

SISTEMA Y MÉTODO DE AUTENTICACIÓN MUTUA

DESCRIPCIÓN

Campo de la invención:

- 5 La invención se enmarca, en general, al sector de acceso de seguridad a redes y a computadores; y más concretamente, al sector de los sistemas de autenticación de usuarios humanos frente a máquinas, servidores, o todo tipo de dispositivos electrónicos sin usar aspectos biométricos del usuario, y sin dependencia de objetos o elementos externos.

Antecedentes de la invención:

- 10 Los métodos de autenticación de usuarios humanos implementados por sistemas informáticos o dispositivos electrónicos, en los que un usuario confirma su identidad para poder realizar alguna acción en un sistema generalmente electrónico, se basan principalmente en métodos de identificación por parte del sistema (huella dactilar, imagen facial) y/o en la compartición de secretos entre el usuario y el sistema de autenticación (contraseñas, pines, etc.), siendo por tanto peligroso, entre otras muchas, por dos razones cruciales:

- Respecto a los métodos basados en la identificación, el usuario no muestra necesariamente deseo de autenticación.
- Los secretos son fácilmente copiables y suplantables, y su almacenamiento y gestión son complicados desde un punto de vista de fugas de información.

- 20 Otros sistemas de autenticación, como los basados en dispositivos externos (tokens, llaves criptográficas, generadores de claves de un solo uso, SMS, etc.) requieren de instalaciones complejas, altos costes en dispositivos, y esquemas complejos de autenticación, entre otros.

- La actualidad de los sistemas de autenticación no basados en elementos externos o en biometría está monopolizada por el uso de contraseñas, obligando al usuario a memorizar complicadas secuencias de números, letras y símbolos, que debería ser única para cada servicio que requiere una autenticación. La cantidad de servicios de este tipo que utilizamos diariamente hace que la capacidad del cerebro humano se vea desbordada, y se recurra a gestores de contraseñas (dependencia de elementos externos) o procesos de autenticación centralizados (usar la autenticación de un proveedor para usar otros servicios), prácticas que conllevan una serie de riesgos intrínsecos y problemas de privacidad. Existen algunas alternativas a las contraseñas de los que cabe destacar su usabilidad y atractivo visual, si bien son de uso muy limitado, estando a nivel comercial prácticamente limitados a los patrones de desbloqueo de Android y la elección de puntos determinados en una imagen (concepto introducido por Windows 8 con el nombre de "Picture Password").

La presente invención describe un nuevo sistema de autenticación, basado en una serie de procesos cognitivos conocidos solo por el usuario (capacidades cognitivas de inferencia, reconocimiento, transformación, cálculo y automatización de procesos mentales), de manera que resulta fácilmente adaptable a sistemas electrónicos actuales sin suponer un coste importante, es fácil de usar para el usuario y es resistente a ser copiable o suplantable. Respecto a los métodos de autenticación que utilizan patrones de desbloqueo de Android o la elección de puntos determinados en una imagen, el método de la presente invención consigue alcanzar niveles de usabilidad similares, con niveles de seguridad muy superiores.

El método propuesto utiliza mecanismos cognitivos sencillos, adaptados a cada usuario (en efecto, escogidos por éste dependiendo de sus capacidades y del nivel de seguridad deseado), mecanismos que a su vez sufren un proceso de automatización, lo que hace más rápida y segura la autenticación, dificultando la compartición. También aporta la autenticación consciente (un usuario no puede ser autenticado sin desearlo) y autenticación mutua (el usuario identifica el servicio donde se autentica de manera inequívoca). El método propuesto es superior a los métodos existentes pues es resistente a ataques no solo de observación (un atacante observa al usuario autenticarse) sino que además lo es a ataques de grabación (un atacante consigue grabar varias sesiones de autenticación), y presenta un nivel superior de defensa ante ataques de phishing.

Descripción de la invención:

La presente invención se refiere a un sistema y un método de autenticación mutua. La invención se basa en un mecanismo de autenticación de usuarios humanos frente a dispositivos electrónicos basado en una o varias imágenes, representadas normalmente en una pantalla, donde las imágenes muestran una especie de teclado cuyas teclas o piezas presentan diferentes rasgos gráficos, y donde el usuario a través de una serie de reglas memorizadas es capaz de proporcionar al sistema un resultado correcto que le permite autenticarse.

La naturaleza del proceso (el cálculo del resultado) que debe realizar el usuario en el proceso de autenticación hace que el mecanismo resulte seguro ante ataques no solo de observación, sino incluso de grabación. La naturaleza dinámica del resultado y la gran combinación de posibilidades que presenta permite que el usuario utilice el mismo proceso para varios sistemas sin afectar esto a la seguridad del mismo.

La naturaleza gráfica, y la mecanicidad de los cálculos y los pasos que el usuario ha de realizar hace que por un lado el proceso sea complicado de compartir a un tercero (previniendo comparticiones inseguras) a la vez que, tras un breve entrenamiento, resulte sencillo, rápido y usable para el usuario.

Respecto a otros métodos de autenticación, aporta una seguridad mucho mayor que pines y contraseñas, sin dependencia de elementos externos, ni necesidad de altos costes de

implementación (como por ejemplo los relacionados con biometría, localización, claves de un solo uso). Igualmente, al no requerir ningún dato biométrico, resulta totalmente anónimo, y respetuoso con el tratamiento de datos identificativos.

Al tratarse de una solución horizontal, las posibles aplicaciones son innumerables, pudiendo utilizarse en cualquier escenario donde hoy sea posible el uso de un pin o una contraseña, sin presentar los problemas de seguridad de estas, ya sea en entornos puramente digitales (e.g. PC, dispositivo móvil), físicos (e.g. puerta de entrada de seguridad a un edificio), virtuales (e.g. dentro de un juego de rol) o incluso en entornos mixtos (e.g. gafas de realidad aumentada sobre una superficie táctil o teclado genérico).

La presente invención presenta un procedimiento y un sistema para permitir la autenticación de un usuario en un sistema electrónico (computador, terminal de venta, página web, dispositivo móvil, terminal público, cajero automático, etc.) a través de una interfaz sencilla y utilizando las capacidades cognitivas del usuario como proceso de autenticación. Para ello el sistema de autenticación muestra al usuario una especie de teclado (denominado teclado virtual o cuerpo), de reducidas dimensiones (por ejemplo, una matriz rectangular de 2 por 5 elementos), donde cada uno de los elementos que lo componen (denominados teclas o piezas) presenta varias modificaciones de un conjunto de símbolos o rasgos gráficos con unas diferentes disposiciones y unas reglas conocidas por el usuario.

El usuario observa el teclado virtual y primeramente es capaz de deducir si el teclado es auténtico. A continuación, el usuario elige una secuencia de teclas dependiente de una secuencia de pasos transformadores sobre el teclado virtual mostrado, pudiendo incluir elementos externos en la computación de esta secuencia. El sistema tiene la capacidad de comprobar si la secuencia introducida es la correcta y, por tanto, validar la intención del usuario de autenticarse en el sistema. El sistema puede repetir este proceso a fin de mejorarla estimación de veracidad del usuario, ya sea mostrando un número concreto de iteraciones al comienzo de la autenticación, o pasado un tiempo revalidando así la misma. Un primer aspecto de la presente invención se refiere a un método de autenticación mutua, que comprende los siguientes pasos:

- Obtener una configuración de teclado de un usuario a autenticar, donde la configuración de teclado incluye una pluralidad de rasgos gráficos, una pluralidad de disposiciones o variaciones de los rasgos gráficos, y unas reglas de generación de teclado.
- Generar al menos un teclado virtual, donde cada teclado virtual está formado por una pluralidad de teclas que incorporan una combinación de rasgos gráficos dispuestos en unas determinadas disposiciones, donde los rasgos gráficos y disposiciones utilizados en cada tecla son seleccionados de la configuración de teclado del usuario en base a las reglas de generación de teclado.
- Mostrar al usuario a autenticar el al menos un teclado virtual.
- Recibir una entrada de usuario correspondiente a una selección de teclas de cada teclado virtual. La entrada de usuario se puede esperar recibir en un tiempo máximo determinado

desde que se muestra el al menos un teclado virtual. La selección de teclas de cada teclado virtual puede comprender ninguna, una o varias teclas. Por ejemplo, si se muestran cuatro teclados virtuales la entrada de usuario puede consistir en la selección de una tecla de cada teclado virtual, o en la selección de dos teclas de los teclados virtuales segundo y cuarto.

- 5 - Obtener unas reglas de autenticación del usuario. La configuración de teclado y las reglas de autenticación del usuario pueden estar almacenadas en la misma entidad o dispositivo (e.g. memoria, bases de datos) o en dispositivos/entidades diferentes.
- Aplicar las reglas de autenticación del usuario sobre el al menos un teclado virtual para obtener al menos una secuencia de teclas correcta.
- 10 - Autenticar al usuario si la selección de teclas de la entrada de usuario es validada con respecto a una secuencia de teclas correcta. Un ejemplo de función de validación es la igualdad (en este caso una selección de teclas es validada cuando coincide con una secuencia de teclas correcta), pero también se pueden emplear otras funciones de validación, como puede ser que el hash resultante de concatenar ambas secuencias sea una secuencia determinada.

15 Un segundo aspecto de la presente invención se refiere a un sistema de autenticación mutua, que comprende una serie de elementos configurados para llevar a cabo el método de autenticación mutua. El sistema comprende una unidad de generación de teclado virtual, una interfaz de entrada, una unidad de autenticación y, opcionalmente, un dispositivo de representación de información configurado para mostrar el al menos un teclado virtual y que puede comprender, por ejemplo, una
20 o varias pantallas o un proyector para mostrar los teclados virtuales al usuario.

Un tercer aspecto de la presente invención se refiere a un medio de almacenamiento no transitorio legible por ordenador, que comprende instrucciones de programa almacenadas en el mismo que, cuando se ejecutan en un procesador, causan que el procesador lleve a cabo el método de autenticación mutua.

25 Puesto que los símbolos y reglas son elegidos con anterioridad por el usuario, esto representa una protección contra ataques de suplantación de identidad ("spoofing" y "phishing"). Dado que la combinación de estos símbolos y reglas es muy numerosa, y la selección final del usuario muy concreta (pudiendo ser tan concreta como elegir dos teclas de entre diez disponibles) esto representa una protección contra ataques como grabación, mirar por encima del hombro ("shoulder surfing"),
30 adivinación, etc. Dado que el proceso de generación de los teclados virtuales y de comprobación de la secuencia introducida por el usuario puede estar distribuido entre diferentes sistemas informáticos, y aplicadas técnicas de criptografía, esto representa una protección antes fugas de información, robo de datos, dependencia de terceros, etc. Por último, dado que el cálculo (proceso de inferencia) de la secuencia correcta, por parte del usuario se realiza de forma totalmente mental y utiliza procesos
35 cognitivos como la automatización, esto representa protección frente el robo de secretos, la

divulgación no intencional, resistencia a la coacción, y la prevención de configuraciones inseguras.

La presente invención se puede utilizar en numerosos escenarios donde se requiera un sistema de autenticación y se disponga de alguna capacidad dinámica de generar las gráficas de los teclados virtuales correspondientes, resultado ideal aquellos sistemas electrónicos que contengan pantallas, como pueden ser ordenadores personales, terminales de uso público, cajeros automáticos, etc. Dado el carácter seguro de este mecanismo frente ataques de observación y grabación, no es necesario que la introducción del resultado se realice de forma protegida (por ejemplo, ocultando con una mano la introducción del PIN en un terminal de pago), siendo por tanto ideal para este tipo de entornos.

A diferencia de otros sistemas más complejos técnicamente, la propuesta aquí presentada permite una fácil adopción e integración con soluciones existentes al no requerir desarrollos complejos ni cambios sustanciales en los sistemas para poder ser actualizados. Las medidas esperadas en términos de usabilidad y aceptabilidad por los usuarios permiten poder establecer este método como un nuevo standard sustituyendo a las actuales aplicaciones de PIN y contraseña.

Al introducir un nuevo mecanismo de autenticación, algo que el usuario es capaz de resolver, es posible ser considerado un segundo factor de autenticación efectivo en plataformas como las de pago, acogiendo a los nuevos requerimientos legales, y pudiendo sustituir mecanismos más costosos y complejos como el reconocimiento de voz, o algunas medidas biométricas.

Los sectores de aplicación, al ser un producto horizontal, son prácticamente cualquiera que requiera un nivel de seguridad en la autenticación, entre otros accesos a plataformas digitales de todo tipo, con especial atención a banca, compras, uso de tarjetas de crédito online, etc. Igualmente, al ser fácilmente implementarle en un producto puramente físico los sectores de aplicabilidad se extienden a la seguridad física, como pueden ser acceso a instalaciones de seguridad o edificios (donde hoy en día la autenticación se suele realizar mediante PIN fijos en teclados metálicos o mecanismos similares), uso de tarjetas de crédito, y en definitiva todos aquellos procesos que requiera una autenticación segura.

La presente invención aporta las siguientes ventajas respecto a los métodos del estado del arte:

- El riesgo de exposición de clave, dado que con la cantidad de configuraciones, rasgos gráficos, y disposiciones o variaciones de los rasgos gráficos, resulta casi nulo (muy reducido comparado con otros métodos).
- La posibilidad de selección de estas configuraciones, rasgos gráficos y variaciones entre multitud de posibilidades (que pueden ser incluso diseñadas por el usuario), que de alguna manera se conforma como parte del secreto.
- La posibilidad de incluir elementos de distracción (rasgos que no importan para la resolución, pero que dificultan aún más los análisis por inteligencia artificial o fuerza bruta).

