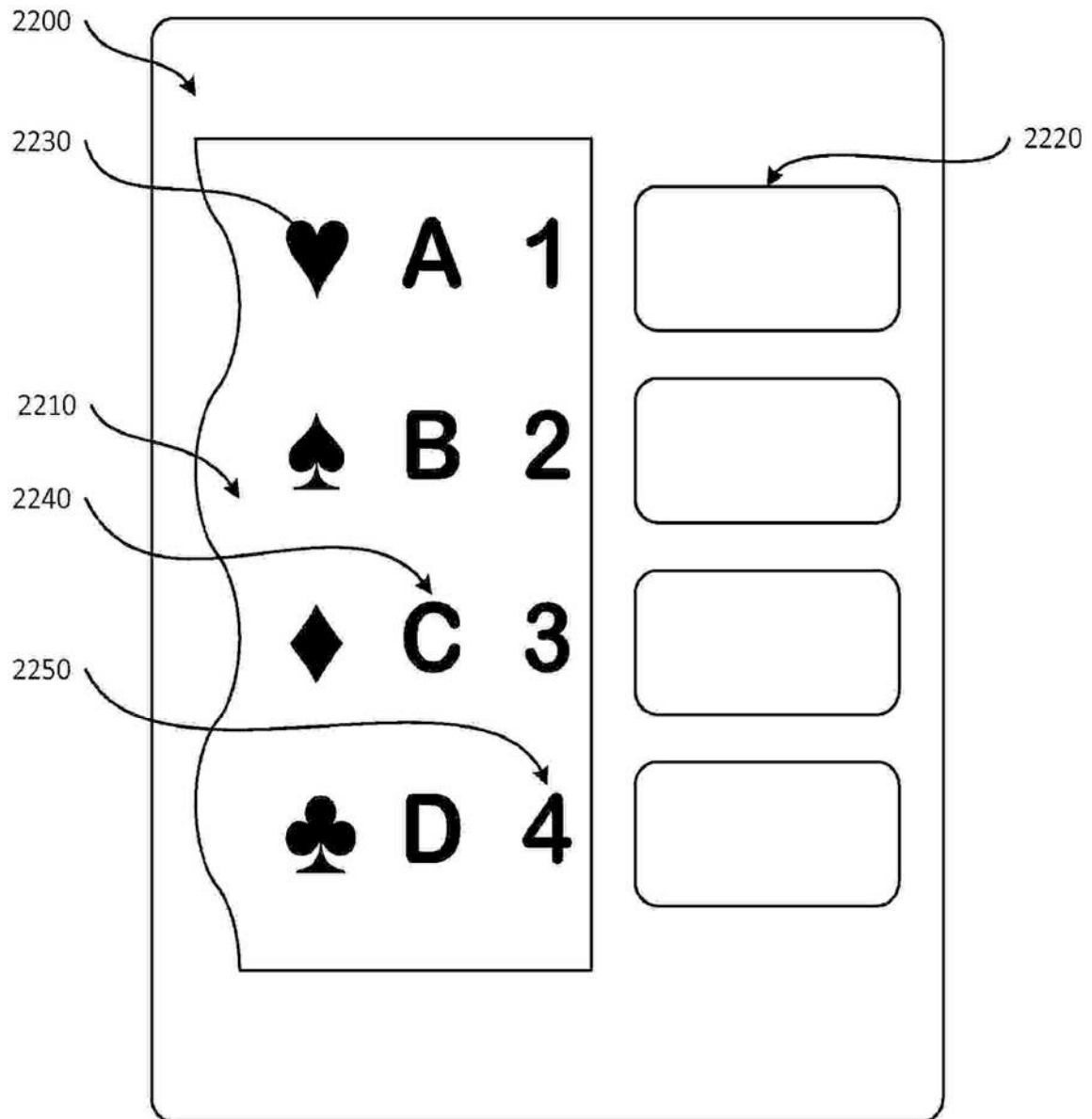


Fig. 22

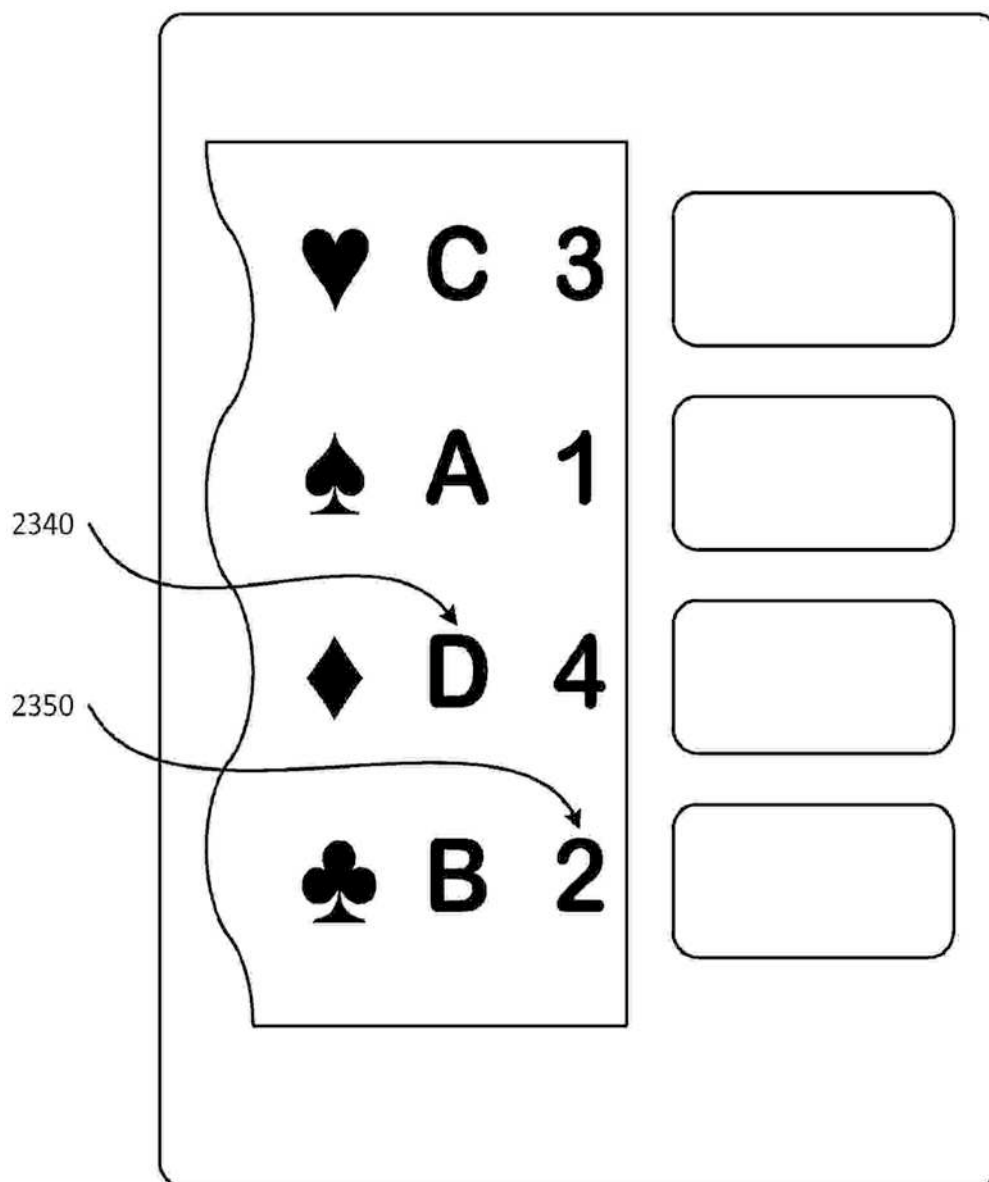


Fig. 23

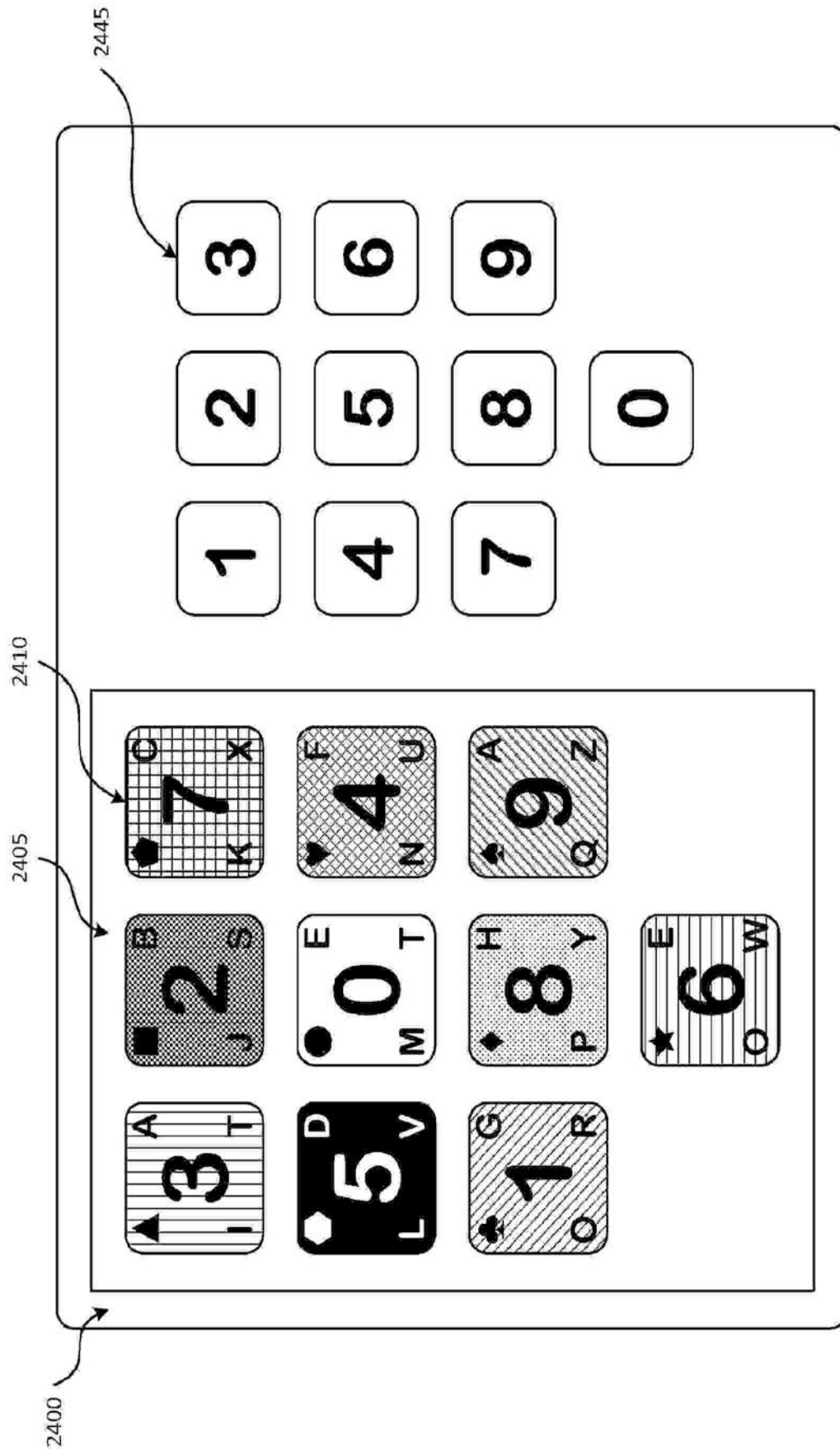


Fig. 24

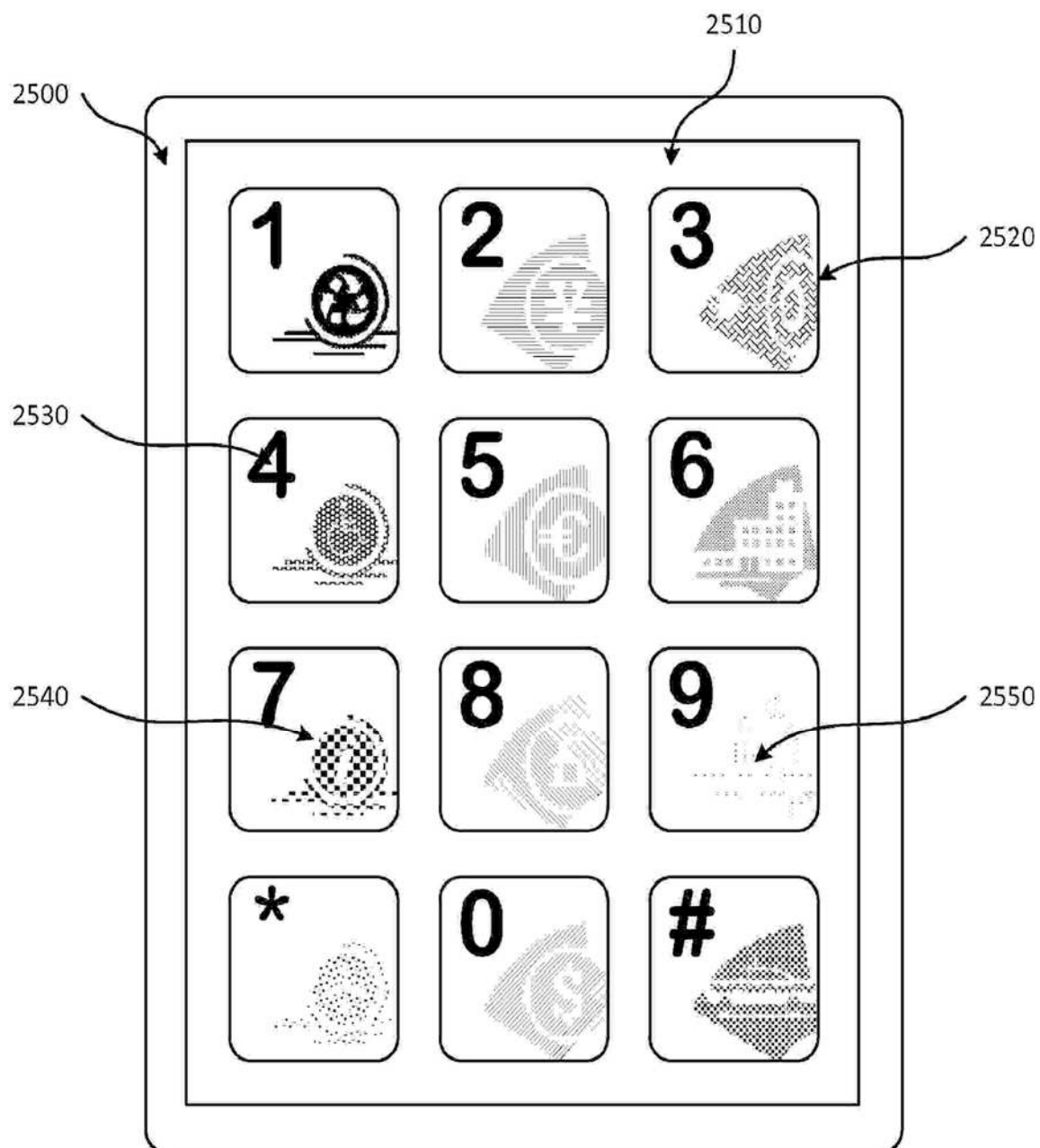