- La capacidad del usuario de elegir todos los elementos confiere una protección anti-phishing importante, dado que solamente los autenticadores/sistemas válidos saben (al tener las instrucciones) crear teclados virtuales correctos que el usuario puede reconocer.
- 5 - La flexibilidad de estas configuraciones podría permitir incluso diferentes formas de “teclados virtuales”; por ejemplo, en forma de reloj, 12 teclas, dispuestas en el perímetro de un círculo, etc.
- El uso de diferentes y múltiples mecanismos cognitivos (capacidades del cerebro humano, no solo saber sumar), y entre ellos, de mecanismos visuales y espaciales (color, desplazamientos), que permite una “automatización” (realizar ciertos pasos muy rápidamente tras un entrenamiento, y sin necesidad de verbalización), lo que permite otro
- 10 aspecto clave de ciberseguridad: aumentar la dificultad de comunicar el secreto.
- Las posibilidades de transformación son numerosas: matemáticas, lógicas, comparaciones de colores, traslación de posiciones, complementariedad de formas. Por tanto, la regla de transformación puede ser algo tan sencillo como una referencia de color y una suma (mucho más sencillo por ejemplo que calcular cuadrados de números), e incluso más seguro (al tener
- 15 una base muy amplia de elecciones y transformaciones posibles)
- Se almacenan (en una parte concreta del sistema) la serie de pasos que el usuario hade reproducir, y así se pueden validar que las resoluciones del usuario y las calculadas por la máquina son la misma. Esto evita el almacenaje de contraseñas, lo cual permite un menor riesgo de fugas.
- La entrada del usuario es suficientemente “sencilla” para que se pueda producir por selección
- 20 directa de la tecla en una pantalla táctil (no necesariamente con un numero asociado), pero también compatible con otros métodos (teclado tradicional, botones físicos, voz, etc.).
- La consecución de selecciones de teclas de cada teclado virtual para formar el resultado final (e.g. dos teclas por teclado virtual) permite niveles de seguridad dinámicos (como si un PIN pudiera tener más o menos dígitos en un supermercado que en un cajero).
- 25 - A su vez, permite incorporar elementos/rasgos gráficos de un teclado virtual en los siguientes, lo que aumenta aún más los niveles de seguridad.
- La no obligatoriedad de ningún elemento externo (e.g. calculadoras como algún método propone para mezclar el secreto con un “nounce” calculado), manteniendo aun así seguridad total contra keyloggers y ataques por grabación múltiple.
- 30 - La posibilidad de mantener una única instancia de las partes críticas (unidad de autenticación, unidad de generación de teclado virtual) para un usuario de forma centralizada, a modo de proveedor de identidad, lo que permite que el resto del sistema no requiera altos niveles de seguridad.
- Permite la delegación del proceso de autenticación a terceros (e.g. entornos no seguros, otra
- 35 página web, en medio de una videoconferencia, pantalla pública), sin riesgos para la seguridad.

Breve descripción de los dibujos:

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta. La **Figura 1** representa un diagrama de flujo de un método de autenticación mutua de acuerdo a una realización de la presente invención. La **Figura 2** representa un sistema de autenticación mutua de acuerdo a una realización concreta de la presente invención.

Las **Figuras 3A-3I** ilustran diferentes implementaciones del sistema de autenticación mutua. Las **Figuras 4A-4M** muestran diferentes ejemplos de teclados virtuales utilizados en el proceso de autenticación. La **Figura 5** muestra un proceso de autenticación que utiliza cuatro teclados virtuales.

Descripción detallada de la invención:

La **Figura 1** muestra un diagrama de flujo de un método de autenticación mutua 100 de acuerdo a una realización de la presente invención. El método de autenticación mutua 100 comprende las siguientes etapas:

- Obtener 110 una configuración de teclado 112 de un usuario a autenticar. La configuración de teclado 112 incluye una pluralidad de rasgos gráficos 114, una pluralidad de disposiciones 116 de los rasgos gráficos 114, y unas reglas de generación de teclado 118.
- Generar 120 al menos un teclado virtual. Cada teclado virtual está formado por una pluralidad de teclas que incorporan una combinación de rasgos gráficos 114 dispuestos en unas determinadas disposiciones 116. Los rasgos gráficos 114 y disposiciones 116 utilizados en cada tecla son seleccionados de la configuración de teclado 112 del usuario en base a las reglas de generación de teclado 118.
- Mostrar 130 el al menos un teclado virtual al usuario a autenticar. Los teclados virtuales se representan preferentemente en una o varias pantallas, ya sea total o parcialmente (por ejemplo, si los teclados virtuales se muestran en una única pantalla de tamaño reducido, e.g. la pantalla de un reloj inteligente, el usuario puede desplazarse por la pantalla para poder ver diferentes partes de un teclado virtual o diferentes teclados virtuales). Alternativamente, los teclados virtuales se pueden mostrar impresos en papel, proyectados en una superficie mediante un proyector, o en cualquier otro medio de representación de información a un usuario.
- Recibir 140 una primera entrada de usuario 142 correspondiente a una selección de teclas 144 de cada teclado virtual realizada por el usuario a autenticar. Opcionalmente, representado en líneas discontinuas, este proceso puede ser iterativo para de esta forma generar 120 y mostrar 130 sucesivamente varios teclados virtuales (e.g. cinco teclados virtuales generados y mostrados de uno en uno) y recibir 140 la primera entrada de usuario 142 correspondiente a cada iteración, donde en cada iteración se puede opcionalmente también obtener 110 la

configuración de teclado 112 del usuario. Mediante estas iteraciones se permite que los teclados virtuales que se vayan mostrando puedan depender de entradas anteriores; por ejemplo, cada teclado virtual puede tener dos selecciones de teclas, donde la primera selección (primera entrada de usuario 142 con selección de teclas) se usa para calcular la solución y la segunda selección (segunda entrada de usuario 106) se utiliza para configurar el siguiente teclado, de forma que si por ejemplo en la segunda selección se elige rojo, el siguiente teclado generado tiene que tener rojo en la primera tecla. La etapa de obtener 104 la segunda entrada de usuario 106 se puede realizar, alternativamente, inmediatamente antes o después de recibir la entrada de usuario 140. Esto refuerza la autenticación mutua, de forma que el usuario puede elegir (mediante la segunda entrada de usuario 106) alguna característica que se combina o se incorpora a las reglas de generación del teclado 118 para que así el usuario pueda comprobar la veracidad del sistema de autenticación.

- Obtener 150 unas reglas de autenticación 152 del usuario.
- Aplicar 160 las reglas de autenticación 152 del usuario sobre el al menos un teclado virtual para obtener al menos una secuencia de teclas correcta 162.
- Autenticar 170 al usuario si la selección de teclas 144 de la primera entrada de usuario 142 es validada con respecto a una secuencia de teclas correcta 162. Por ejemplo, tal y como se muestra en la realización de la **Figura 1**, la selección de teclas 144 puede ser validada si coincide con una secuencia de teclas correcta 162.

El orden en que se realizan algunas de las etapas puede variar con respecto al orden representado en el diagrama de flujo de la **Figura 1**. Así, por ejemplo, la etapa 150 de obtención de reglas de autenticación del usuario puede realizarse antes, simultáneamente o después de la etapa 110 de obtención de configuración de teclado del usuario. Por ejemplo, si la configuración de teclado del usuario 112 y las reglas de autenticación del usuario 152 se encuentran almacenadas en un mismo dispositivo de almacenamiento de datos, ambos datos se pueden recuperar simultáneamente al acceder a dicho dispositivo de almacenamiento de datos. También, la etapa 160 de aplicar las reglas de autenticación 152 del usuario sobre el al menos un teclado virtual se puede realizar antes, simultáneamente o después de la etapa 130 de mostrar el al menos un teclado virtual en pantalla.

El método de autenticación mutua 100 puede opcionalmente comprender cualquiera de las siguientes etapas mostradas en línea discontinua:

- Una etapa inicial de obtener 102 una identificación del usuario a autenticar, previa a la etapa de obtener 110 la configuración de teclado 112 del usuario.
- Obtener 104 una segunda entrada de usuario 106, de forma que al menos uno de los teclados virtuales 212 se genera en base a las reglas de generación de teclado 118 y utilizando dicha segunda entrada de usuario 106. Por ejemplo, las reglas de generación de teclado 118

pueden especificar que el teclado virtual generado tiene que incluir una letra seleccionada por el usuario en la segunda tecla, y donde la segunda entrada de usuario 106 puede incluir la selección de dicha letra; de esta forma, si el usuario selecciona por ejemplo la letra “B” como segunda entrada de usuario 106, el teclado generado debe incluir la letra “B” en la segunda tecla. Si no lo incluye, el usuario puede ya saber que el sistema de autenticación no es legítimo. La segunda entrada de usuario 106 se puede aportar en cualquier parte del proceso, una o varias veces (e.g. de manera iterativa), para emplearla en la generación de cualquier teclado virtual. Por ejemplo, se podría aportar junto con la identificación del usuario (o en un momento anterior o posterior) para tenerlo en cuenta en la etapa de generar teclados virtuales 120. O se puede aportar de forma iterativa, en cada iteración (líneas discontinuas) en la que se generan sucesivamente diferentes teclados virtuales; en este caso la segunda entrada de usuario 106 puede corresponder a una selección de teclas de uno o varios teclados virtuales (en el ejemplo anterior, el usuario seleccionaría una tecla que incorpore la letra “B”) que se empleará para la generación de los teclados virtuales de cada sucesiva iteración.

- Mostrar 130 o representar al usuario a autenticar el al menos un teclado virtual (e.g. en una o varias pantallas).

En la **Figura 2** se representa un sistema de autenticación mutua 200 de acuerdo a una realización de la presente invención. El sistema de autenticación mutua 200 comprende una unidad de generación de teclado virtual 210, una interfaz de entrada 230 y unidad de autenticación 240.

En una realización, el sistema de autenticación mutua 200 comprende además un dispositivo de representación de información, que puede comprender por ejemplo al menos una pantalla 220.

La unidad de generación de teclado virtual 210 está configurada para obtener la configuración de teclado 112 de un usuario 201 a autenticar y generar al menos un teclado virtual 212, según se ha descrito en las etapas 110 y 120 de la **Figura 1**.

La al menos una pantalla 220 está configurada para mostrar, según se describe en la etapa 130 de la **Figura 1**, el al menos un teclado virtual 212, donde cada teclado virtual 212 está formado por una pluralidad de teclas 214. En el ejemplo de la **Figura 2** el sistema de autenticación mutua 200 emplea una única pantalla en la que se representan dos teclados virtuales. Sin embargo, el sistema de autenticación mutua 200 puede incluir un número cualquiera de pantallas 220, y a su vez cada pantalla 220 puede mostrar cualquier número (de 1 a n) de teclados virtuales 212.

La interfaz de entrada 230 está configurada para recibir una primera entrada de usuario 142 correspondiente a una selección de teclas 144 de cada teclado virtual 212 realizada por el usuario 201, según se describe en la etapa 140 de la **Figura 1**. En una realización la pantalla 220 (o pantallas) puede ser una pantalla táctil, y la interfaz de entrada 230 comprendería dicha pantalla

táctil, donde la selección de teclas 144 se realiza mediante la pulsación en la pantalla 220 táctil, por parte del usuario 201, en teclas 214 seleccionadas de cada teclado virtual 212 representado, con el objeto de autenticarse ante el sistema. En otras realizaciones, la interfaz de entrada puede comprender un teclado físico para la introducción de la selección de teclas, un micrófono con un software de reconocimiento de voz para introducir la selección del usuario mediante voz, o en general cualquier tipo de interfaz que permita recibir una selección de teclas 144 por parte del usuario 201.

La selección de teclas 144 del usuario puede ser realizada de múltiples formas: por selección directa sobre las propias teclas o sobre elementos afines (e.g. teclas de un teclado físico que representan alguna característica de las mismas, como la letra, el dígito o el color), por eliminación de teclas, por reordenación de teclas, por fusión/combinación de teclas, u otros procesos a través de los cuales el resultado es una secuencia de teclas o valores de alguna característica determinada en un orden específico. También se puede seleccionar teclas utilizando otro tipo de interfaces, como por ejemplo utilizando gestos (e.g. señalando a las teclas seleccionadas, las cuales se identifican mediante una cámara de reconocimiento de imágenes), una interfaz sonora (por reconocimiento de voz, a través del cual el usuario emite verbalmente su selección de teclas 144), entre otras interfaces.

En función de la configuración de las reglas de autenticación 152, puede ser necesario que el usuario seleccione una, dos o más teclas 214 de cada teclado virtual 212 mostrado en pantalla 220. Por ejemplo, el usuario 201 puede pulsar las teclas '2' y '8' (esto es, las teclas en las que aparecen los números 2 y 8) del teclado virtual 212 superior y las teclas '5' y '0' del teclado virtual 212 superior (esto es, se deben seleccionar dos teclas 214 de cada teclado virtual 212). En función de las reglas de autenticación 152 seguidas, el orden de selección de las teclas 214 puede ser tenido en cuenta para la autenticación. En este caso no sería lo mismo seleccionar en el teclado virtual 212 superior primero la tecla '2' y luego la tecla '8' que al revés, primero la tecla '8' y luego la tecla '2'.

La unidad de autenticación 240 está configurada para ejecutar las etapas relativas a la autenticación del usuario, una vez recibida la selección de teclas 144 del usuario 201 (etapas 150, 160 y 170 de la **Figura 1**). En particular, la unidad de autenticación 240 obtiene unas reglas de autenticación 152 del usuario 201 y aplica dichas reglas de autenticación 152 del usuario 201 sobre el al menos un teclado virtual 212 generado por la unidad de generación de teclado virtual 210, obteniendo de esta forma al menos una secuencia de teclas correcta 162. Finalmente, autentica al usuario 201 si la selección de teclas 144 de la primera entrada de usuario 142 es validada con respecto a una secuencia de teclas correcta 162 (por ejemplo, si la primera entrada del usuario 142 coincide exactamente con una secuencia de teclas correcta 162). En el caso de que la selección de teclas 144 no sea correctamente validada (por ejemplo, si la selección de teclas 144 no coincide con ninguna secuencia de teclas correcta 162), el usuario 201 no es autenticado (de forma similar a no introducir el pin correcto que se esperaba del usuario). En definitiva, la unidad de autenticación 240 se encarga de emitir un resultado de la

autenticación 242, el cual puede ser positivo (autenticación correcta) o negativo (autenticación fallida).