Fig. 25

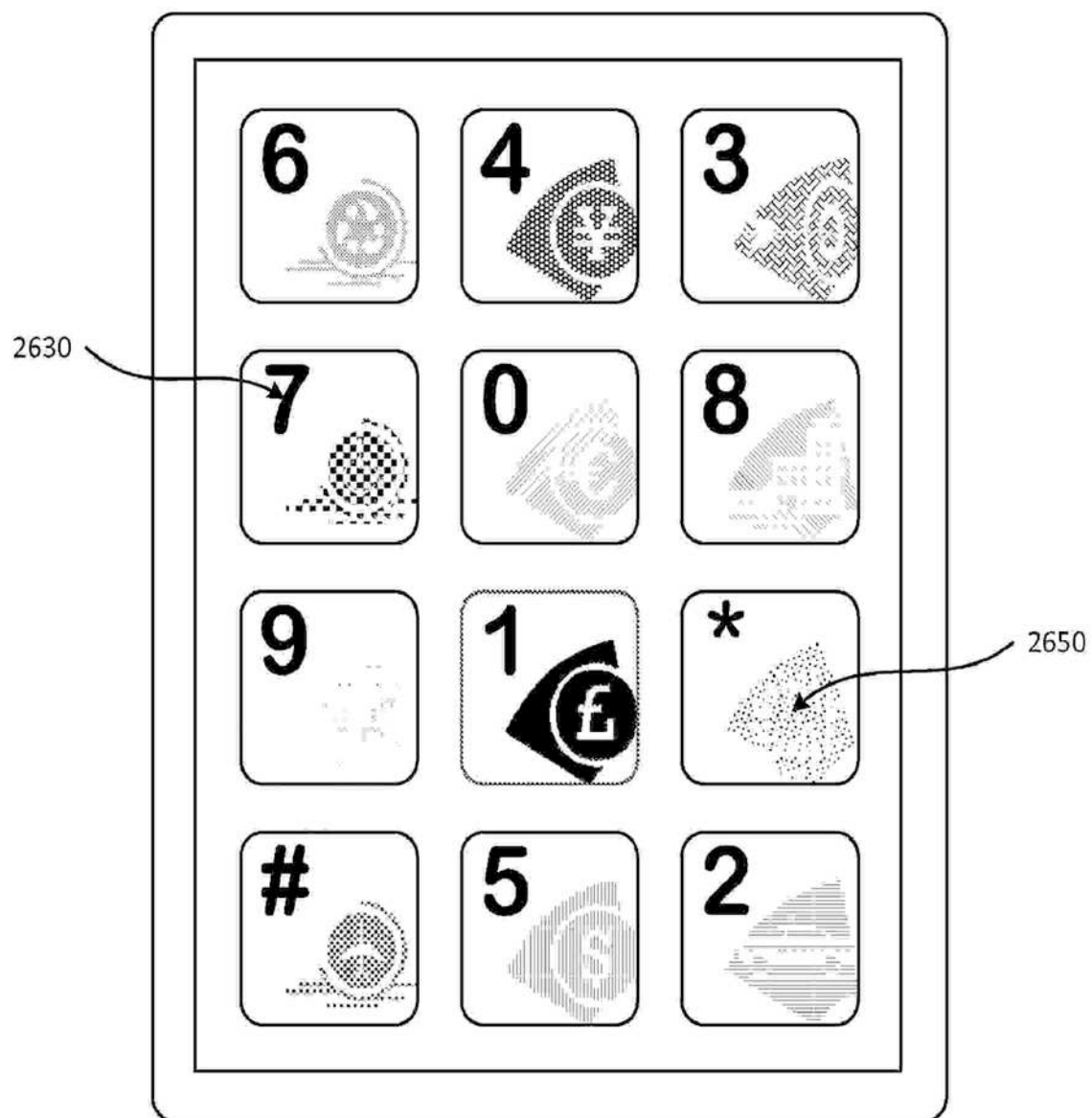


Fig. 26

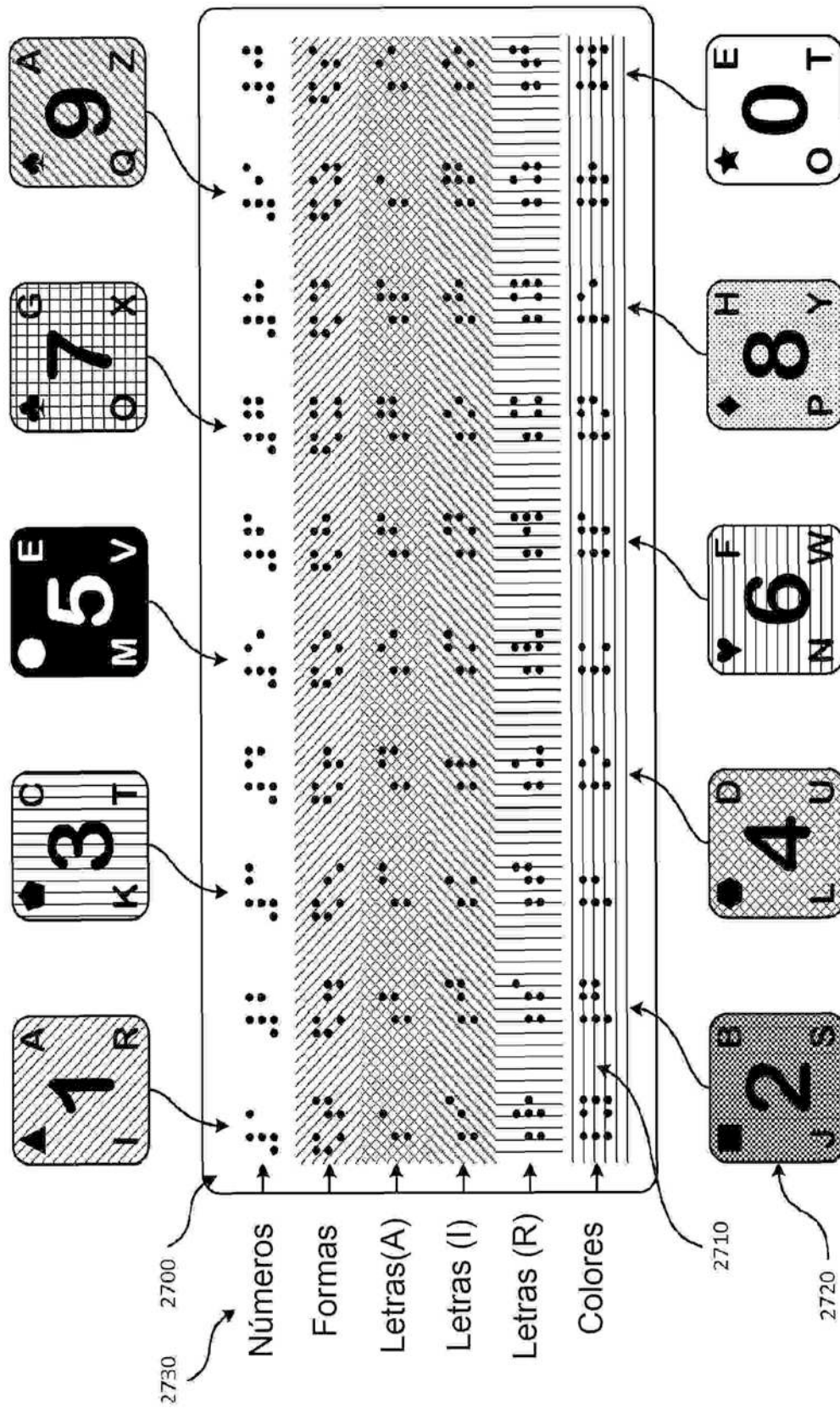


Fig. 27

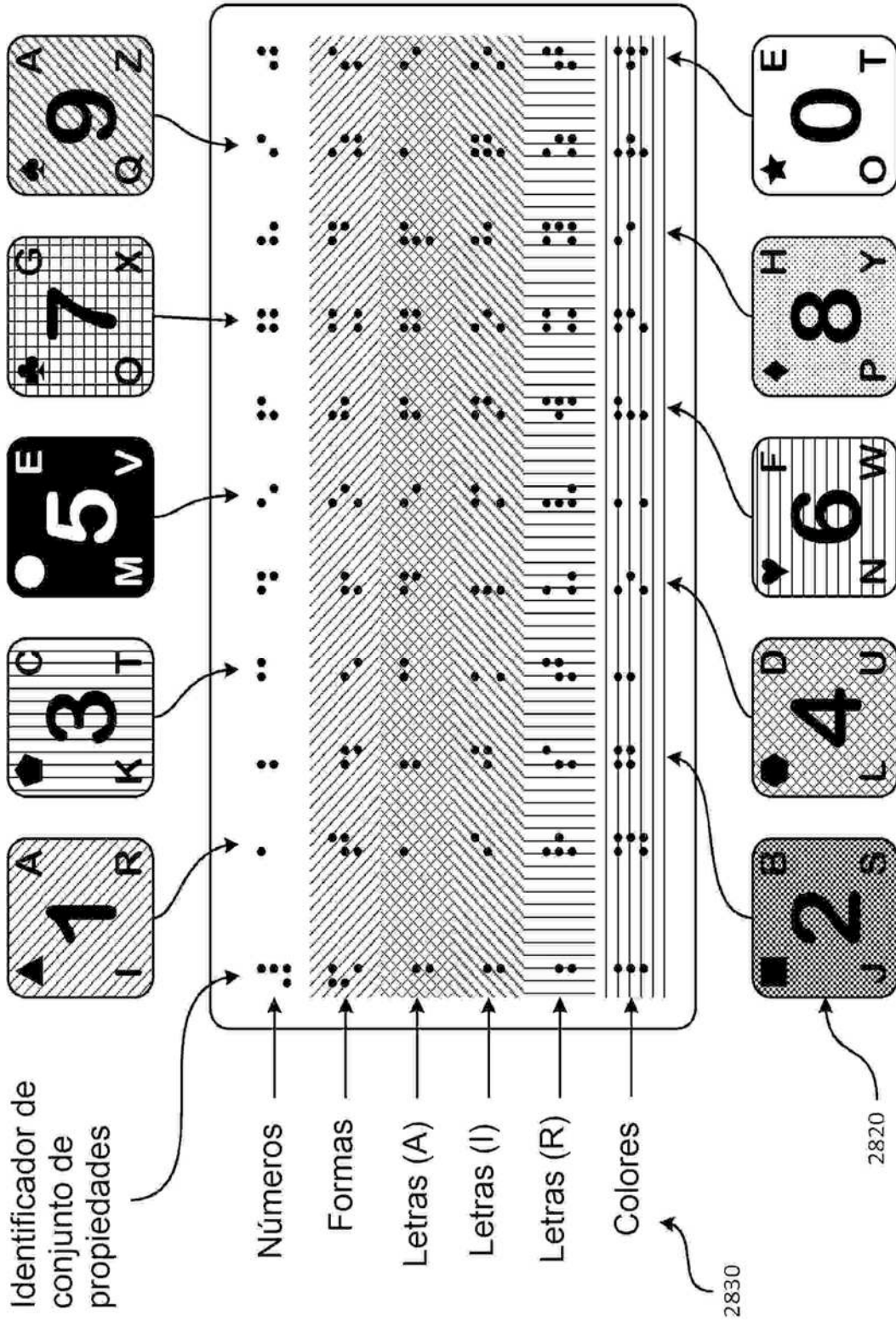
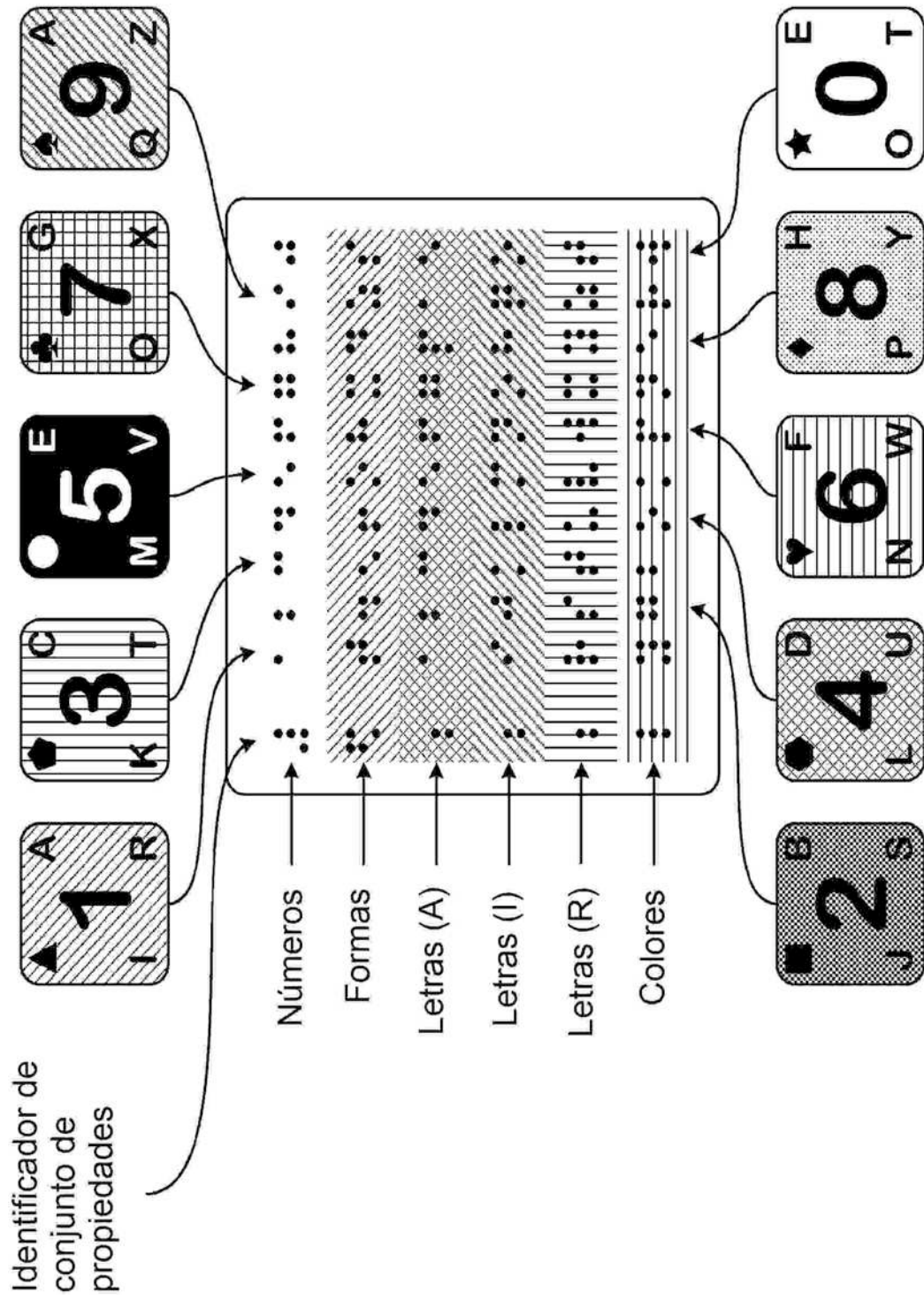


Fig. 28



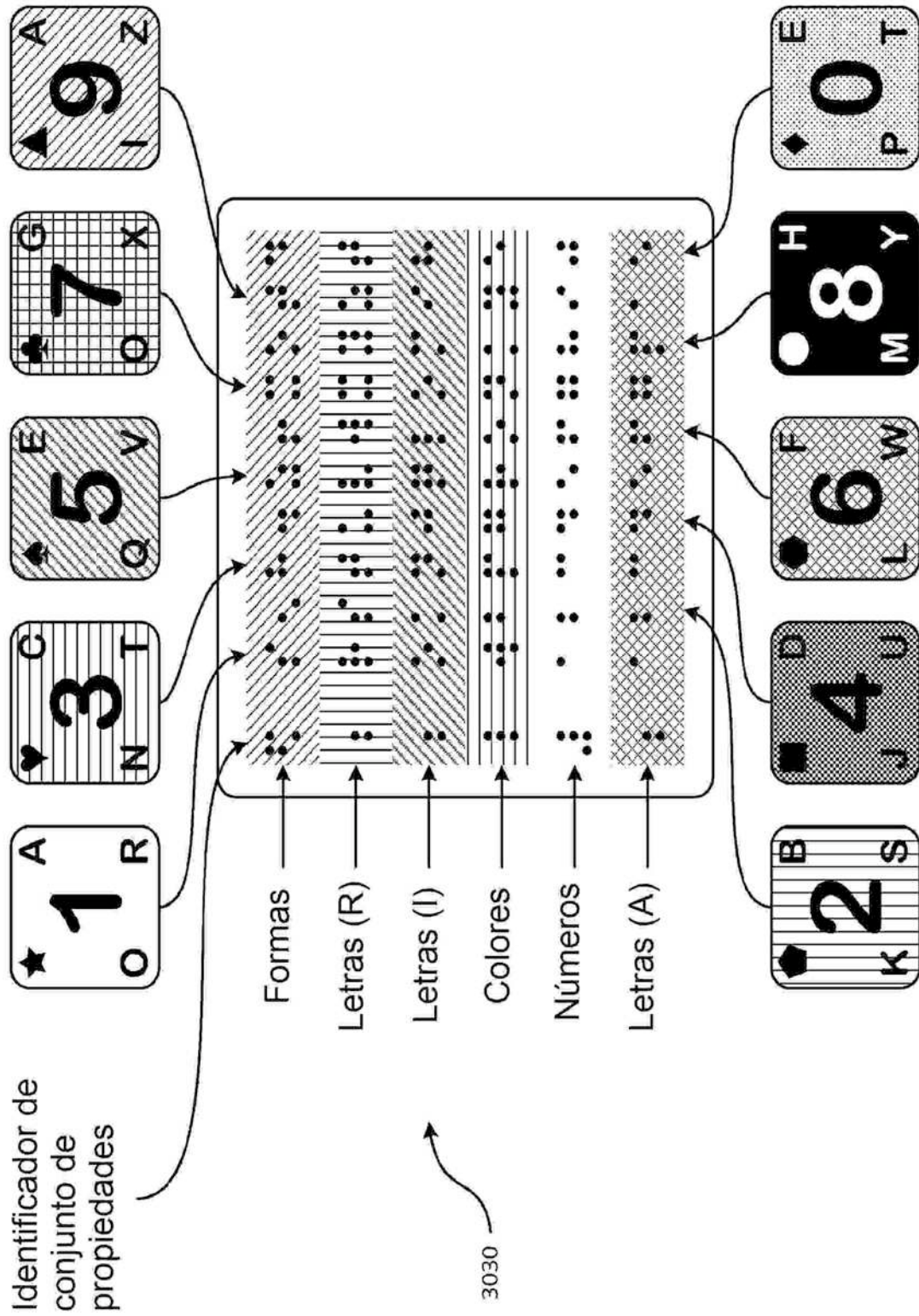


Fig. 30

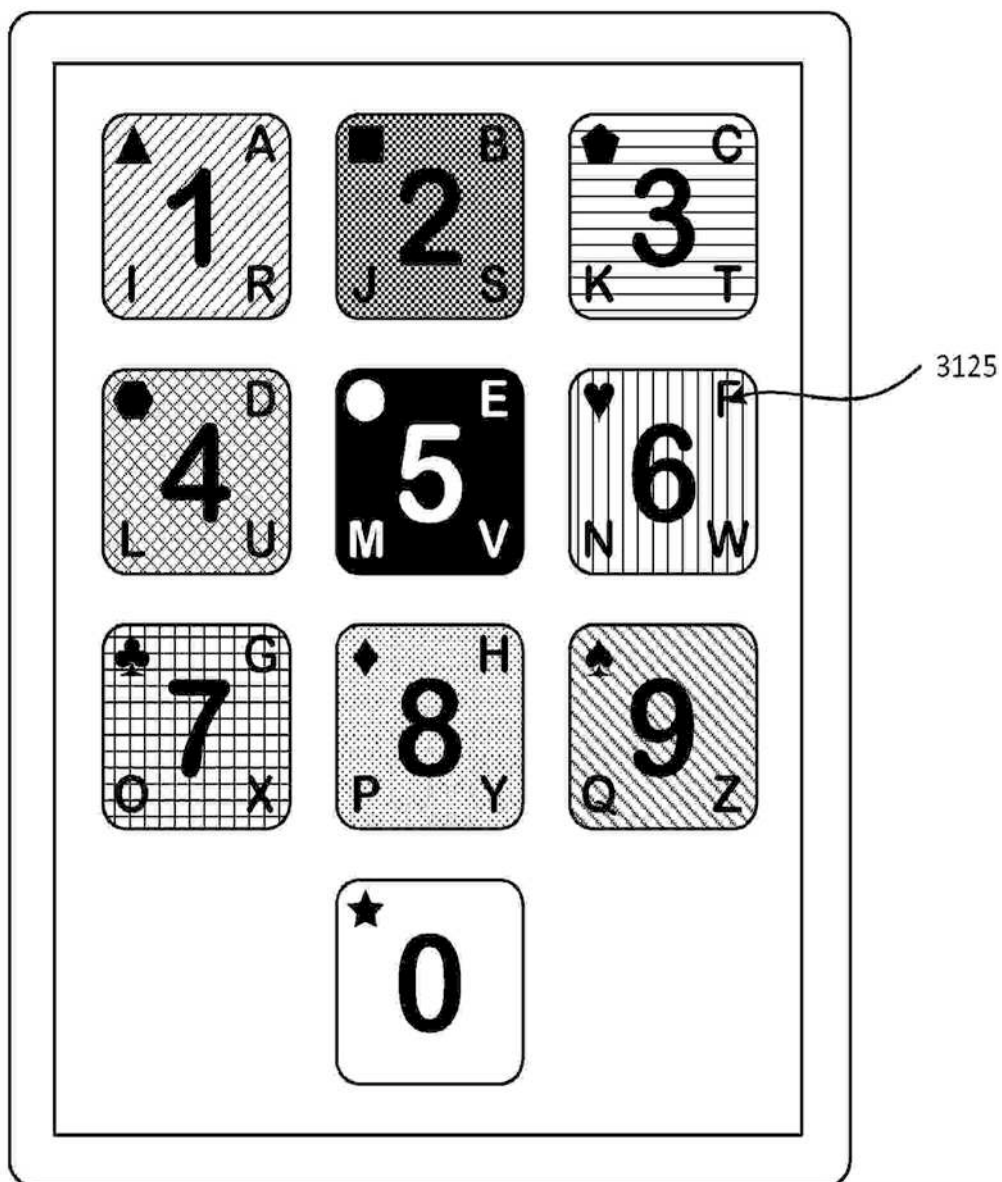
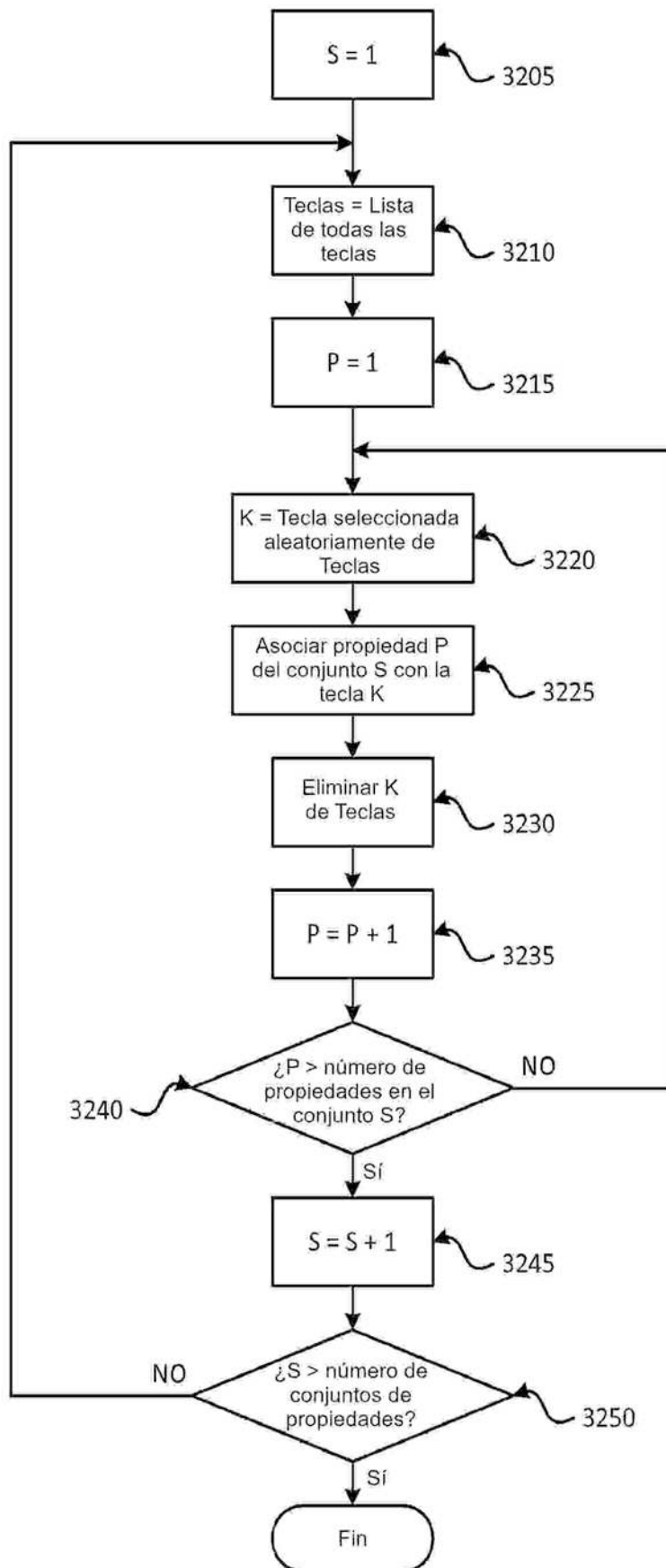