El sistema de autenticación mutua 200 puede comprender una unidad de identificación de usuario 202 configurada para obtener 102 una identificación 204 del usuario 201 a autenticar. Por ejemplo, la identificación 204 puede incluir introducir, por parte del usuario 201 mediante un teclado, un nombre de usuario y/o una contraseña con la que el sistema de autenticación mutua 200 pueda identificar al usuario 201. La identificación 204 del usuario 201 es recibida por la unidad de identificación de usuario 202, la cual a su vez la transmite a la unidad de generación de teclado virtual 210 y a la unidad de autenticación 240.

La unidad de generación de teclado virtual 210 puede estar configurada para obtener la configuración de teclado 112 del usuario 201, una vez convenientemente identificado, mediante el acceso a una base de datos 211 externa (e.g. en un servidor remoto) o una memoria 213 interna (una memoria o medio de almacenamiento de datos que forma parte del sistema de autenticación mutua 200), con el objeto de obtener la configuración de teclado 112 del usuario identificado. La base de datos 211 o memoria 213 puede incluir múltiples configuraciones de teclado 112, correspondientes a diferentes usuarios. De esta forma, la identificación del usuario permite acceder al registro adecuado de la base de datos o memoria 213, correspondiente al usuario que ha sido identificado.

La unidad de autenticación 240 puede estar configurada para obtener las reglas de autenticación 152 del usuario 201, una vez identificado, mediante el acceso a una base de datos 241 externa (e.g. en un servidor remoto) o una memoria 243 interna al sistema (e.g. una memoria flash, un disco duro, o cualquier otro medio de almacenamiento de datos). El medio de almacenamiento de datos empleado para almacenar la configuración de teclado 112 (e.g. base de datos 211 o memoria 213) puede ser el mismo medio de almacenamiento en el que se almacenan las reglas de autenticación 152. Por ejemplo, la configuración de teclado 112 y las reglas de autenticación 152 de múltiples usuarios pueden estar almacenadas en una única memoria o base de datos, ya sea externa al sistema (e.g. situada en un servidor remoto) o interna al mismo.

Los elementos que componen el sistema pueden formar parte de un mismo dispositivo electrónico o pueden estar distribuidos en diferentes dispositivos electrónicos. En el primer caso, el sistema de autenticación mutua 200 se puede implementar en cualquier dispositivo electrónico que incluya una interfaz de entrada 230, una unidad de control o procesador con capacidad para procesar datos (e.g. un portátil, un ordenador, una tableta electrónica, un teléfono inteligente, un procesador integrado en cualquier circuito electrónico, etc.) y, opcionalmente, una pantalla 220 (o cualquier otro soporte físico o virtual donde se represente a un usuario a autenticar la sucesión de teclados). De esta forma, diferentes componentes del sistema (como la unidad de identificación de usuario 202, la unidad de generación de teclado virtual 210 y la unidad de autenticación 240) pueden ser unidades lógicas que están incorporadas dentro de un procesador o controlador del dispositivo electrónico.

Por ejemplo, tal y como se muestra en la **Figura 3A**, el sistema de autenticación mutua 200 se puede implementar en un ordenador 310, el cual incluye un monitor 312 (con función de pantalla 220), un teclado 314 y/o ratón (con función de interfaz de entrada 230), un procesador (con función de unidad de identificación de usuario 202, unidad de generación de teclado virtual 210 y unidad de autenticación 240), y un disco duro donde se almacenan la configuración de teclado 112 y las reglas de autenticación 152 del usuario 201 (y, opcionalmente, de otros usuarios). Alternativamente, la configuración de teclado 112 y las reglas de autenticación 152 pueden estar almacenadas en un medio de almacenamiento remoto, como una base de datos de un servidor externo, a la cual accede el ordenador mediante una unidad de comunicación, ya sea alámbrica o inalámbrica.

En la **Figura 3B** se muestra un ejemplo en el que el sistema de autenticación mutua 200 está implementado en un teléfono inteligente 320. En este caso la pantalla táctil 322 del teléfono inteligente 304 tiene la función de pantalla 220 y de interfaz de entrada 230. En este caso el resultado de la autenticación 242 que obtiene el sistema de autenticación mutua 200 puede emplearse, por ejemplo, para desbloquear el teléfono o en general para cualquier operación realizada en el teléfono inteligente en la que se requiera una autenticación del usuario 201.

El sistema de autenticación mutua 200 se puede implementar en otros muchos dispositivos electrónicos, como por ejemplo en un reloj inteligente 323 para autenticar operaciones del usuario (**Figura 3C**); en un cajero automático 324 para sacar dinero en efectivo (**Figura 3D**); en un terminal punto de venta para pagos con tarjeta (**Figura 3E**); o en un sistema de control de acceso 326 para acceder a espacios públicos/privados (**Figura 3F**) o para la apertura de armarios o taquillas (e.g. en un gimnasio).

Los dispositivos electrónicos (310, 320, 323, 324, 325) mostrados en las **Figuras 3A-3E** comprenden una pantalla 220 para mostrar el teclado virtual 212 (o teclados virtuales).

Sin embargo, el dispositivo electrónico representado en la **Figura 3F**, sistema de control de acceso 326, no dispone de una pantalla 220. En este caso el teclado virtual 212 (o los teclados virtuales, en caso de que haya varios) se muestra impreso, por ejemplo en una hoja 327 de cartulina o papel. La unidad de generación de teclado virtual 210 del sistema de autenticación mutua 200 genera el teclado virtual 212, el cual se imprime en una hoja 327 utilizando una impresora y se dispone adyacente al sistema de control de acceso 326 o a la puerta 328 controlada por el mismo, por ejemplo pegada a la pared. Ese teclado virtual 212 marcará una o varias secuencias de teclas correctas 162 que debe introducir el usuario, utilizando la interfaz de entrada 230 (e.g. un teclado), para poder abrir la puerta 328. Este teclado virtual 327 se podría reemplazar periódicamente, por ejemplo cada día o cada ciertas horas se podría imprimir una nueva instancia de teclado virtual 327 para dificultar ataques de observación de terceros. En esta realización el sistema de autenticación mutua 200 se podría implementar fácilmente en sistemas de control de acceso 326 ya existentes, los cuales no dispongan de pantalla 220.

La unidad de autenticación 240 puede estar configurada para obtener una pluralidad de secuencias de teclas correctas 162 mediante la aplicación de las reglas de autenticación 152 del usuario 201 sobre el al menos un teclado virtual 212.

En el caso de que haya una pluralidad de secuencias de teclas correctas 162, cada secuencia de teclas correcta 162 puede estar asociada a una identidad diferente, esto es, a un usuario diferente. De esta forma la unidad de autenticación 240 puede estar configurada para identificar al usuario entre un conjunto de usuarios, en función de la secuencia de teclas correcta 162 que haya introducido el usuario como su selección de teclas 144.

En el ejemplo de la **Figura 3F** cada usuario podría tener asociado unas reglas de autenticación 152 diferentes, de forma que aplicando las reglas de autenticación 152 de los diferentes usuarios sobre el mismo teclado virtual se llegaría a secuencias de teclas correctas 162 diferentes. De esta forma la secuencia de teclas correcta 162 concreta que haya introducido el usuario no sólo serviría para autenticar al usuario y abrir la puerta, sino también para identificarle de entre un grupo de usuarios. Así, suponiendo por ejemplo que la secuencia de teclas correcta 162 para el usuario 1 sean las teclas {5, 2, 8}, y para el usuario 2 sean las teclas {7, 3, 1}, cuando un usuario no autorizado vaya a autenticarse ante el sistema de control de acceso 326 no sabrá qué teclas debe seleccionar porque desconocerá las reglas de autenticación 152 a aplicar, con lo que el sistema no le permitirá el acceso. Si un usuario autorizado introduce las teclas {7, 3, 1}, el sistema de autenticación mutua 200 abrirá la puerta 328 porque la selección de teclas 144 es validada con respecto a una de las secuencias de teclas correctas 162, en concreto con respecto a la secuencia de teclas correcta 162 que corresponde al usuario 2. Y, además, el sistema será capaz de identificar a qué usuario ha dado acceso, en este caso al usuario 2. Esta doble funcionalidad de autenticación e identificación puede ser muy útil por ejemplo para controlar los accesos de trabajadores a un área de trabajo (e.g. un laboratorio), donde la autenticación garantizaría que el usuario es un trabajador autorizado para el acceso a la estancia, y la identificación permitiría identificar el usuario concreto al que se le ha dado acceso.

El tener una pluralidad de secuencias de teclas correctas 162 puede emplearse también para que la unidad de autenticación 240 autentique al usuario 201 según diferentes niveles de autenticación, en función de la secuencia de teclas correcta 162 con respecto a la que la selección de teclas 144 es validada. Por ejemplo, un primer nivel de autenticación puede ser “autenticación correcta” y un segundo nivel de autenticación puede ser “autenticación con alarma”. La autenticación con diferentes niveles puede ser útil en situaciones que se requiera conocer aspectos adicionales a la propia autenticación, como por ejemplo si existe una situación peligrosa o de alarma. Así, un cajero puede habilitar el acceso a la caja mediante un primer nivel de autenticación (una primera secuencia de teclas correcta 162), o habilitar el acceso a la caja mediante un segundo nivel de autenticación (una segunda secuencia de teclas correcta 162), donde el primer nivel de autenticación implica una

autenticación correcta y el segundo nivel de autenticación implica una autenticación con alarma, la cual podría ser empleada cuando el usuario está amenazado.

En el ejemplo representado en la **Figura 3G** el sistema de autenticación mutua 200 se implementa en un dispositivo electrónico 329 que comprende una pluralidad de pantallas 220 en las que se representa un teclado virtual 212. En concreto, en cada pantalla 220 se representa una tecla 214 del teclado virtual 212. Las teclas 214, ordenadas en una matriz de 3 filas y 3 columnas, componen el teclado virtual 212. Las pantallas 220 del dispositivo electrónico 329 son táctiles, haciendo por tanto las funciones de interfaz de entrada 230. El usuario realiza la selección de teclas 144 interactuando (e.g. mediante pulsación) con la propia pantalla 220 en las que se representan las teclas 214, minimizando de esta forma los componentes hardware requeridos para la autenticación.

En los ejemplos mostrados en las **Figura 3A-3G** los elementos del sistema de autenticación mutua 200 pueden formar parte de un único dispositivo electrónico. Sin embargo, los elementos del sistema de autenticación mutua 200 pueden estar distribuidos en diferentes entidades o dispositivos electrónicos. Por ejemplo, tal y como se representa en la **Figura 3H**, el sistema de autenticación mutua puede incluir un dispositivo cliente 330 y entidades externas al dispositivo cliente 330 (e.g. uno o más servidores), conectadas por ejemplo a través de Internet. El dispositivo cliente 330 es el dispositivo electrónico o entidad que quiere realizar una autenticación de un usuario 202, como por ejemplo un ordenador o un teléfono inteligente (la autenticación puede ser requerida por una aplicación operando en el dispositivo electrónico). De acuerdo al ejemplo de la **Figura 3H**, el dispositivo cliente 330 recibe la identificación del usuario 204 y solicita a un servidor de generación de teclado virtual 340 (que tiene las funciones de la unidad de generación de teclado virtual 210) la generación de al menos un teclado virtual 212. Cuando lo recibe, el dispositivo cliente 330 lo muestra en una pantalla 220 (e.g. en la pantalla del dispositivo donde está operando la aplicación web). A continuación, una vez el dispositivo cliente 330 ha recibido del usuario 201 la selección de teclas 144, el dispositivo cliente 330 solicita la autenticación del usuario 201 a un servidor de autenticación 350, enviándole para ello el al menos un teclado virtual 212 generado, la identificación del usuario 204 y la selección de teclas 144. El servidor de autenticación 350 (que tiene las funciones de la unidad de autenticación 240) envía al dispositivo cliente 330 el resultado de la autenticación 242. El dispositivo cliente 330 actuará en función del resultado de la autenticación 242, e.g. bloqueando el acceso al usuario en el caso de autenticación fallida.

De esta forma el dispositivo cliente 330 ha realizado una autenticación del usuario sin tener almacenada localmente información del usuario 201 que pueda ser comprometida. Dicha información (e.g. las reglas de generación de teclado o las reglas de autenticación 152 determinadas para el usuario 201) están almacenadas de forma segura en los servidores remotos 340 y 350. Así, la autenticación se ha realizado de forma segura, sin posible robo de la información comprometida

del usuario 201 aunque el dispositivo cliente 330 sea objeto de un ataque. En otras posibles realizaciones el sistema se puede implementar en un número mayor o menor de entidades o dispositivos. Por ejemplo, la pantalla 220 puede estar ubicada externa al dispositivo cliente 330, en otro dispositivo. En otro ejemplo, el dispositivo cliente 330 se puede comunicar con un único servidor, el cual tiene las funciones de generación de teclado virtual y de autenticación (esto es, el servidor de generación de teclado virtual 340 y el servidor de autenticación 350 pueden ser la misma entidad).

Las funciones de la unidad de autenticación 240 pueden estar distribuidas en varios dispositivos, por ejemplo un primer dispositivo que se encarga de aplicar las reglas de autenticación para obtener la secuencia de teclas correcta y un segundo dispositivo que se encarga de validar la selección de teclas con respecto a la secuencia de teclas correcta para autenticar al usuario. Así, en el ejemplo de la **Figura 3I** (muy similar al de la **Figura 3H**), el dispositivo cliente 330 puede enviar al servidor de autenticación la identificación 204 del usuario a autenticar y el teclado virtual 212, pero sin enviar la selección de teclas 144 del usuario. El dispositivo cliente 330 recibe la secuencia de teclas correcta 162 generada por el servidor de autenticación 350, y valida la selección de teclas 144 con respecto a la secuencia de teclas correcta 162 para autenticar al usuario 201.