Fig. 31

Fig. 32

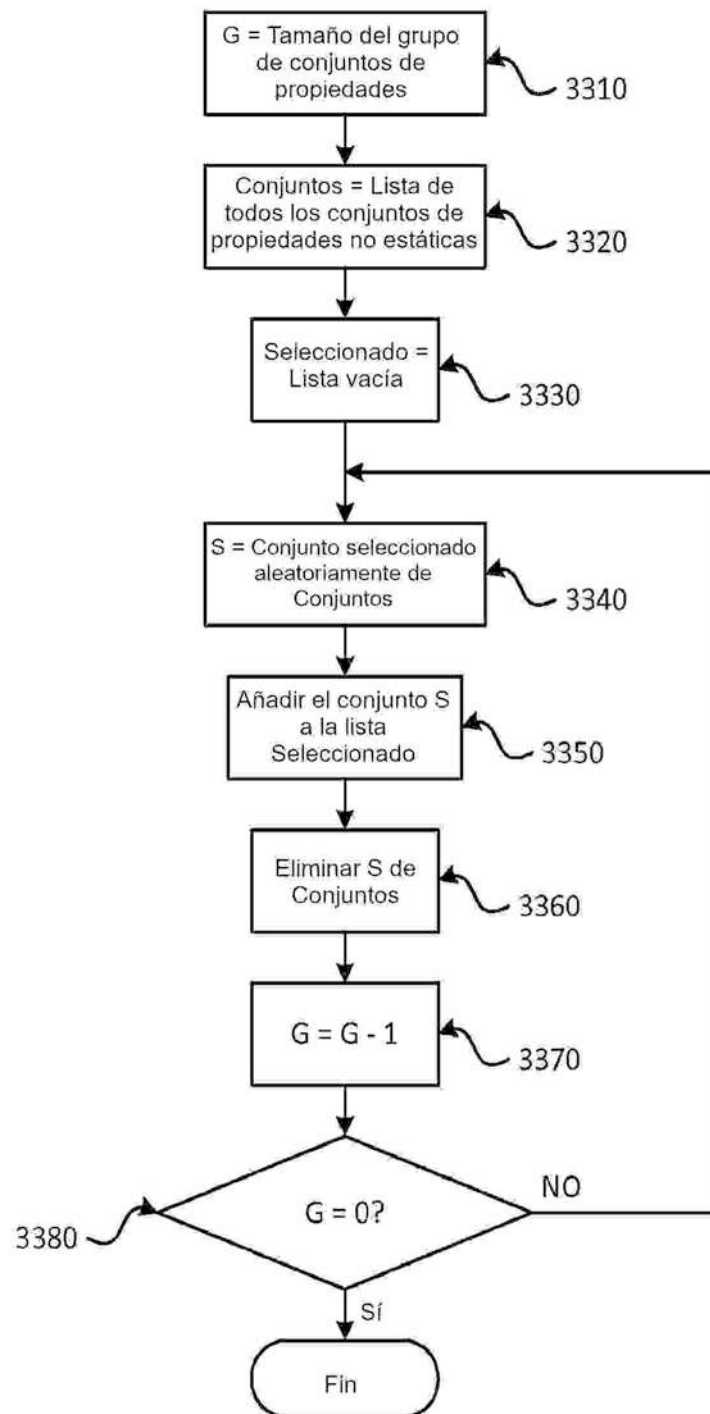


Fig. 33

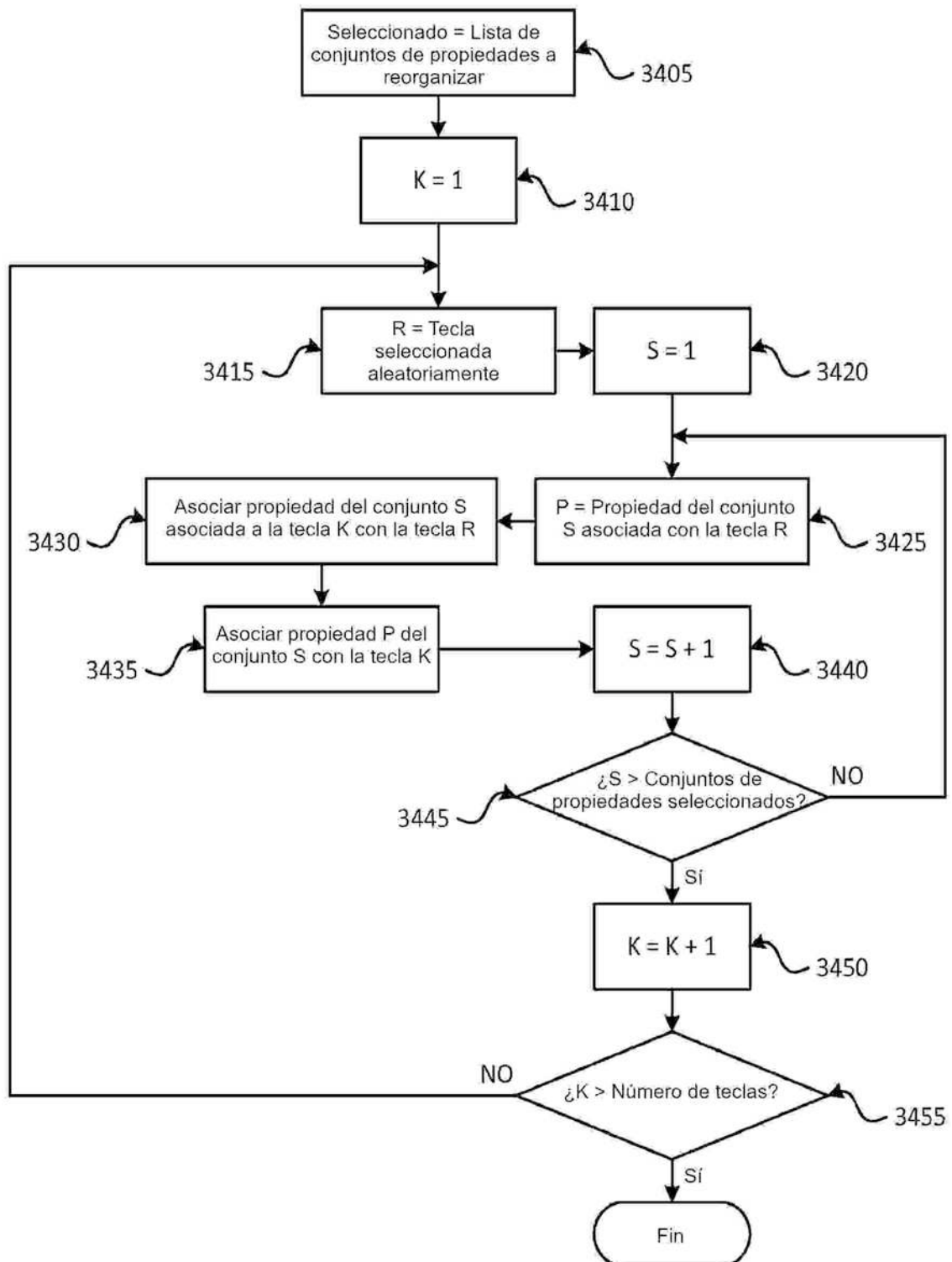


Fig. 34



Fig. 35

Fig. 36a

Dispersión de propiedades

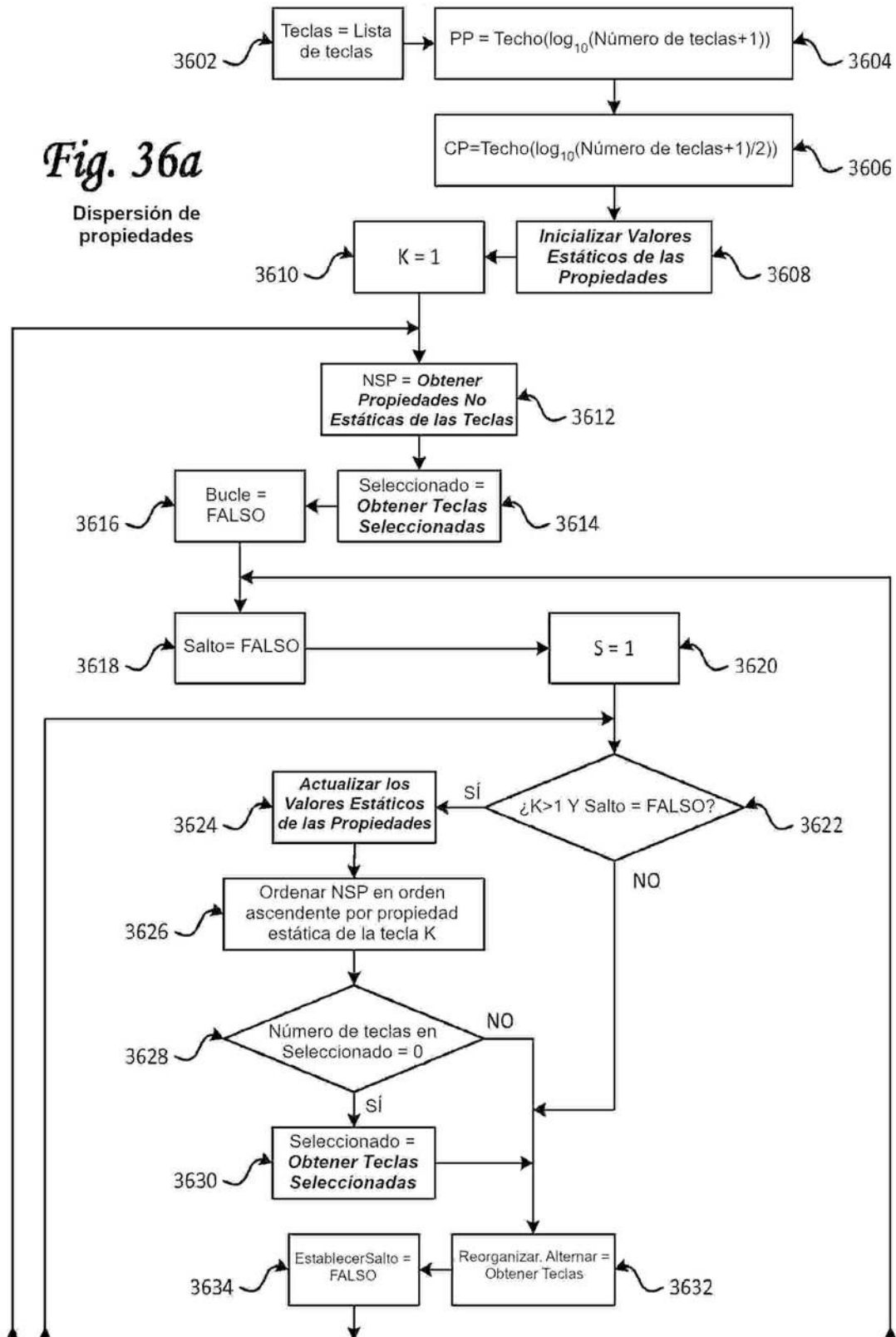


Fig. 366

Dispersión de propiedades

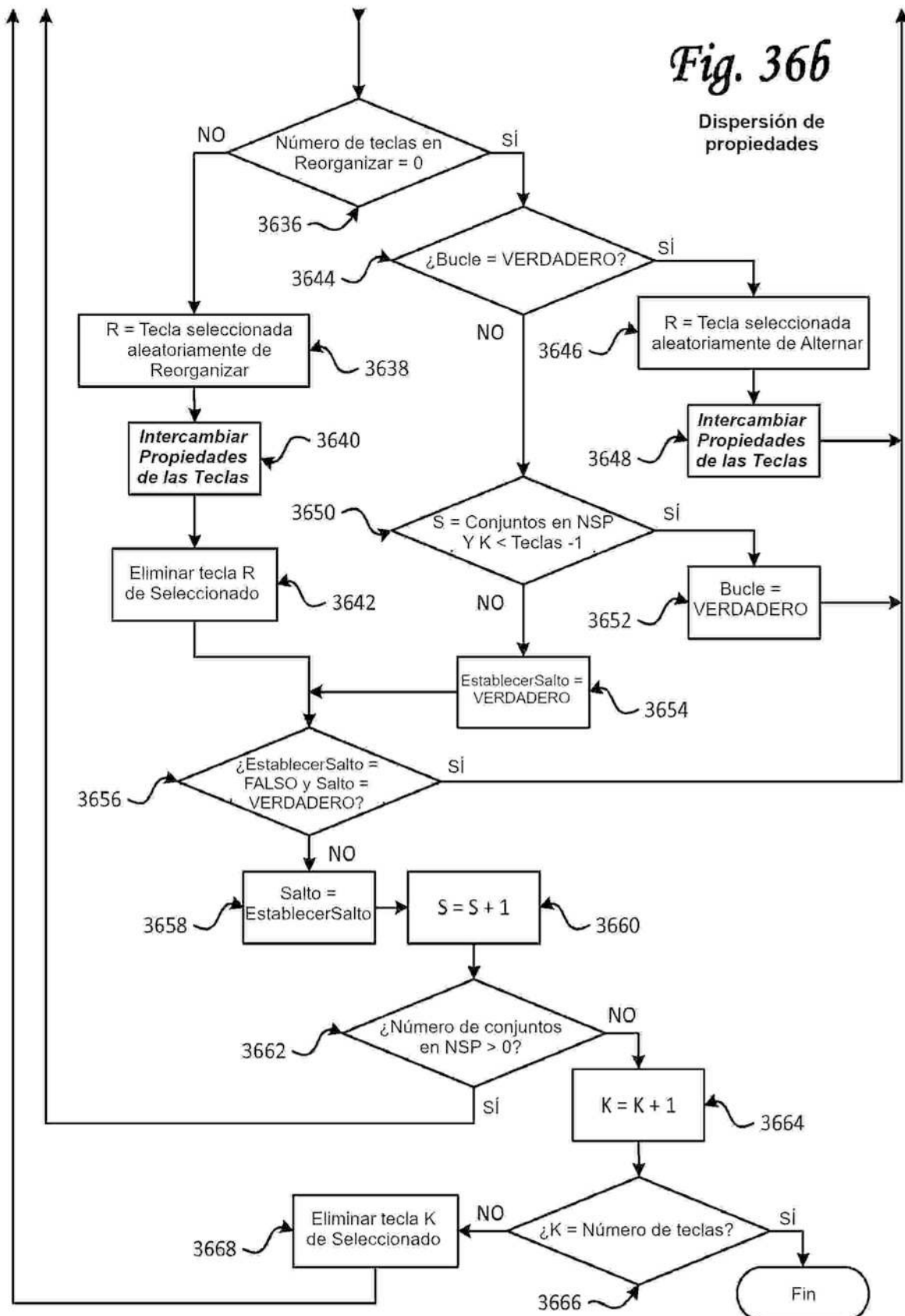
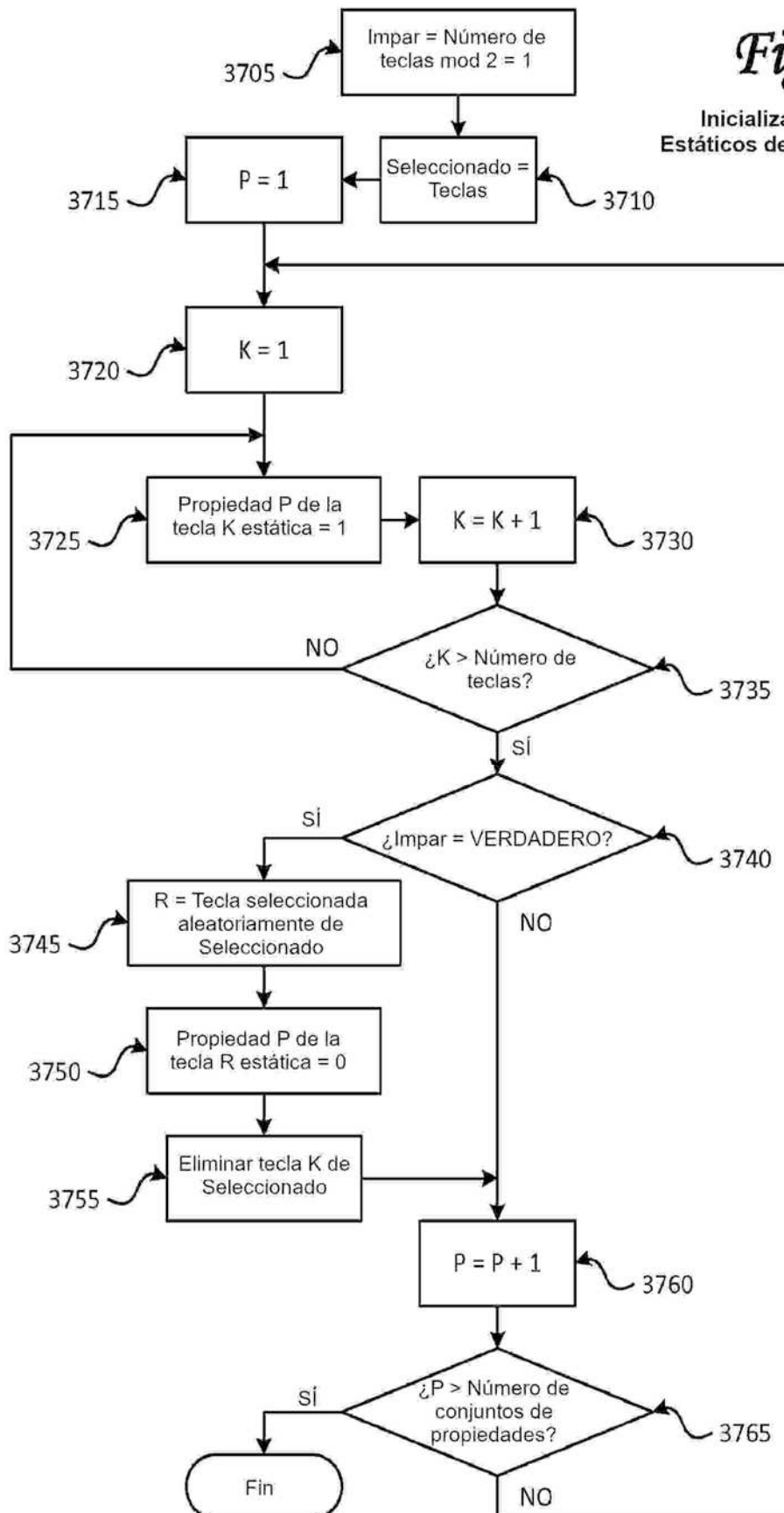
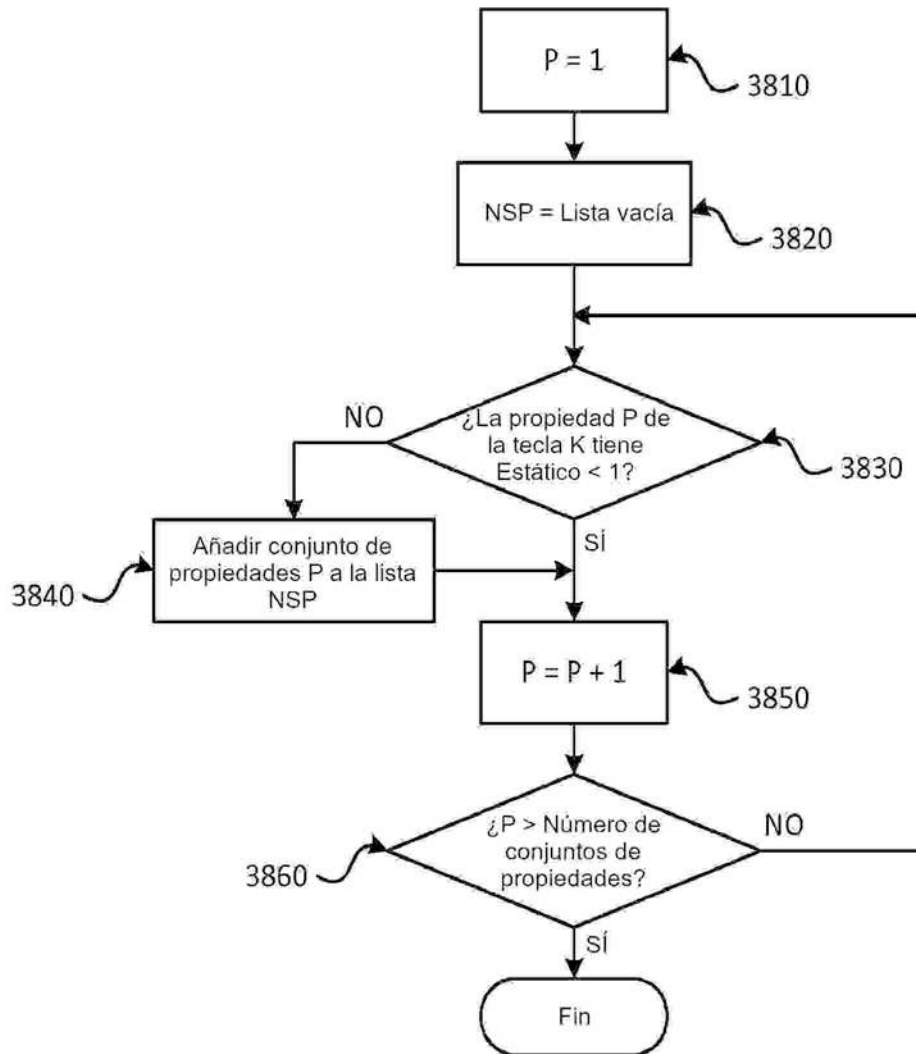
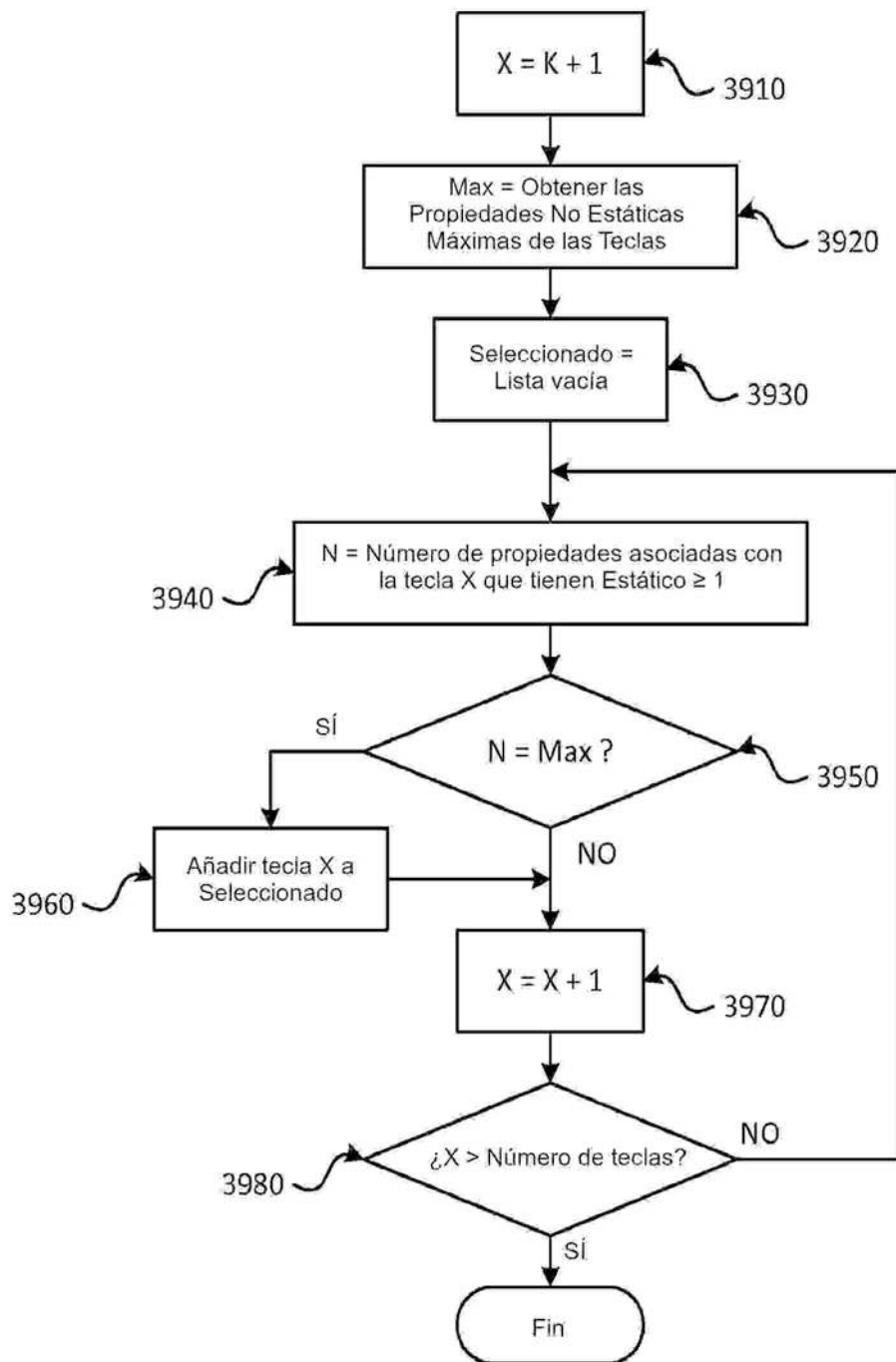