A continuación, se muestran varios ejemplos que ilustran varios teclados virtuales generados, empleando diferentes rasgos gráficos 114, disposiciones 116 y reglas de generación de teclado 118. El proceso de autenticación está basado en una o varias imágenes (teclado virtual 212) representada en una o varias pantallas 220, donde cada imagen ilustra un número de piezas (teclas 214) parecidas pero diferentes en cuanto a sus características visuales, donde cada una de ellas muestra diferentes rasgos gráficos con los cuales el usuario 201 puede establecer unas reglas para llegar a un resultado, el cual es introducido por el usuario 201 utilizando la misma pantalla (en el caso de que sea táctil), un teclado u otro sistema de introducción de datos dispuesto para ello.

En la **Figura 4A** se representa, a modo de ejemplo, un teclado virtual 212 formado por un conjunto de diez teclas 214, si bien un teclado virtual 212 puede estar compuesto por un número N (siendo $N \geq 2$) cualquiera de teclas 214. En este ejemplo las teclas 214 están agrupadas en una matriz rectangular de dos filas y cinco columnas. Las teclas 214 pueden sin embargo agruparse de múltiples formas (e.g. una distribución circular, una distribución rectangular, una distribución libre), según se haya determinado en las reglas de generación de teclado 118 de la configuración de teclado 112 del usuario 201 correspondiente. En este ejemplo las teclas 214 podrían disponerse por ejemplo en círculo, en una matriz de 5 filas y 2 columnas, o cualquier otra disposición que se considere apropiada.

Cada tecla 214 se configura según una combinación de rasgos gráficos 114 y disposiciones 116 de los mismos. En el ejemplo de la **Figura 4A** se consideran los siguientes rasgos gráficos 114 y disposiciones 116:

- Rasgos gráficos:

~ Números 402 (0 a 9).

~ Vocales 404 (a, e, i, o, u).

~ Consonantes 406 (b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, z).

5 ~ Colores (cinco colores: rojo, azul, verde, amarillo, negro). El color azul de los rasgos gráficos se representa con rayado inclinado hacia abajo-derecha (e.g. números 2 y 7), el color amarillo se ilustra con un rayado inclinado hacia arriba derecha (e.g. números 1 y 6), el color rojo mediante rayado vertical, el color negro mediante rayado horizontal, y el color verde mediante un relleno punteado.

10 - Cada tecla 214 puede tener dos diferentes disposiciones 116 de los rasgos gráficos 114:

~ Número a la izquierda, ocupando toda la altura de la tecla y $\frac{2}{3}$ de la anchura, dejando el tercio derecho dispuesto en tres huecos de un tercio de altura situados verticalmente donde se colocan tres letras de determinada forma (1 vocal arriba y 2 consonantes debajo).

~ Número a la derecha, mismas proporciones, y los tres huecos a la izquierda.

15 Algunos rasgos gráficos pueden incluir subrasgos o características (tales como tamaño y color) de los rasgos gráficos. De esta forma, un rasgo gráfico 114 puede estar formado por un rasgo principal, el cual define la forma del rasgo gráfico 114, y un rasgo secundario o subrasgo, que define una característica del rasgo principal, como por ejemplo el tamaño o el color del rasgo principal. Así, en el ejemplo de la **Figura 4A**, el rasgo principal “9” tiene como rasgo secundario el color negro. En el caso de que el rasgo principal “9” pudiera representarse en la tecla 214 con varios tamaños diferentes, cada uno de dichos posibles tamaños sería un rasgo secundario del rasgo principal.

20

Las disposiciones 116 se pueden considerar de manera individual a nivel de rasgo gráfico 114. Así, en lugar de considerar dos disposiciones de tecla diferentes en el ejemplo de la **Figura 4A**, se puede considerar que cada rasgo gráfico 114 puede tener varias disposiciones diferentes:

25 - Los números 402 tienen dos posibles disposiciones en la tecla 214, a la derecha o a la izquierda de la tecla 214.

- Las vocales 404 tienen dos posibles disposiciones en la tecla 214, arriba a la derecha o arriba a la izquierda de la tecla 214.

30 - Las consonantes 406 tienen cuatro posibles disposiciones en la tecla 214, medio-derecha, medio-izquierda, abajo-derecha, abajo-izquierda de la tecla 214.

En las **Figuras 4B-4M** se muestran a modo de ejemplo otros posibles teclados virtuales 212.

El teclado virtual 212 de la **Figura 4B** se compone de 10 teclas 214, agrupadas en dos filas y cinco columnas. Cada tecla 214 está formada por un número 402 y dos letras 408 (vocales o consonantes). El número 402 ocupa toda la altura de la tecla y la mitad de la anchura, dejando el

lado derecho dispuesto en dos huecos de mitad de altura situados verticalmente donde se colocan dos letras 408.

En la **Figura 4C** se representa un teclado virtual 212 formado por una pluralidad de teclas 214. Cada tecla 214 incluye varios rasgos gráficos 114: un elemento numérico 412 incluido en un rectángulo de un determinado color (e.g. un “7” con fondo verde, representado con un rayado punteado), cuatro bordes 414 (representados por rectángulos) y cuatro vértices 416 (representados por unos pequeños cuadrados). El elemento numérico 412 se dispone en una determinada disposición 116 dentro de la tecla 214 (e.g. disposición centrada, disposición esquina superior izquierda, disposición lateral izquierda), de entre múltiples disposiciones posibles. Los bordes 414 y vértices 416 también pueden tener múltiples disposiciones, tal y como se aprecia en la **Figura 4C**, donde la disposición puede incluir la rotación del rasgo gráfico 114 (por ejemplo, dos bordes 414 aparecen en disposición horizontal y dos bordes 414 aparecen representados en disposición vertical, girados 90°). Además, los bordes 414 y vértices 416 pueden adoptar diferentes colores como rasgos secundarios. En este ejemplo, y teniendo en cuenta que las figuras se muestran en blanco y negro, el color rojo se representa con un rayado inclinado hacia arriba-derecha, el color amarillo con un rayado inclinado hacia abajo-derecha, el color cian con un rayado horizontal, y el color azul con un rayado vertical.

En el teclado virtual 212 de la **Figura 4D** las teclas 214 incluyen dos elementos numéricos 412 (un “7” y un “3”, cada uno con un tamaño diferente y con un fondo de un color diferente), dos elementos textuales 418 (las letras “A” y “Z”, con un fondo de un color determinado), y dos rectángulos 420. Los elementos numéricos 412 dispuestos en cualquiera de las esquinas, suponiendo por tanto doce configuraciones diferentes (ya solo considerando los elementos numéricos 412). A su vez, los rectángulos 420 y elementos textuales 418 pueden tener múltiples disposiciones dentro de la tecla, lo cual incrementa el número de posibles combinaciones de rasgos gráficos 114 para generar una tecla 214. En las disposiciones de los rectángulos 420 también se considera el giro (un rectángulo aparece horizontalmente dispuesto y el otro rectángulo aparece vertical).

En el ejemplo de la **Figura 4E** el teclado virtual 212 se compone de diez teclas 214 dispuestas en dos filas y cinco columnas. Cada tecla 214 incorpora un borde 422 rectangular de color blanco y un elemento numérico 402 incluido en un rectángulo con fondo negro (rasgo gráfico principal), el cual puede adquirir diferentes rasgos secundarios: uno de cinco colores posibles en parejas par-impar, y uno de dos tamaños disponibles (también según color). Los números 402 pueden adoptar diferentes disposiciones respecto al borde 422 (e.g. centrado, en una esquina, en un lateral). De esta forma existen multitud de combinaciones de rasgos gráficos 114 (incluyendo rasgos principales y secundarios) y de disposiciones 116 para generar un teclado virtual 212.

El teclado virtual 212 de la **Figura 4F** se compone de cuatro teclas 214 dispuestas en fila. Cada tecla 214 incluye un elemento central compuesto por un número 402 (en el ejemplo se muestra el número

“7”) y tres letras 408 (“A”, “J” y “X”, en el ejemplo), dispuestas de manera similar a la primera tecla 214 del teclado virtual 212 del ejemplo de la **Figura 4A**. El elemento central se puede situar de diez maneras diferentes respecto a un conjunto de bordes 424 (rectángulos dispuestos horizontal o verticalmente en los laterales de la tecla 214) y vértices 426 (pequeños cuadrados en las esquinas).

5 En el ejemplo se muestra el elemento central cubriendo los bordes (primera tecla); en la esquina arriba-izquierda, dejando los bordes abajo y a la derecha (segunda tecla); arriba centrado, dejando los bordes laterales en lugares opuestos y ambos bordes horizontales en el lado inferior (tercera tecla); y situado de forma central (cuarta tecla). De esta manera resultan diez variaciones identificables para este tipo de disposición del elemento central respecto a los bordes 424 y vértices 426.

10 En la **Figura 4G** se muestra un ejemplo monocromo de un teclado virtual 212 donde los rasgos gráficos 114 de cada tecla 214 incluyen un número 402, una vocal 404 y dos consonantes 406, de forma similar al ejemplo de la **Figura 4A** pero en este caso en negro, sin incluir por tanto color como rasgo secundario. Los rasgos gráficos 114 también incluyen cuatro bordes laterales 430 rectangulares (dispuestos en cada lateral de la tecla 214) y cuatro vértices 432 cuadrados (dispuestos

15 en cada esquina de la tecla 214), los cuales sí incluyen al color como rasgo secundario, ya que cada uno de los bordes laterales 430 y de los vértices 432 pueden estar rellenos de color blanco o de color negro, lo cual aumenta el número posible de combinaciones de rasgos gráficos y disposiciones. Los números 402 y letras (404, 406) se pueden disponer a izquierda o derecha. Cada tecla 214 del teclado virtual 212 emplea un número 402 diferente. En el teclado virtual 212 se emplean cinco

20 vocales 404 diferenciables en parejas según la disposición derecha/izquierda, y veinte consonantes 406. Por tanto, el número de posibles combinaciones de rasgos gráficos 114 y disposiciones 116 para formar el teclado virtual 212 es enorme.

En la **Figura 4H** se muestra otro ejemplo de teclado virtual 212 basado en el teclado de la **Figura 4G**, pero incluyendo cinco colores como rasgos secundarios para cada rasgo gráfico (número 402, vocal 404, consonante 406, borde lateral 430 y vértice 432). Los rasgos gráficos 114 están coloreados de manera independiente: los bordes laterales 430 y los vértices 432 o esquinas según la fila (superior/inferior) y el número 402 y las vocales 404 según la disposición derecha/izquierda. Los números y letras, así como sus respectivos colores, coinciden con los mostrados en la **Figura 4A**. En este ejemplo las consonantes se encuentran coloreadas aleatoriamente sin ser considerado

25 un rasgo característico, dato que un posible atacante desconoce y que haría más complejo un intento de análisis. Una disposición adicional se incluye en este teclado virtual 212: la localización del elemento principal formado por el número 402 y las tres letras (404, 406) respecto a unos bordes finos 434 que lo separan de los bordes laterales 430 principales de colores, con diez posibles variaciones en la disposición, lo cual incrementa aún más el número total de combinaciones rasgos gráficos 114 y disposiciones 116 disponibles.

30

35

La **Figura 4I** representa el ejemplo anterior de la **Figura 4H** pero ampliado el número de colores a diez, aumentando el número total de combinaciones rasgos gráficos 114 y disposiciones 116 disponibles. Como hay diez teclas y diez colores, los colores de un mismo rasgo gráfico 114 no se repiten en el teclado virtual 212 (con la excepción de las consonantes 406, donde el color se elige aleatoriamente). La **Figura 4J** muestra el mismo ejemplo de la **Figura 4H** pero con fondo de color negro, donde los números y letras, y sus respectivos colores, coinciden con los mostrados en la **Figura 4A**. Utilizar un fondo de color blanco (**Figura 4H**) o un fondo de color negro (**Figura 4J**) puede ser otro rasgo gráfico (rasgo secundario) a considerar en la generación del teclado virtual 212, lo cual podría realizarse en función de un elemento externo (como por ejemplo considerando el día par o impar de la fecha actual), lo que permitiría añadir una seguridad adicional contra el spoofing y el phishing. Por ejemplo, si al usuario 201 se le muestra un teclado virtual 212 con fondo de color negro y sin embargo el usuario 201, conocedor de las reglas de generación de teclado 118, sabe que por ser día par se le tendría que representar el teclado virtual 212 con fondo de color blanco, el usuario es capaz de detectar que el teclado virtual 212 es incorrecto y ha podido haber algún ataque contra la seguridad en el proceso de autenticación.

En los ejemplos de las **Figuras 4A-4J** se utiliza una configuración relativamente simple para el teclado virtual 212; sin embargo, las configuraciones de los teclados virtuales 212 pueden ser más complejas (por ejemplo, 24 teclas 214 dispuestas en cuatro filas y seis columnas). En las **Figuras 4K-4M** se ilustran otros posibles teclados virtuales 212 con diferentes configuraciones y rasgos gráficos.

Como se puede observar en las diferentes realizaciones de teclados virtuales 212, se pueden emplear una gran variedad de rasgos gráficos 114. Los rasgos gráficos pueden comprender, por ejemplo, cualquiera de los siguientes elementos: un número 402, una vocal 404, una consonante 406, bordes laterales 430, vértices 432, bordes finos 434, diferentes símbolos (e.g. círculo, estrella, triángulo, palos de una baraja, etc.), colores, fuentes de letras, grafismos realizados por el usuario, y patrones de relleno, entre otros.