Fig. 37Inicializar los Valores
Estáticos de las Propiedades



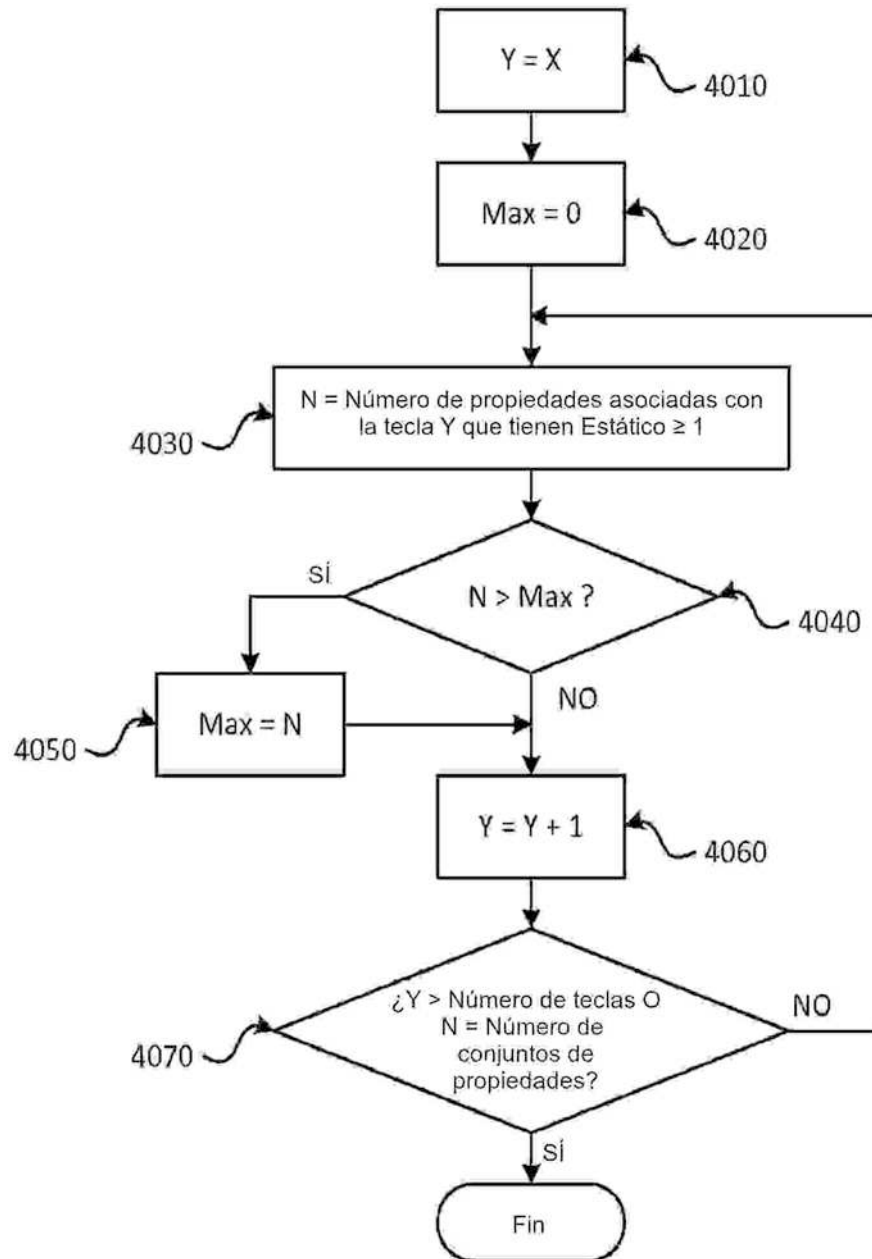
Obtener las Propiedades
No Estáticas de las Teclas