Por tanto, y volviendo a la **Figura 2**, en el proceso de autenticación el sistema de autenticación mutua 200 genera un teclado virtual 212 (o teclados virtuales) en base a una configuración previa, de acuerdo a unas reglas de generación de teclado 118. El sistema de autenticación mutua 200 por un lado computa un resultado que se considera correcto (secuencia de teclas correcta 162) de acuerdo a unas reglas de autenticación 152, y por otro lado muestra en pantalla 220 al usuario 201 el teclado virtual 212 (o teclados virtuales) generado para que el usuario 201 pueda computar su propio resultado y seleccionar las teclas 214 oportunas (selección de teclas 144). Finalmente, el sistema de autenticación mutua 200 comprueba si la selección de teclas 144 del usuario es validada con respecto a una secuencia de teclas correcta 162 para autenticar al usuario (e.g. en el caso de que

coincidan) o no autenticarle (e.g. en caso de que no coincidan).

Los teclados virtuales 212 se generan mediante una combinación de rasgos gráficos 114 y disposiciones de los mismos en cada tecla 214, de acuerdo a las reglas de generación de teclado 118 previamente fijadas. La configuración de teclado 112 de un usuario 201 sede termina previamente, en una etapa de configuración de teclado en la que puede intervenir el propio usuario 201 o se puede realizar de manera automática por un sistema informático. El proceso de configuración, específico para un usuario 201, se lleva a cabo a través de la selección de los rasgos gráficos 114 y disposiciones 116, de forma que cada tecla 214 resultado la variación de un número determinado de rasgos gráficos 114 y disposiciones 116 de los rasgos gráficos, de modo que las probabilidades estadísticas se mantienen constantes, evitando así ataques por análisis de probabilidad.

En el proceso de configuración los rasgos gráficos 114 se seleccionan de entre un conjunto de rasgos gráficos disponibles (que pueden incluir rasgos principales relativos a la forma y rasgos secundarios, como tamaño y color). En dicha selección puede intervenir el usuario. Alternativamente, la selección puede ser realizada de manera automática, e.g. aleatoriamente. Para cada rasgo gráfico se pueden seleccionar varios rasgos secundarios, como por ejemplo dos posibles tamaños o cinco posibles colores. Algunos rasgos gráficos pueden venir definidos únicamente por un rasgo principal, sin tener rasgos secundarios. Los rasgos gráficos 114 pueden incluir, entre otras múltiples opciones: otros elementos gráficos como símbolos en lugar de letras o números, diferentes fuentes de letra o tamaños, formas geométricas sencillas como cuadrados y rectángulos delimitando zonas específicas de cada tecla, patrones de colores dentro de estas formas geométricas, mayos o menor número decolores afectando estos no solo a los elementos mencionados, pero también a los bordes, o a los fondos de dichos elementos.

En el proceso de configuración las posibles disposiciones 116 de cada rasgo gráfico también se seleccionan de entre un conjunto de disposiciones disponibles; por ejemplo, para algunos rasgos gráficos no se seleccionan disposiciones, y para otros rasgos gráficos sí se seleccionan distintas disposiciones relativas a la posición y/o orientación del rasgo gráfico 114 dentro de la tecla 214 (e.g. el rasgo gráfico puede estar dispuesto a la derecha o a la izquierda de la tecla, el rasgo gráfico puede estar girado 0° o 90°, etc.). Las diferentes disposiciones pueden combinarse entre sí (e.g. se combinan las distintas posiciones con las distintas orientaciones posibles), lo cual aumenta las combinaciones posibles de rasgos gráficos y disposiciones para generar cada tecla 214. En la selección de las disposiciones 116 puede intervenir el usuario; alternativamente, la selección puede ser realizada de manera automática (e.g. aleatoriamente). Las disposiciones pueden contar con parámetros más complejos y numerosos (por ejemplo, la disposición del carácter numérico puede estar situada de diez maneras diferentes respecto a un borde de una anchura determinada: centrada, arriba/abajo/derecha/izquierda, en las cuatro esquinas, o cubriendo gran parte de este).

En el proceso de configuración también se determinan las reglas de generación de teclado 118, las cuales tienen en cuenta los rasgos gráficos 114 y disposiciones 116 seleccionados, e incorporan unas reglas generales que determinan la manera en que se genera cada teclado utilizando los rasgos gráficos 114 y disposiciones 116 seleccionadas. Las reglas de generación de teclado 118 incluyen instrucciones para determinar el número de teclas 214 a generar para cada teclado, cómo se disponen las teclas del teclado virtual 212 (e.g. de manera circular; en una matriz de 5 filas y 2 columnas, etc.), y cómo se determina el contenido (rasgos gráficos 114 y disposiciones 116) de cada tecla 214. Por ejemplo, las reglas de generación de teclado 118 empleadas en generar el teclado virtual 212 de la **Figura 4A** pueden incluir las siguientes reglas:

- Aleatoriamente se disponen diez teclas 214 eligiendo cinco disposiciones a izquierda y cinco disposiciones a derecha.
- En cada una de las teclas 214 se ubica de forma aleatoria un número 402 sin repetir del conjunto decimal (por tanto, un número 402 diferente en cada tecla 214).
- Los números 402 de la fila superior son coloreados de forma aleatoria por cada uno de los cinco colores disponibles, sin repetir. De igual manera la fila inferior.
- Cinco pares de vocales 404 (dos “A”, dos “B”, etc.) son coloreadas aleatoriamente y son dispuestas en el hueco pequeño superior teniendo en cuenta la disposición izquierda/derecha, de modo que cada vocal 402 cubra ambas opciones (e.g. las dos vocales “A” están ubicadas a la derecha en una tecla, y a la izquierda en la otra tecla donde aparece esta vocal).
- Las veinte consonantes 406 son coloreadas uniformemente en los cinco colores disponibles (es decir, cuatro de cada color), y son dispuestas de manera aleatoria en los huecos pequeños medio e inferior.

De esta manera, el número de combinaciones posible de teclados virtuales 212 para esta configuración específica sería el resultante de la combinación de todas las posibilidades para las disposiciones, para los números, para el color de los números, etc.

La configuración de cada teclado virtual es específica para un usuario en concreto, pudiendo existir configuraciones muy similares e indistinguibles al ojo de terceros para otros usuarios (por ejemplo, las vocales son dispuestas en los huecos teniendo en cuenta la columna superior/inferior, en lugar de la disposición derecha/izquierda).

Las reglas de generación de teclado 118 pueden también incluir instrucciones para determinar el número de teclados virtuales 212 a generar, donde cada teclado virtual 212 puede generarse utilizando las mismas reglas de generación o unas reglas diferentes (e.g. generar dos teclados virtuales 212 usando unas primeras reglas de generación para el primer teclado virtual y unas segundas reglas de generación para el segundo teclado virtual). El número de teclados a generar

puede emplearse para configurar el nivel de dificultad de la autenticación (para un usuario es más sencillo una autenticación que utilice un único teclado virtual que una autenticación que emplee dos teclados virtuales).

En el proceso de configuración también se determinan las reglas de autenticación 152 del usuario 201. Estas reglas determinan los criterios que se deben utilizar para, a partir de uno o varios teclados virtuales 212, seleccionar unas determinadas teclas 214. Las reglas de autenticación 152 determinan también cuántas teclas se deben seleccionar, y pueden también determinar el modo en que se realiza la primera entrada de usuario 142 con la selección de teclas 144. Por ejemplo, y comparando con una clave de un pin de cuatro dígitos, la autenticación puede consistir en seleccionar dos teclas 214 (a modo de los dos primeros dígitos de un pin) de un primer teclado virtual 212 y otras dos teclas 214 (a modo de los dos últimos dígitos de un pin) de un segundo teclado virtual 212, donde dichos primer y segundo teclados virtuales se pueden representar a la vez o secuencialmente uno tras otro (en este último caso la autenticación consistirá en dos pasos sucesivos en los que se utilizaran dos instancias diferentes del teclado virtual 212).

Las reglas de autenticación 152 permiten obtener un resultado concreto dada una instancia de un teclado virtual 212 generado según las reglas de generación de teclado 118. Las reglas de autenticación 152 son individuales para cada usuario 201, y constituyen el único secreto que el usuario 201 ha de aprender. Dependiendo de la complejidad que se desee, las reglas de autenticación 152 pueden ser de diversa naturaleza, tales como:

- Elección de una tecla 214 o secuencia de teclas 214 basándose en uno o varios rasgos gráficos 114 o en la disposición 116 del rasgo o rasgos gráficos 114.
- Extracción de un rasgo o valor de una tecla 214 elegida.
- Modificación/transformación de ese rasgo o valor en otro.
- Referencia de otra tecla 214 basándose en el rasgo/valor/posición u otras características de la tecla 214 elegida.

A continuación, se ejemplifica una de las innumerables secuencias de reglas de autenticación 152 que el usuario 201 puede elegir a modo de mecanismo de autenticación, utilizando por ejemplo el teclado virtual 212 de la **Figura 4J**:

- Elegir la tecla 214 que incluye el rasgo gráfico 114 del número 5, y anotar la vocal que contiene (en el ejemplo de la **Figura 4J**, la tecla 214 seleccionada es la tecla de la primera fila y primera columna, y la vocal seleccionada es la "I").
- Elegir como primer resultado la otra tecla 214 del teclado virtual 212 que contiene el rasgo gráfico 114 de la misma vocal (en el ejemplo, la otra tecla 201 que contiene la vocal "I" es la tecla con el rasgo numérico "8" situada en la fila de abajo, cuarta columna).

- Elegir la tecla 214 de la fila opuesta cuyo número es azul (en este caso, la fila opuesta es la fila de arriba, y la tecla de la fila de arriba que contiene un número azul es la tecla 214 de la quinta columna, con el número “2” azul). Los colores de las letras y números en el teclado virtual 212 de la **Figura 4J** coincide con los colores ilustrados en la **Figura 4A** utilizando diferentes tipos de rayado.
- Elegir la tecla 214 de la fila opuesta y misma columna (es decir, fila inferior y quinta columna, la tecla con el número “6”), extraer la consonante situada en el hueco inferior de la tecla (la “Z”) y calcular la siguiente consonante (obteniendo en este caso la consonante “A”).
- Elegir como segundo resultado la tecla 214 con esta última consonante (la tecla con la consonante “A” es la tecla con el número “1” que se encuentra en la fila superior, cuarta columna).
- Introducir consecutivamente el primer resultado y el segundo resultado (en este ejemplo, el usuario introduce la tecla “8” y después la tecla “1”). El resultado se puede introducir por ejemplo mediante la pulsación secuencial de dichas teclas, en el caso de que se represente el teclado virtual 212 en una pantalla táctil. Alternativamente, el resultado se puede introducir por otros tipos de interfaces (e.g. un teclado físico, un comando de voz, etc.).

En este ejemplo de proceso de autenticación el usuario 201 ha de elegir por tanto una pareja de teclas 214 resultante de la instancia de teclado virtual 212 generada a tal propósito. En las reglas de autenticación 152 se pueden incluso incorporar elementos externos, como por ejemplo el día del mes y las dos primeras letras de la ciudad donde se realiza la autenticación. Así, en el caso de que la autenticación se realice el día 24 del mes desde Madrid (“MA”), se disponen las siguientes reglas:

- Elegir como primer resultado la tecla 214 situada a la derecha de la tecla 214 que incluya la primera aparición de la primera letra de la ciudad (en el ejemplo, la consonante “M”). Si la tecla con la consonante “M” resulta estar situada en la quinta columna, se elegirá entonces la tecla situada en la primera columna de la misma fila del teclado virtual 212. Utilizando por ejemplo el teclado de la **Figura 4J**, la tecla elegida sería la tecla “6”, al ser la tecla situada a la derecha de la tecla “8” que contiene la consonante “M”.
- Elegir como segundo resultado la tecla 214 situada a la derecha de la tecla 214 con la primera aparición de la segunda letra de la ciudad (en el ejemplo, la vocal “A”), donde el teclado virtual 212 se recorre de izquierda a derecha y de arriba a abajo. Utilizando el teclado de la **Figura 4J** la tecla elegida sería la tecla “2”, al ser la tecla situada a la derecha de la tecla “1” que contiene la primera aparición de la vocal “A”.
- Introducir consecutivamente el primer resultado y el segundo resultado.

Las reglas de autenticación 152 pueden aumentar en complejidad, basándose en otros elementos externos como pueden ser parte del identificador del servicio donde se produce el proceso de

autenticación; incorporación de mensajes OTP específico para ese proceso de autenticación; cálculos matemáticos más complejos (multiplicaciones, módulos, exponenciación, etc.); transformaciones de posición más complejas como movimiento de caballo; comparaciones lógicas (e.g. si la disposición de la primera “E” está en la izquierda, elegir el valor 7, y si está en la derecha elegir el valor 4, o dependiendo del valor par/impar del rasgo numérico de una determinada teclas), transformaciones entre letras, valores numéricos y posiciones (si es “A” sumar 1, si es “E” sumar 2, etc.).

En las reglas de autenticación 152 el resultado elegido puede incluir la selección de una única tecla o de múltiples teclas (e.g. cuatro teclas). En el caso de que el resultado incluya varias teclas seleccionadas, el orden de la selección de las teclas realizado por el usuario 201 puede ser relevante o no de cara a la autenticación, en función de la configuración de la autenticación. Por ejemplo, si un usuario sigue las reglas de autenticación 152 y obtiene como resultado las teclas “2”, “8” y “5”, el resultado de la autenticación 242 puede considerarse positivo en el caso de que el usuario introduzca las teclas en ese mismo orden dictado por las reglas de autenticación 152, y no en otro orden. Alternativamente, de cara a la autenticación se podría permitir la introducción de las teclas en cualquier otro orden (e.g. “2”, “5”, “8”). En la **Figura 5** se muestra un proceso de autenticación empleando cuatro teclados virtuales (212a, 212b, 212c, 212d) generados por la unidad de generación de teclado virtual 210. Los teclados virtuales se pueden mostrar de diferentes maneras; por ejemplo, se pueden mostrar secuencialmente, un teclado tras otro (de forma que para cada teclado virtual representado el usuario elige una o varias teclas 214 como resultado), o se pueden mostrar varios teclados virtuales 212 a la vez (e.g. se muestran de golpe todos los teclados virtuales, y el usuario tiene que elegir una o varias teclas 214 como resultado utilizando unas determinadas reglas de autenticación 152).