Fig. 38



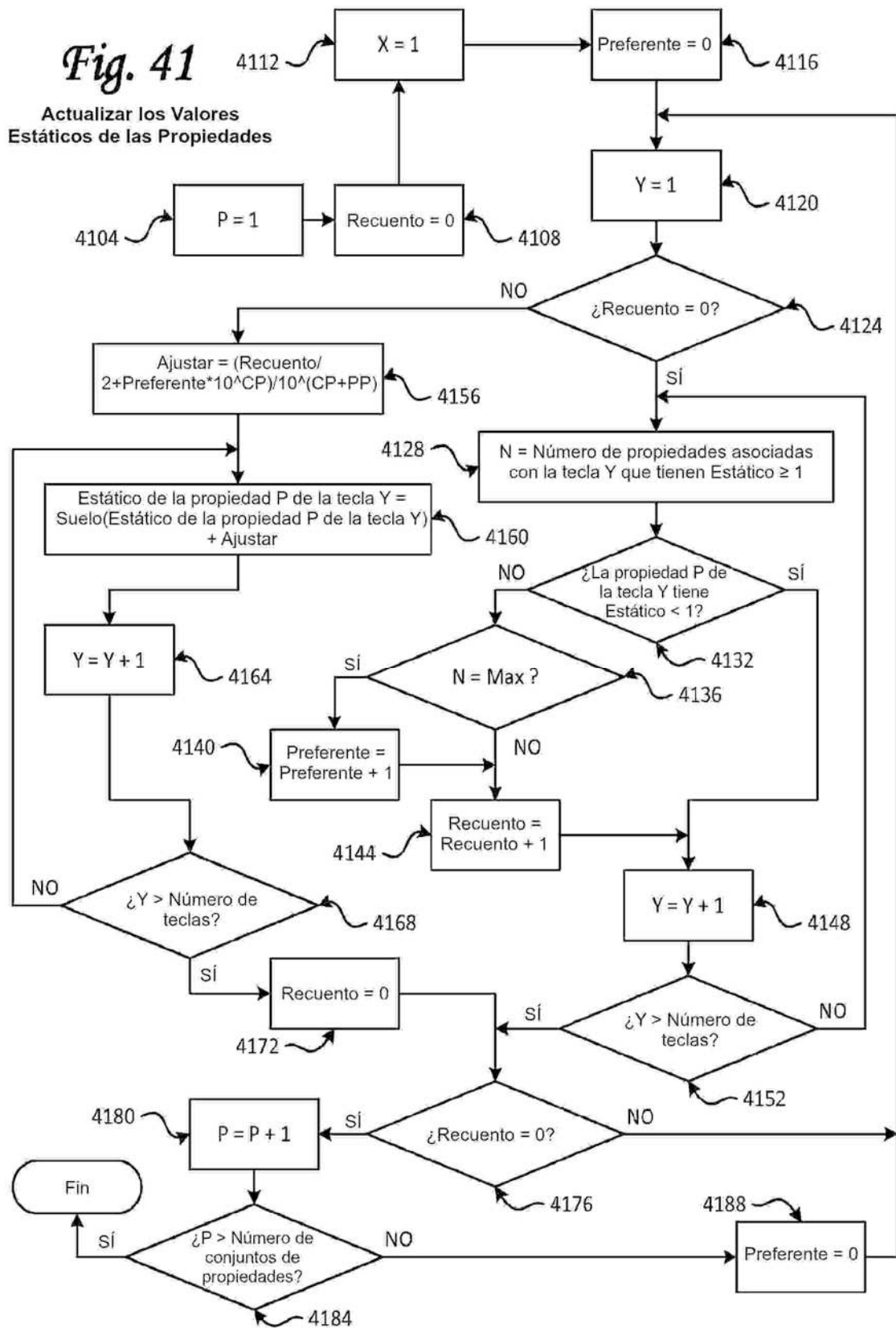
Obtener Teclas Seleccionadas

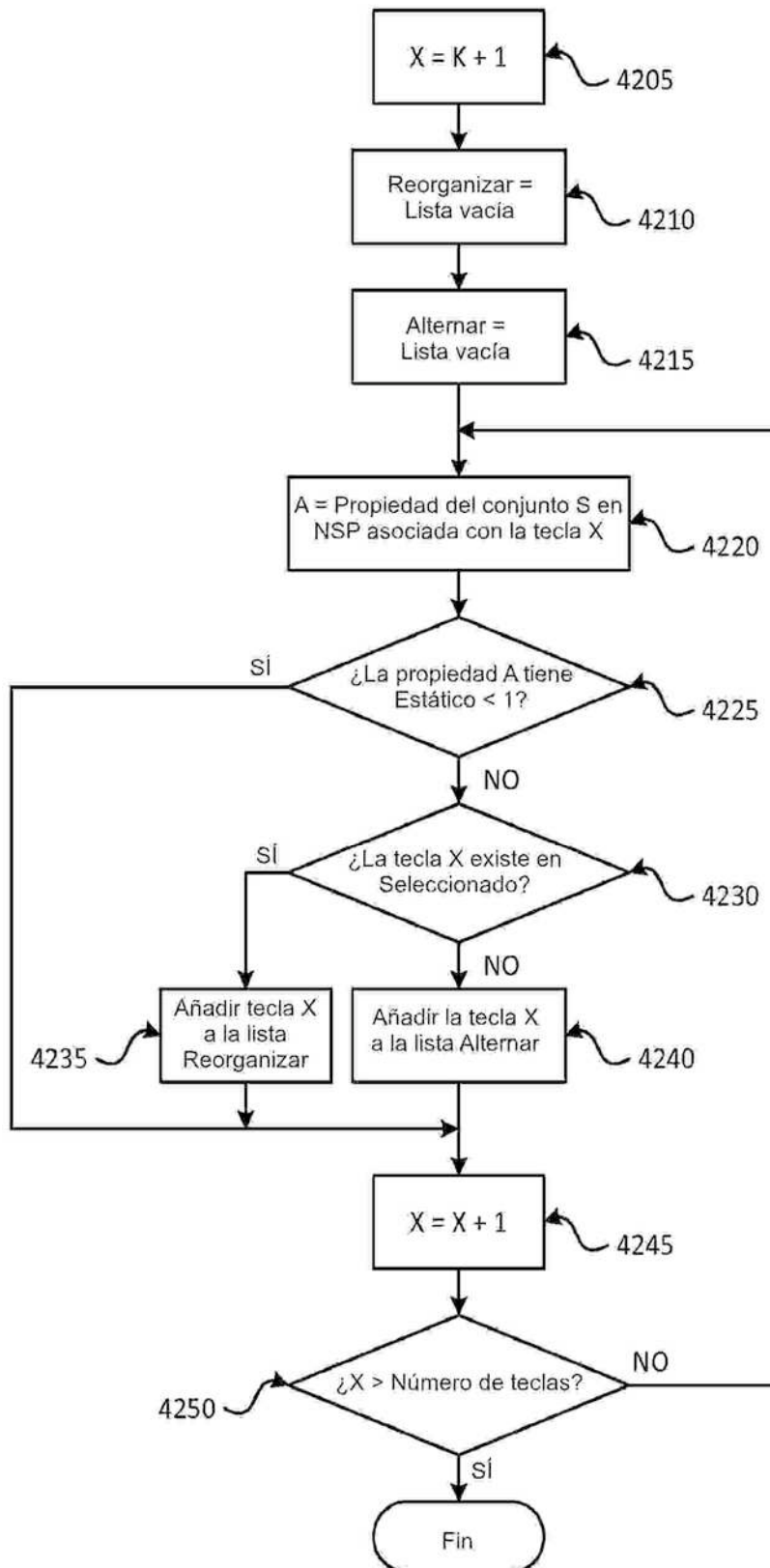
Fig. 39



Obtener las Propiedades No
Estáticas Máximas de las Teclas

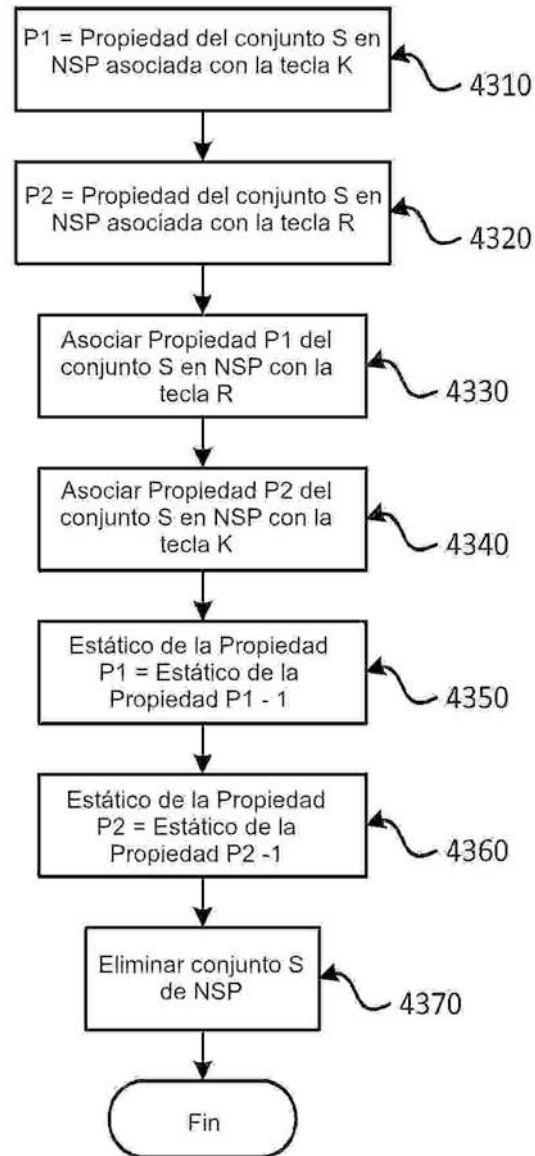
Fig. 40





Obtener Teclas

Fig. 42



Intercambiar las Propiedades de las Teclas

Fig. 43

Nombre del conjunto	Identificador del conjunto (decimal)	Tamaño del conjunto	Tamaño de elemento del conjunto (bytes)	Elementos del conjunto									
				Nombre del elemento									
				Representación en la interfaz de la propiedad									
				Valor de interpretación del sistema en hexadecimal (decimal)									
Forma	1	10	1	Triángulo	Cuadrado	Pentágono	Hexágono	Círculo	Corazón	Trébol	Diamante	Pica	Estrella
	A (10)	B (11)	C (12)	D (13)	E (14)	F (15)	10 (16)	11 (17)	12 (18)	13 (19)			
Número	2	10	1	Uno	Dos	Tres	Cuatro	Cinco	Seis	Siete	Ocho	Nueve	Cero
				1	2	3	4	5	6	7	8	9	0
	14 (20)	15 (21)	16 (22)	17 (23)	18 (24)	19 (25)	1A (26)	1B (27)	1C (28)	1D (29)			
Alfabeto A	3	10	1	A latina	B latina	C latina	D latina	E latina	F latina	G latina	H latina	Arroba	Exclamación
				A	B	C	D	E	F	G	H	@	!
	1E (30)	1F (31)	20 (32)	21 (33)	22 (34)	23 (35)	24 (36)	25 (37)	26 (38)	27 (39)			
Alfabeto I	4	10	1	I latina	J latina	K latina	L latina	M latina	N latina	O latina	P latina	Q latina	Dólar
				I	J	K	L	M	N	O	P	Q	\$
	28 (40)	29 (41)	2A (42)	2B (43)	2C (44)	2D (45)	2E (46)	2F (47)	30 (48)	31 (49)			
Alfabeto R	5	10	1	R latina	S latina	T latina	U latina	V latina	W latina	X latina	Y latina	Z latina	Amperсанд
				R	S	T	U	V	W	X	Y	Z	&
	32 (50)	33 (51)	34 (52)	35 (53)	36 (54)	37 (55)	38 (56)	39 (57)	3A (58)	3B (59)			
Color	6	10	1	Amarillo	Verde	Azul	Naranja	Negro	Púrpura	Marrón	Gris	Rojos	Blanco
	3C (60)	3D (61)	3E (62)	3F (63)	40 (64)	41 (65)	42 (66)	43 (67)	44 (68)	45 (69)			
Posición	7	10	1	0,0	0,1	0,2	1,0	1,1	1,2	2,0	2,1	2,2	3,1
	46 (70)	47 (71)	48 (72)	49 (73)	4A (74)	4B (75)	4C (76)	4D (77)	4E (78)	4F (79)			

Fig. 44

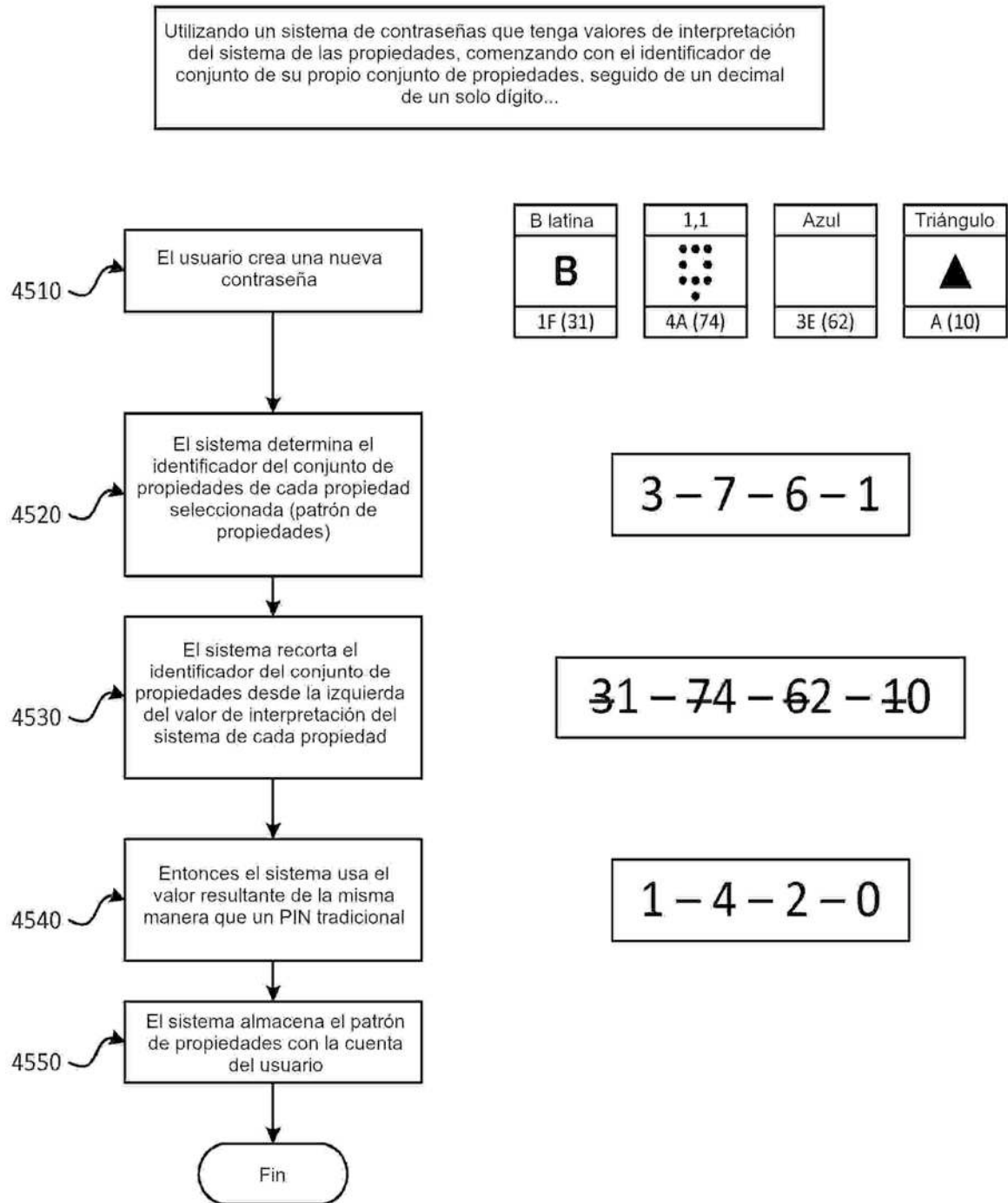
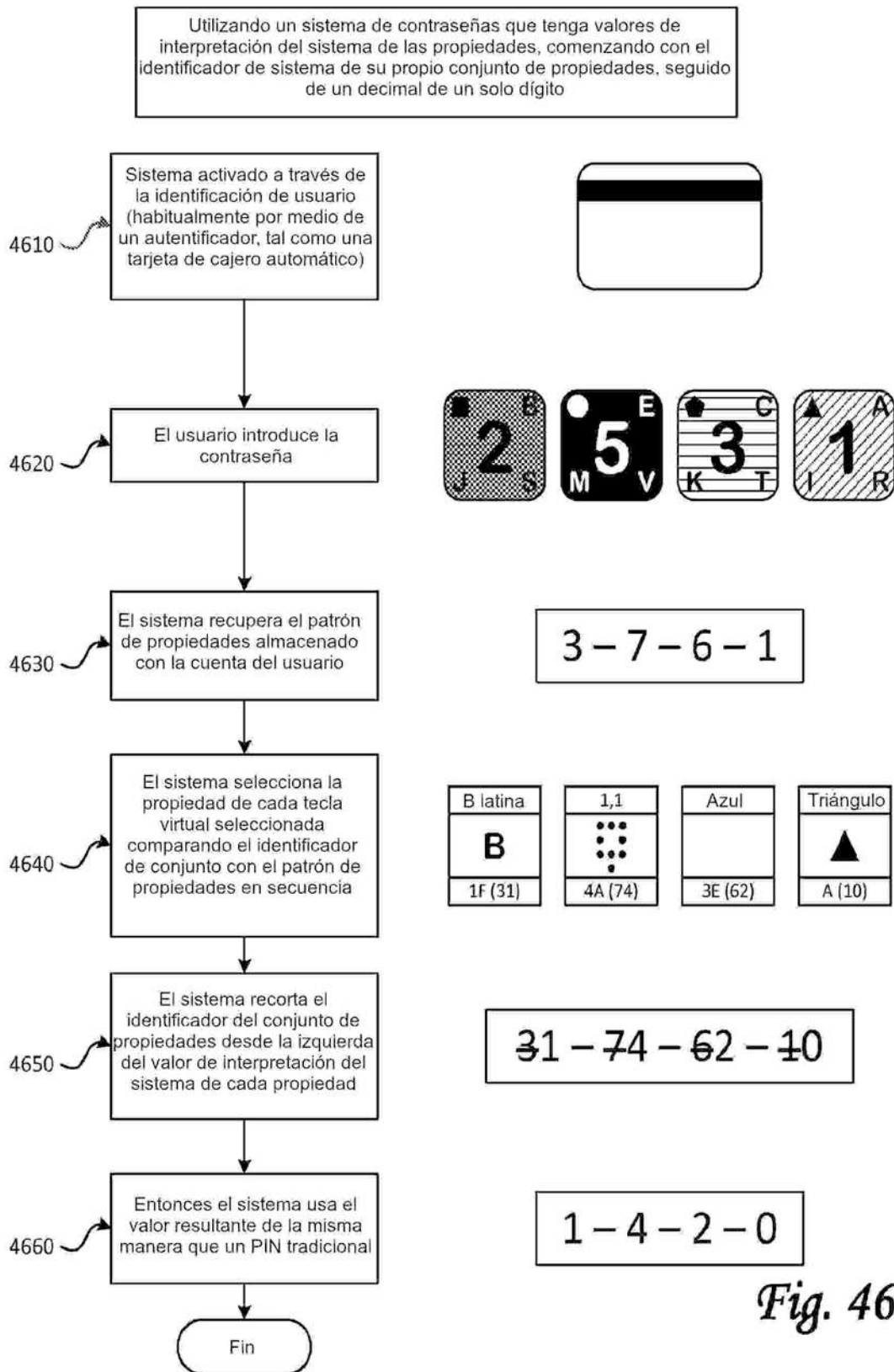