Cada uno de los cuatro teclados virtuales (212a, 212b, 212c, 212d) se han generado de acuerdo a las siguientes reglas de generación de teclado 118, similares a las utilizadas para la **Figura 4I**:

- Cada teclado virtual está formado por diez teclas 214 dispuestas en cinco columnas y dos filas, usando una paleta de diez colores (azul, cian, amarillo, verde, menta, rojo, rosa, naranja, morado y gris), para una configuración de seguridad de 108 (equivalente a un pin de 8 cifras) introducidas de dos en dos.
- Cada tecla 214 está compuesta de:
 - ~ Un elemento central, formado por un número 402 ocupando dos tercios horizontalmente, y una vocal 404 y dos consonantes 406 en sentido vertical ocupando el tercer tercio horizontal. En el teclado virtual cinco veces está el número 402 dispuesto a la izquierda y otras cinco veces está el número 402 dispuesto a la derecha. La vocal 404 está dispuesta en el hueco superior, reservando los otros dos huecos (medio e inferior) para las consonantes 406.
 - ~ Un elemento borde, que contiene a su vez dos rasgos gráficos diferentes: cuatro bordes

laterales 430 y cuatro vértices 432 o esquinas.

- La situación del elemento central viene determinada por un rasgo gráfico de posición, de diez variaciones ilustradas a través de unos bordes finos 434 grises alrededor del elemento central (arriba, abajo, derecha, izquierda, cada una de las cuatro esquinas, centrado, y ampliado -i.e. sin bordes finos 434-). Por ejemplo, denotando cada tecla 214 por el valor numérico que muestra, en el primer teclado virtual 212a de la **Figura 5**, la tecla “3” tiene una variación central, al disponer de 4 bordes finos 434; la tecla “9” tiene una variación ampliada, al no tener bordes finos 434; la tecla “6” tiene una variación derecha, al no tener bordes finos 434 a la derecha; la tecla “1” tiene una variación arriba-derecha, al no tener bordes finos 434 arriba y a la derecha.
- El rasgo gráfico de los cuatro bordes laterales 430 de cada tecla 214 está coloreado de uno de los diez colores disponibles.
- El rasgo gráfico de los cuatro bordes laterales 430 de cada tecla 214 tiene un patrón de coloreado de diez variaciones posibles, una diferente en cada tecla 214:
 - ~ Cuatro variaciones en “C”, con la apertura para arriba (e.g. tecla “4” del primer teclado virtual 212a), abajo (e.g. tecla “2” del primer teclado virtual 212a), derecha (e.g. tecla “7” del primer teclado virtual 212a) e izquierda (e.g. tecla “3” del primer teclado virtual 212a).
 - ~ Cuatro variaciones en “L” apuntando para cada una de las cuatro esquinas (e.g. teclas “1”, “9”, “0” y “5” del primer teclado virtual 212a).
 - ~ Coloreados únicamente los bordes laterales 430 verticales (e.g. tecla “6” del primer teclado virtual 212a).
 - ~ Coloreados únicamente los bordes laterales 430 horizontales (e.g. tecla “8” del primer teclado virtual 212a).
- El rasgo gráfico de los cuatro vértices 432 de cada tecla 214 está coloreado de uno de los diez colores disponibles.
- El rasgo gráfico de los cuatro vértices 432 de cada tecla 214 muestra un patrón de coloreado de diez variaciones posibles, una diferente en cada tecla 214:
 - ~ Tres vértices 432 coloreados dejando el cuarto vértice sin colorear, en cada una de las esquinas.
 - ~ Dos vértices 432 coloreados arriba, abajo, derecha e izquierda.
 - ~ Dos vértices 432 coloreados en esquinas diametralmente opuestas.
- En cada tecla 214 se incluye un número 402 no repetido del conjunto de los primeros diez números naturales (i.e. de “0” a “9”). A su vez, cada uno de los números 402 está coloreado de uno de los diez posibles colores.
- En cada teclado virtual se muestra cada una de las cinco vocales 404 aleatoriamente en la columna derecha, e igualmente en la columna izquierda. El rasgo vocal se colorea de cada uno de los 10 colores disponibles aleatoriamente.

- Existen 20 rasgos consonantes 406 diferentes (esto es, se emplean 20 diferentes consonantes), que se reparten aleatoriamente entre los 20 huecos disponibles en las diez teclas 214. Los rasgos consonantes 406 situados centralmente se colorean de cada uno de los 10 colores disponibles aleatoriamente. Igualmente, las consonantes 406 situadas en el hueco inferior se colorean aleatoriamente de cada uno de los 10 colores disponibles.

Con esta configuración, la operación de elección de una o varias teclas para el proceso de autenticación puede estar definida, entre otras variables:

- Por la posición de la tecla 214.
- Por el color de los cuatro vértices 432, de los cuatro bordes laterales 430, de la cifra numérica 402, de la vocal 404, de la consonante 406 media, o de la consonante 406 inferior.
- Por el patrón de coloreado de los cuatro vértices 432 o de los cuatro bordes laterales 430.
- Por la vocal 404 y su disposición derecha o izquierda.
- Por una consonante 406.
- Por el valor del número 402 de la tecla 214.

Esta operación de elección de tecla se puede combinar con una operación de extracción (e.g. de la tecla X extraer el valor del rasgo Y), de modificación, transformación y referencia, entre otras, hasta conformar una selección de teclas 144 como primera entrada de usuario 142, donde la selección de teclas 144 puede incluir cualquier número de teclas seleccionadas, en función de la configuración (e.g. una tecla seleccionada, dos teclas seleccionadas, etc.).

Algunas de las posibles reglas de autenticación 152 del usuario 201 serían:

- Elegir las dos teclas 214 del teclado virtual 212 que incluyen la vocal "A".
- Extraer sus valores numéricos (donde el 0 se interpreta como 10).
- Multiplicar estos valores.
- Sumar el valor del número 402 mostrado en cian en el teclado virtual 212.

- Como resultado, elegir las teclas 214 a la derecha de cada cifra de este resultado, considerando como la derecha de la tecla situada en la quinta columna a la tecla de la primera columna de la misma fila.

Aplicando estas reglas de autenticación a los cuatro teclados virtuales (212a, 212b, 212c, 212d) de la **Figura 5**, se obtiene:

- Para el primer teclado virtual 212a (identificando las teclas por su valor numérico):
 - ~ Las teclas con "A" son las teclas "0" y "3", que multiplicadas son 30.
 - ~ El número 402 de color cian es el "6", que sumado a 30 resulta 36.
 - ~ Las teclas elegidas como resultado son las situadas a la derecha de cada cifra "3" y "6", esto

es, las teclas “8” y “1”, respectivamente.

- Para el segundo teclado virtual 212b:

~ Las teclas con “A” son las teclas “4” y “6”, que multiplicadas son 24.

~ El número 402 de color cian es el “5”, que sumado a 24 resulta 29.

5 ~ Las teclas elegidas como resultado son las situadas a la derecha de cada cifra “2” y “9”, esto es, las teclas “3” y “2”, respectivamente.

- Para el tercer teclado virtual 212c:

~ Las teclas con “A” son las teclas “0” y “9”, que multiplicadas son 90, ya que se considera que la tecla “0” tiene un valor de 10.

10 ~ El número 402 de color cian es el “9”, que sumado a 90 resulta 99.

~ Las teclas elegidas como resultado son las situadas a la derecha de cada cifra “9” y “9”, esto es, las teclas “1” y “1”, respectivamente (i.e. la tecla “1” se selecciona en este caso dos veces).

- Para el cuarto teclado virtual 212d:

15 ~ Las teclas con “A” son las teclas “0” y “8”, que multiplicadas son 80, ya que se considera que la tecla “0” tiene un valor de 10.

~ El número 402 de color cian es el “1”, que sumado a 80 resulta 81.

~ Las teclas elegidas como resultado son las situadas a la derecha de cada cifra “8” y “1”, esto es, las teclas “6” y “7”, respectivamente.

20 Conformando así el resultado final el valor “81321167”. Este resultado se puede introducir de múltiples formas; por ejemplo, mediante voz o teclado. En el caso de que se emplee una pantalla 220 táctil para representar los teclados virtuales, como se ilustra en el ejemplo de la **Figura 5**, se puede exigir al usuario 201 introducir la selección de teclas 144 de cada teclado virtual (212a, 212b, 212c, 212d) mediante la pulsación de las teclas seleccionadas en cada teclado virtual. De manera
25 ventajosa, la propia representación gráfica de los teclados virtuales 212 se puede emplear como medio de entrada de usuario para la autenticación, no requiriendo de medios de entrada adicionales (como un teclado físico o una interfaz gráfica adicional).

El proceso de autenticación de la presente invención se puede considerar que es un método de autenticación mutua, ya que por un lado la unidad de autenticación 240 del sistema de autenticación
30 se encarga de autenticar al usuario 201, pero a su vez el usuario 201 es capaz de autenticar al sistema de autenticación ya que el usuario 201 conoce, además de las reglas de autenticación 152, los rasgos gráficos 114 y disposiciones 116 que pueden adoptar los teclados virtuales 212 representados, así como las reglas de generación de teclado 118 empleadas (de hecho, el usuario 201 ha podido intervenir en todo el proceso de configuración de los teclados virtuales, o incluso llegar
35 a crear nuevos rasgos gráficos que los propuestos por el sistema). De esta forma, si un sistema

informático quiere hacerse pasar por el sistema de autenticación autorizado, el usuario 201 será capaz de detectar esta situación fraudulenta al comprobar que los teclados virtuales 212 representados no se corresponden con los rasgos gráficos 114, las disposiciones 116 o las reglas de generación de teclado 118 previamente adoptadas en la configuración de teclado 112 del usuario 201. Para realizar un ataque de este tipo, el sistema informático atacante debería conocer en detalle las reglas de generación de teclado 118, las cuales estarían guardadas a buen recaudo (e.g. en un servidor). Las reglas de generación de teclado 118 pueden incluso considerar elementos externos (como por ejemplo el día del mes, de forma que en los días pares del mes se empleen un tipo de rasgos gráficos 114 y disposiciones 116, y en los días impares otros diferentes). De esta forma, el proceso de autenticación de un usuario realizado en la presente invención añade una capa adicional de seguridad, ya que permite que el propio usuario autentique al propio sistema de autenticación (esto es, compruebe que el sistema de autenticación no es un impostor).

El proceso de autenticación de la presente invención se puede emplear en cualquier aplicación en la que se requiera autenticar a un usuario, como por ejemplo, sin ser limitativo:

- Acceso a una aplicación o a una página web.
- Método desbloqueo de un dispositivo electrónico (e.g. un teléfono inteligente), donde la unidad de generación de teclado virtual 210 y la unidad de autenticación 240 están ambas en el propio dispositivo (ya sea en memoria, en chip dedicado, etc.).
- Método de desbloqueo de un fichero comprimido-codificado-enchifrado (se puede considerar similar al desbloqueo de un dispositivo pero a nivel de software, donde la "clave" hasheada de alguna forma estaría auto contenida en el fichero).
- Autenticación a niveles progresivos de seguridad en una app (e.g. una app bancaria donde para acceder pide resolver un par de teclados virtuales, y para confirmar la operación de transferencia pide resolver otro u otros teclados virtuales más).
- Uso de cajeros, pagos en un terminal punto de venta (TPV), donde la autenticación valida una operación en concreto.
- Control de accesos (e.g. una puerta de alta seguridad de control de acceso a un edificio).
- El uso como mecanismo de captcha, al ser una instrucción verbal de fácil comprensión, pero complicado para que una máquina lo realice automáticamente.
- Como token de sesión (si se utiliza un par teclado-solución único, este puede utilizarse como token de sesión al conformar una clave única y con un riesgo de colisión prácticamente despreciable).

REIVINDICACIONES

1. Un método de autenticación mutua, que comprende:

~ obtener (110) una configuración de teclado (112) de un usuario (201) a autenticar, donde la configuración de teclado (112) incluye:

- una pluralidad de rasgos gráficos (114),
- una pluralidad de disposiciones (116) de los rasgos gráficos (114), y
- unas reglas de generación de teclado (118);

~ generar (120) al menos un teclado virtual (212), donde cada teclado virtual (212) está formado por una pluralidad de teclas (214) que incorporan una combinación de rasgos gráficos (114) dispuestos en unas determinadas disposiciones (116), donde los rasgos gráficos (114) y disposiciones (116) utilizados en cada tecla (214) son seleccionados de la configuración de teclado (112) del usuario (201) en base a las reglas de generación de teclado (118);

~ mostrar (130) el al menos un teclado virtual (212);

~ recibir (140) una primera entrada de usuario (142) correspondiente a una selección de teclas (144) de cada teclado virtual (212);

- obtener (150) unas reglas de autenticación (152) del usuario (201);

~ aplicar (160) las reglas de autenticación (152) del usuario (201) sobre el al menos un teclado virtual (212) para obtener al menos una secuencia de teclas correcta (162); y

~ autenticar (170) al usuario (201) si la selección de teclas (144) de la primera entrada de usuario (142) es validada con respecto a una secuencia de teclas correcta (162).

2. El método de acuerdo a la reivindicación 1, que comprende obtener (102) una identificación (204) del usuario (201) a autenticar previa a la obtención (110) de la configuración de teclado (112).