Fig. 45



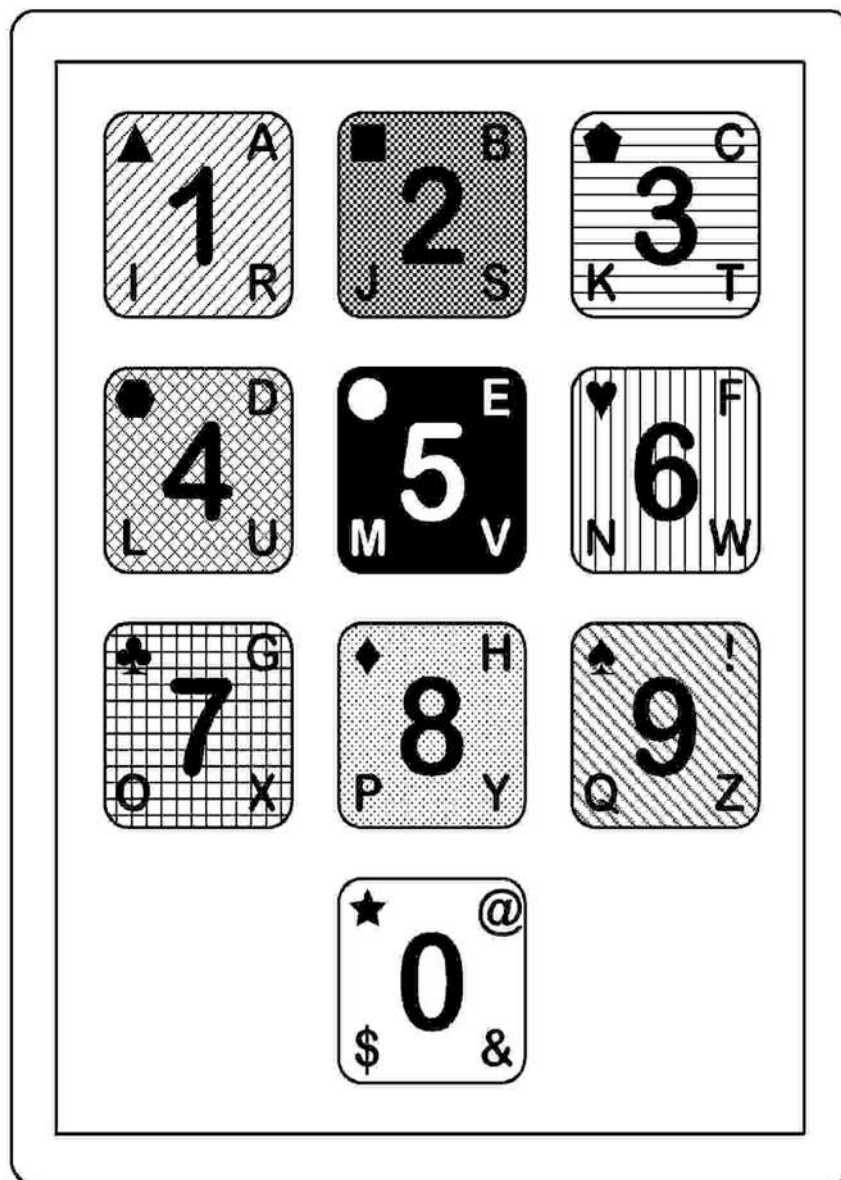


Fig. 47

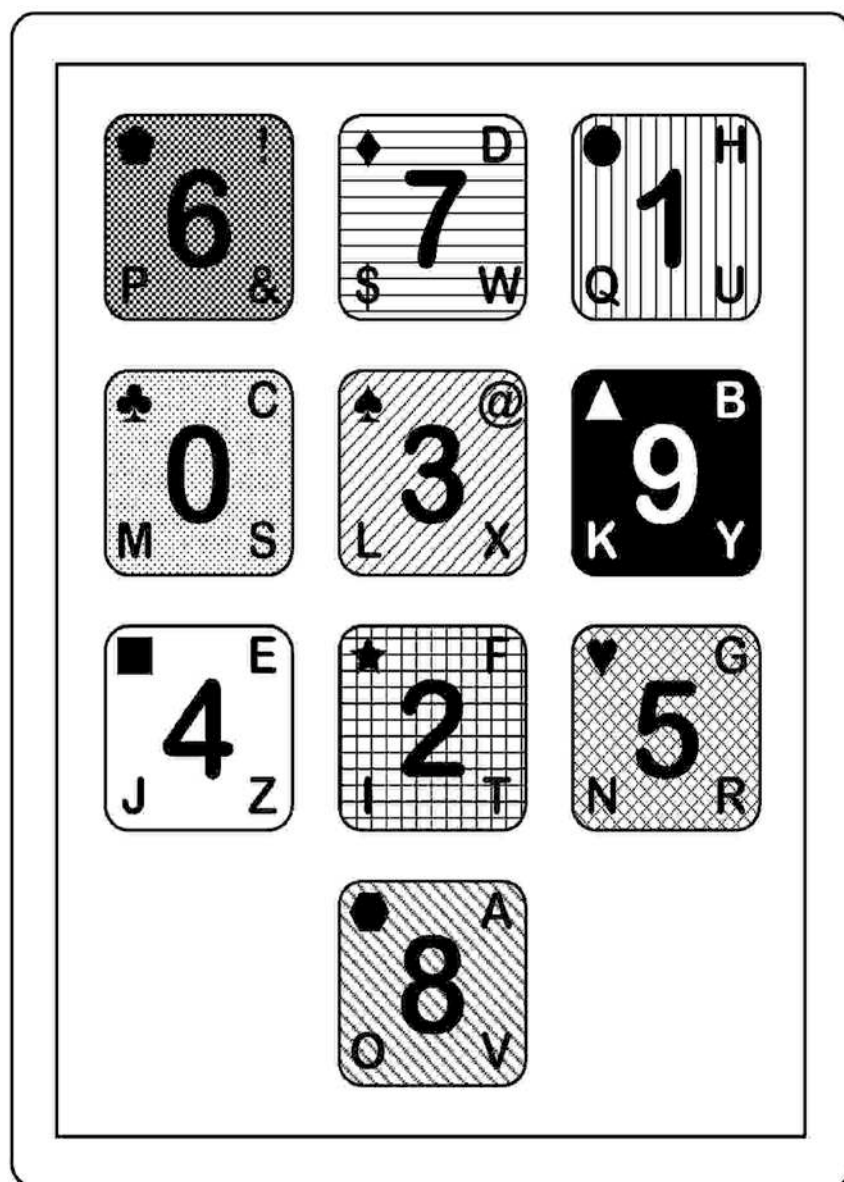


Fig. 48

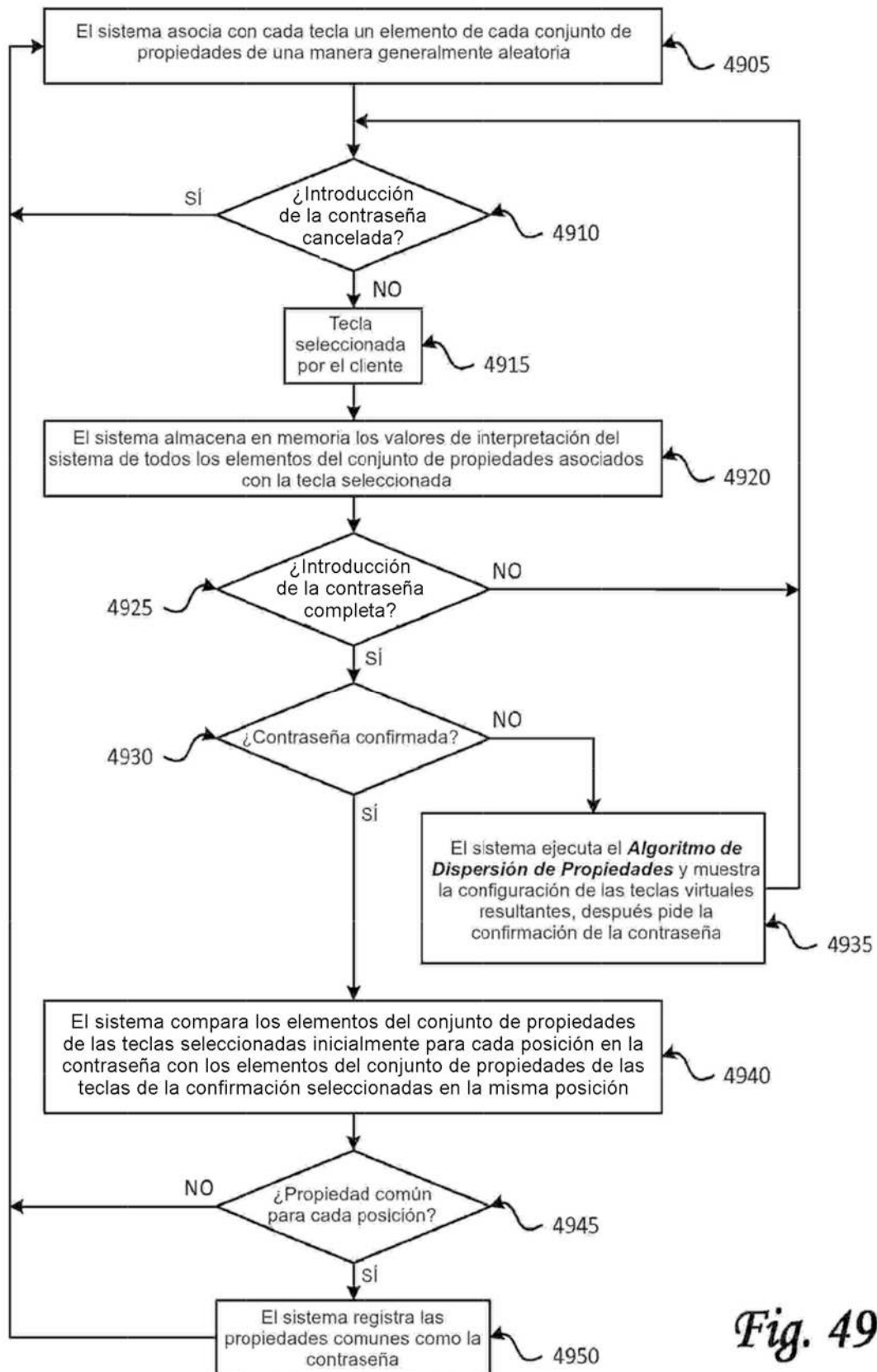


Fig. 49

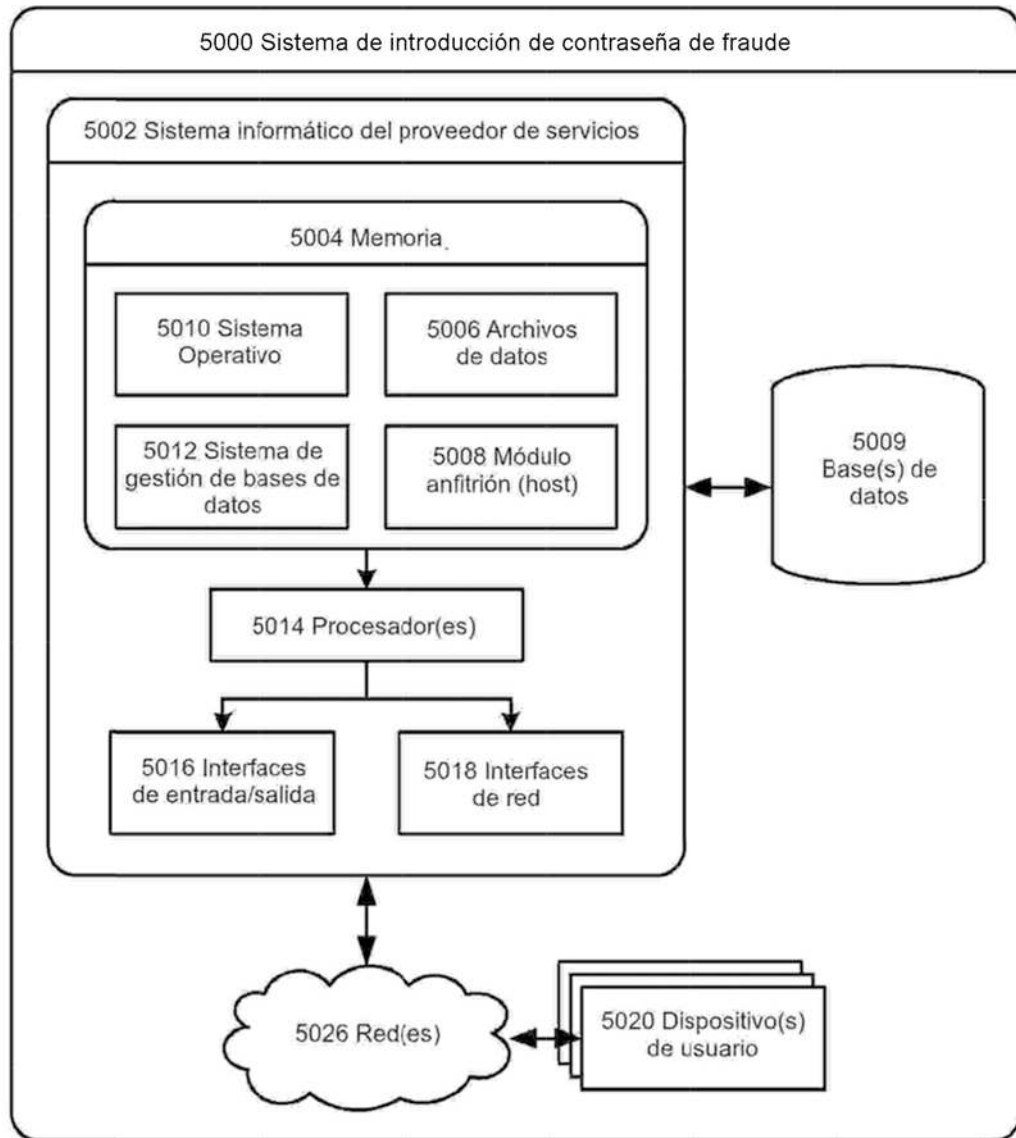


Fig. 50

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

5 *Esta lista de referencias citada por el solicitante es únicamente para mayor comodidad del lector. No forman parte del documento de la Patente Europea. Incluso teniendo en cuenta que la compilación de las referencias se ha efectuado con gran cuidado, los errores u omisiones no pueden descartarse; la EPO se exime de toda responsabilidad al respecto.*

Documentos de patentes citados en la descripción

- 10 • WO 2006064241 A2 • US 2004230843 A1