3. El método de acuerdo a cualquiera de las reivindicaciones anteriores, que comprende obtener (104) una segunda entrada de usuario (106), y donde al menos un teclado virtual (212) se genera en base a las reglas de generación de teclado (118) en combinación con dicha segunda entrada de usuario (106).

4. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde el al menos un teclado virtual (212) se muestra (130) en al menos una pantalla (220).

5. El método de acuerdo a la reivindicación 4, donde la al menos una pantalla (220) es táctil y donde la selección de teclas (144) se realiza mediante la pulsación en teclas (214) seleccionadas de cada teclado virtual (212) mostrado en la al menos una pantalla (220) táctil.

6. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde la configuración de teclado (112) del usuario (201) se obtiene mediante el acceso a una base de datos (211) o una memoria (213).
- 5 7. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde las reglas de autenticación (152) del usuario (201) se obtienen mediante el acceso a una base de datos (241) o una memoria (243).
8. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde mediante la aplicación de las reglas de autenticación (152) del usuario (201) sobre el al menos un teclado virtual (212) se obtiene una pluralidad de secuencias de teclas correctas (162).
- 10 9. El método de acuerdo a la reivindicación 8, donde la autenticación del usuario (201) comprende diferentes niveles de autenticación, en función de la secuencia de teclas correcta (162) con respecto a la que la selección de teclas (144) es validada.
10. El método de acuerdo a cualquiera de las reivindicaciones 8 a 9, que comprende identificar al usuario entre un conjunto de usuarios, en función de la secuencia de teclas correcta (162) con respecto a la que la selección de teclas (144) es validada.
- 15 11. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde las disposiciones (116) de los rasgos gráficos (114) en cada tecla (214) definen la posición y/o orientación del rasgo gráfico (114) dentro de la tecla (214).
12. El método de acuerdo a cualquiera de las reivindicaciones anteriores, donde los rasgos gráficos (114) están formados por:
- 20 ~ rasgos principales, que definen la forma del rasgo gráfico (114), y
~ rasgos secundarios, que definen una característica de los rasgos principales.
13. Un sistema de autenticación mutua, que comprende:
- ~ una unidad de generación de teclado virtual (210) configurada para:
- 25 · obtener (110) una configuración de teclado (112) de un usuario (201) a autenticar, donde la configuración de teclado (112) incluye:
- ~ una pluralidad de rasgos gráficos (114),
~ una pluralidad de disposiciones (116) de los rasgos gráficos (114), y
~ unas reglas de generación de teclado (118); y
- 30 · generar (120) al menos un teclado virtual (212), donde cada teclado virtual (212) está formado por una pluralidad de teclas (214) que incorporan una combinación de rasgos gráficos (114) dispuestos en unas determinadas disposiciones (116), donde

los rasgos gráficos (114) y disposiciones (116) utilizados en cada tecla (214) son seleccionados de la configuración de teclado (112) del usuario (201) en base a las reglas de generación de teclado (118);

- 5 - una interfaz de entrada (230) configurada para recibir (140) una primera entrada de usuario (142) correspondiente a una selección de teclas (144) de cada teclado virtual (212); y
- una unidad de autenticación (240) configurada para:
 - obtener (150) unas reglas de autenticación (152) del usuario (201);
 - 10 · aplicar (160) las reglas de autenticación (152) del usuario (201) sobre el al menos un teclado virtual (212) para obtener al menos una secuencia de teclas correcta (162); y
 - autenticar (170) al usuario (201) si la selección de teclas (144) de la primera entrada de usuario (142) es validada con respecto a una secuencia de teclas correcta (162).

15 **14.** El sistema de acuerdo a la reivindicación 13, que comprende una unidad de identificación de usuario (202) configurada para obtener (102) una identificación (204) del usuario (201) a autenticar.

15. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 14, donde la interfaz de entrada (230) está configurada para obtener (104) una segunda entrada de usuario (106), y donde la unidad de generación de teclado virtual (210) está configurada para generar al menos un teclado virtual (212) en base a las reglas de generación de teclado (118) en combinación con dicha
20 segunda entrada de usuario (106).

16. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 15, que comprende además un dispositivo de representación de información configurado para mostrar (130) el al menos un teclado virtual (212).

25 **17.** El sistema de acuerdo a la reivindicación 16, donde el dispositivo de representación de información comprende al menos una pantalla (220) táctil, la interfaz de entrada (230) comprende dicha al menos una pantalla (220) táctil, y la selección de teclas (144) se realiza mediante la pulsación, por parte del usuario (201), en teclas (214) seleccionadas de cada teclado virtual (212) representado.

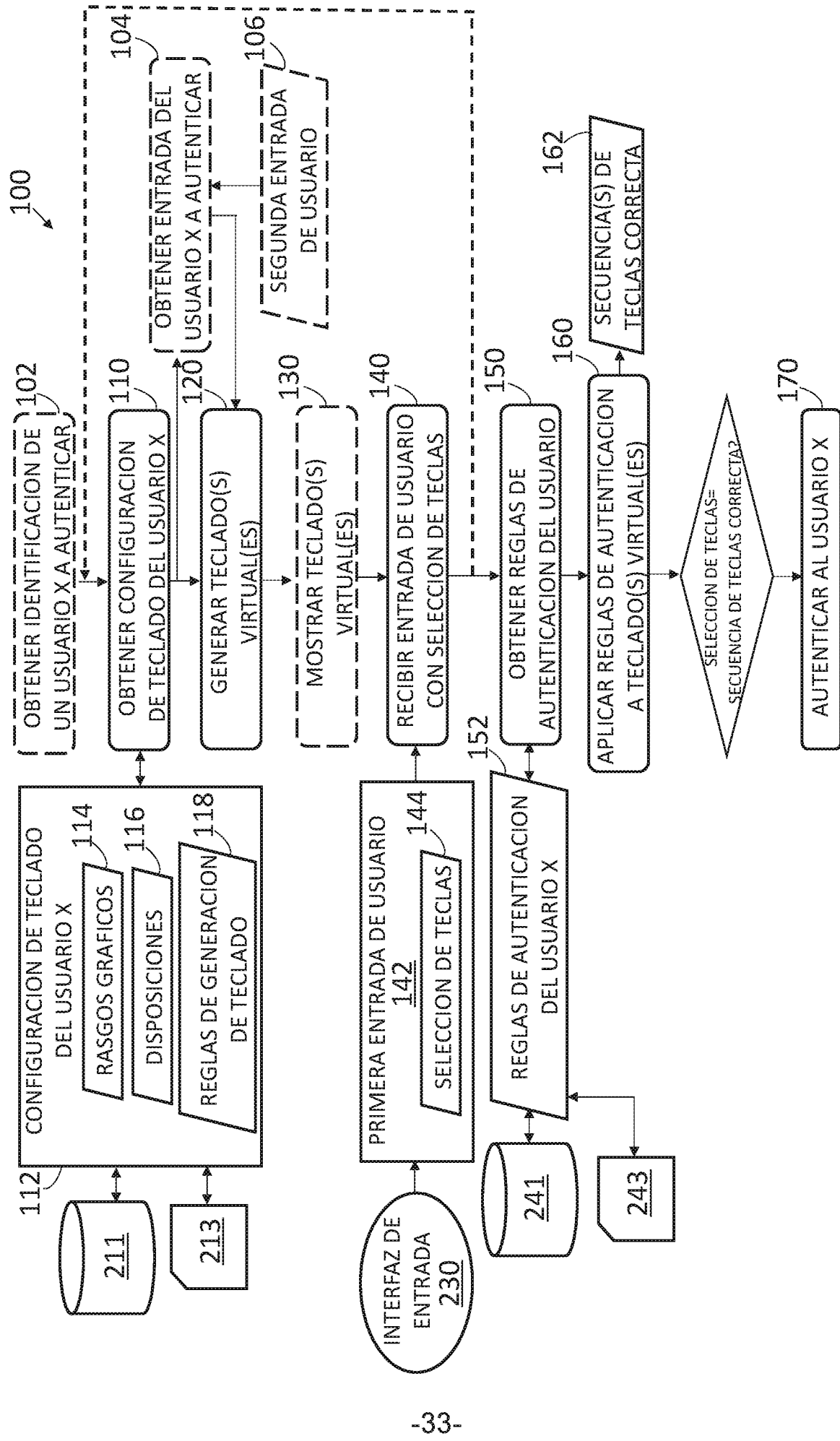
30 **18.** El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 17, donde la unidad de generación de teclado virtual (210) está configurada para obtener (110) la configuración de teclado (112) del usuario (201) mediante el acceso a una base de datos (211) externa o una memoria (213) interna.

19. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 18, donde la unidad de autenticación (240) está configurada para obtener las reglas de autenticación (152) del usuario (201) mediante el acceso a una base de datos (241) externa o una memoria (243) interna.
- 5 20. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 19, donde la unidad de autenticación (240) está configurada para obtener una pluralidad de secuencias de teclas correctas (162) mediante la aplicación de las reglas de autenticación (152) del usuario (201) sobre el al menos un teclado virtual (212).
- 10 21. El sistema de acuerdo a la reivindicación 20, donde la unidad de autenticación (240) está configurada para autenticar al usuario (201) según diferentes niveles de autenticación, en función de la secuencia de teclas correcta (162) con respecto a la que la selección de teclas (144) es validada.
- 15 22. El sistema de acuerdo a cualquiera de las reivindicaciones 20 a 21, donde la unidad de autenticación (240) está configurada para identificar al usuario entre un conjunto de usuarios, en función de la secuencia de teclas correcta (162) con respecto a la que la selección de teclas (144) es validada.
23. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 22, donde los elementos del sistema forman parte de un mismo dispositivo electrónico.
24. El sistema de acuerdo a cualquiera de las reivindicaciones 13 a 22, donde los elementos del sistema están distribuidos en diferentes dispositivos electrónicos.
- 20 25. Un medio de almacenamiento no transitorio legible por ordenador, que comprende instrucciones de programa almacenadas en el mismo que, cuando se ejecutan en un procesador, causan que el procesador lleve a cabo el método de cualquiera de las reivindicaciones 1 a 12.

RESUMEN

Método y sistema de autenticación mutua. El sistema comprende:

- 5 - una unidad de generación de teclado virtual (210) para obtener (110) una configuración de teclado (112) de un usuario (201), incluyendo rasgos gráficos (114), disposiciones (116) y reglas de generación de teclado (118); y generar (120) un teclado virtual (212) formado por teclas (214) con combinación de rasgos gráficos (114) en unas determinadas disposiciones (116) en base a las reglas de generación de teclado (118);
- una interfaz de entrada (230) para recibir (140) una selección de teclas (144) del teclado virtual (212);
- 10 - una unidad de autenticación (240) para aplicar (160) unas reglas de autenticación (152) del usuario (201) sobre el teclado virtual (212), obteniendo al menos una secuencia de teclas correcta (162), y autenticar (170) al usuario (201) si la selección de teclas (144) es validada con respecto a una secuencia de teclas correcta (162).



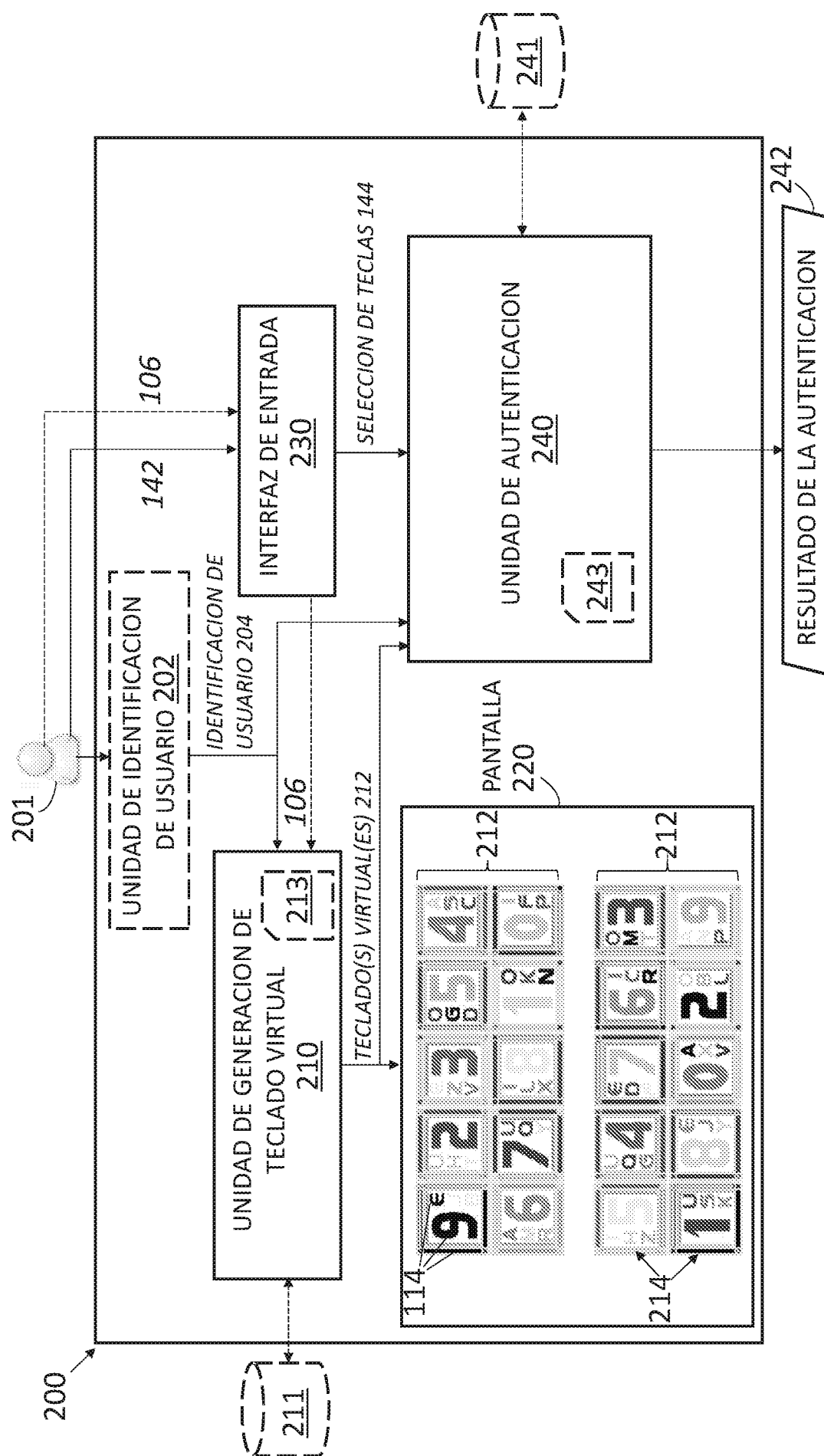


FIG. 2

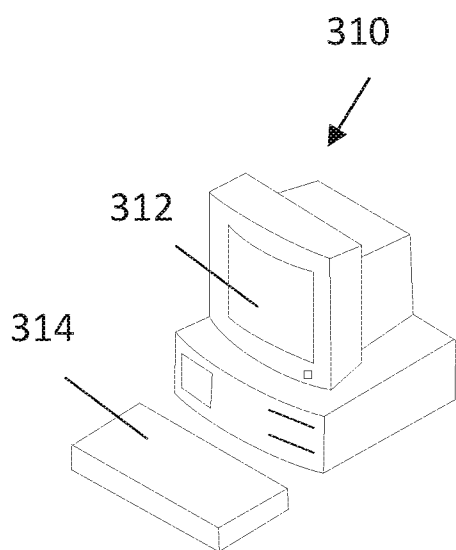


FIG. 3A

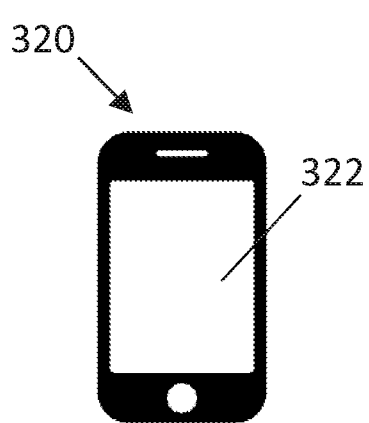


FIG. 3B

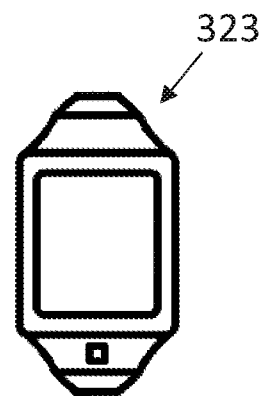


FIG. 3C

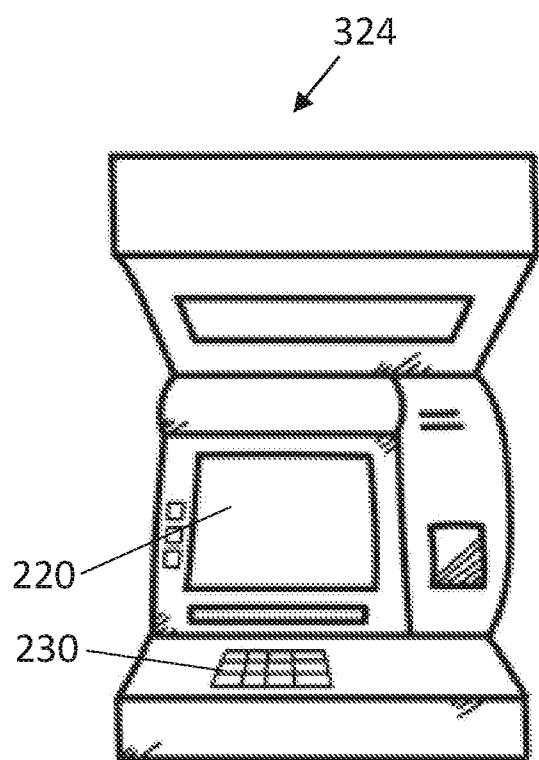


FIG. 3D

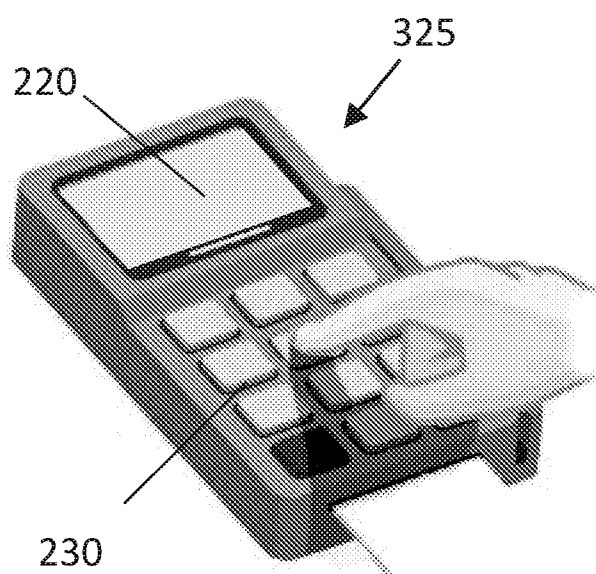


FIG. 3E

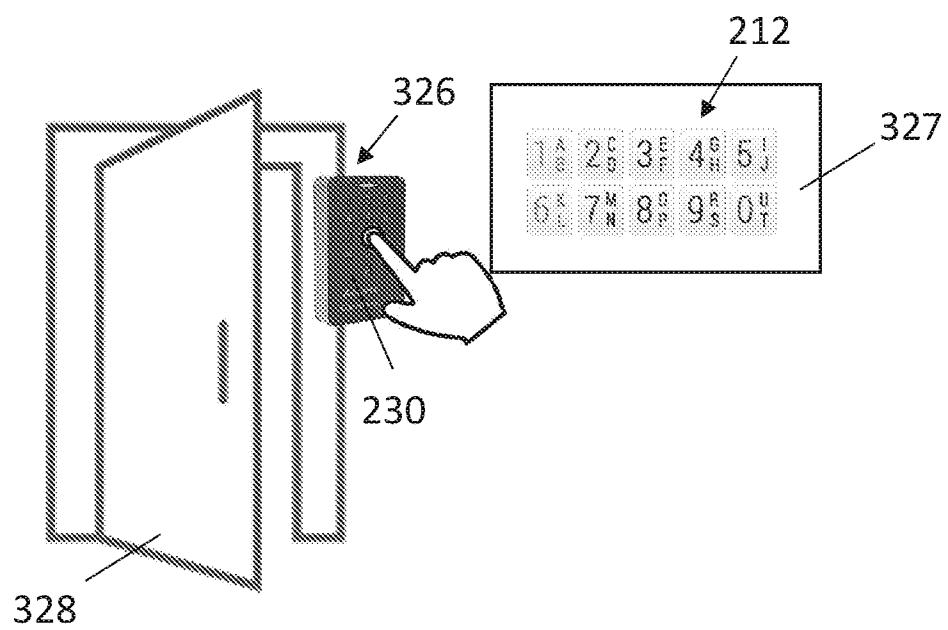


FIG. 3F

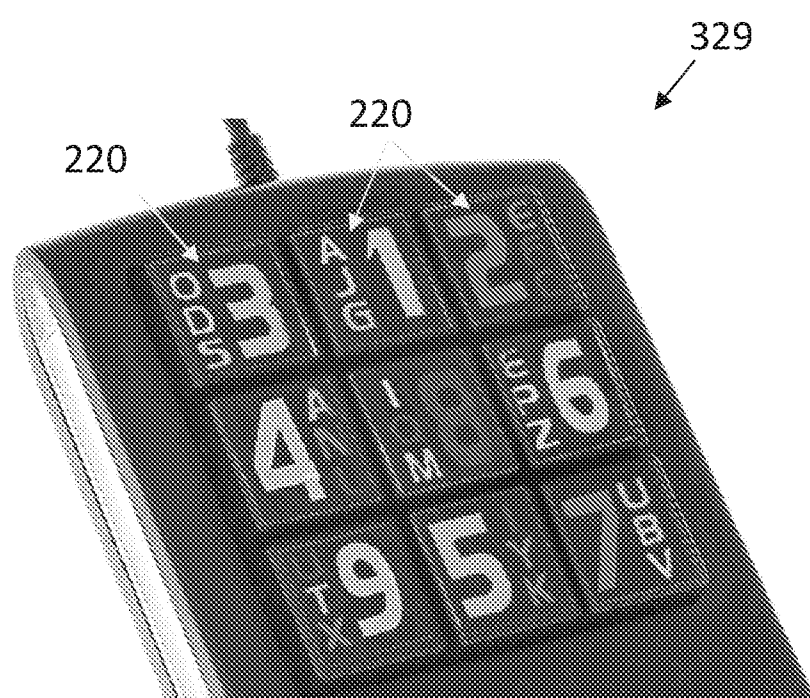


FIG. 3G

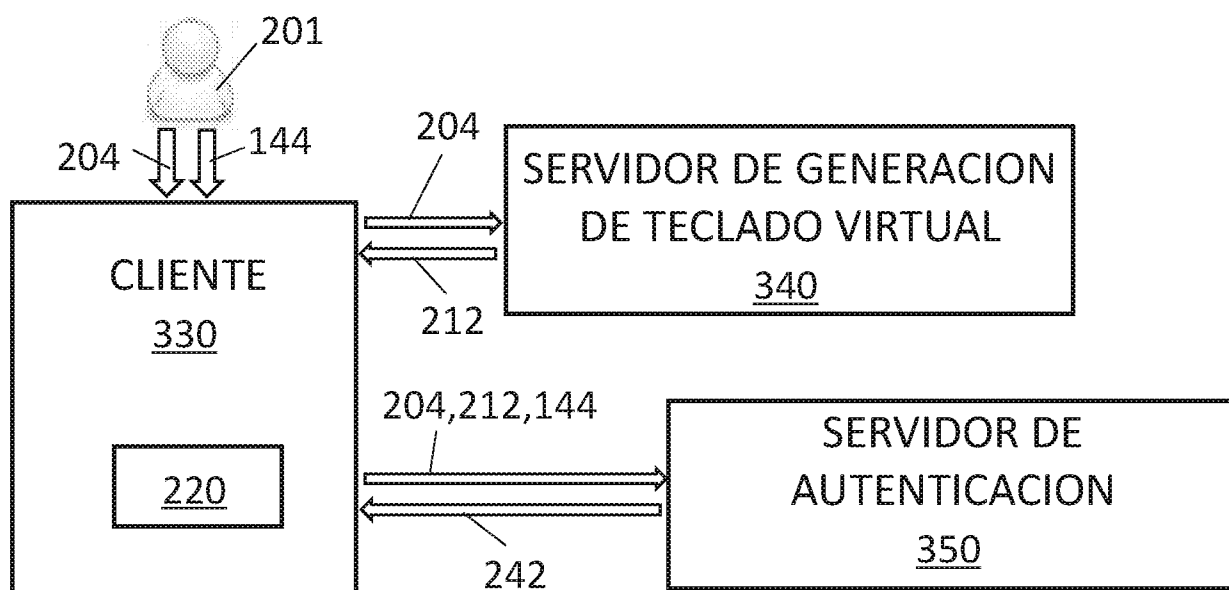


FIG. 3H

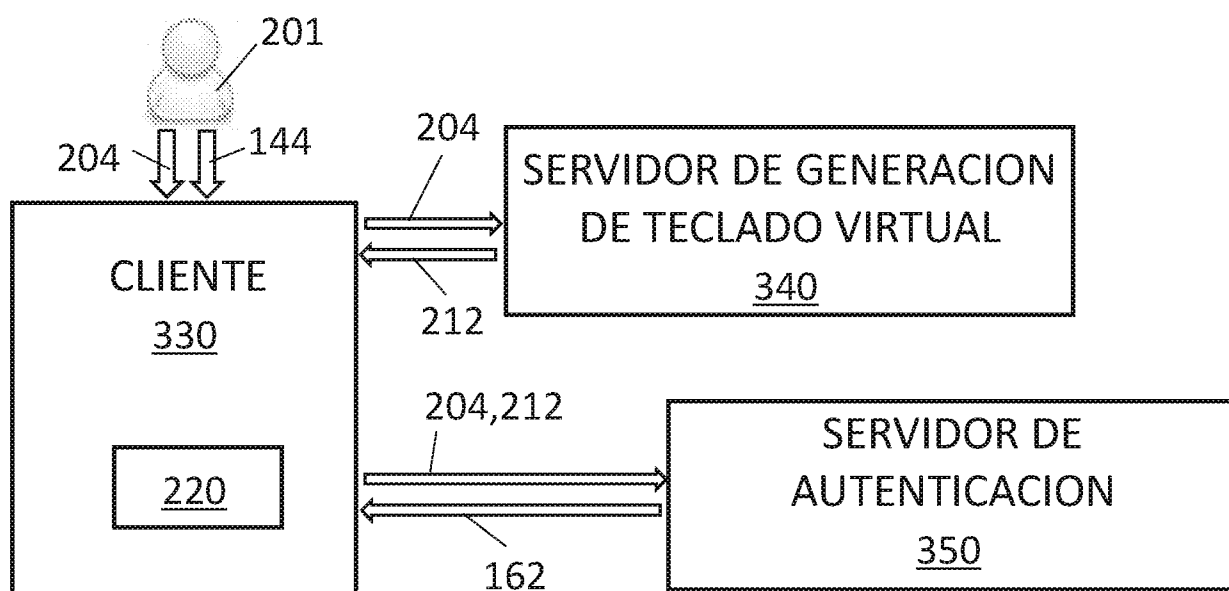


FIG. 3I

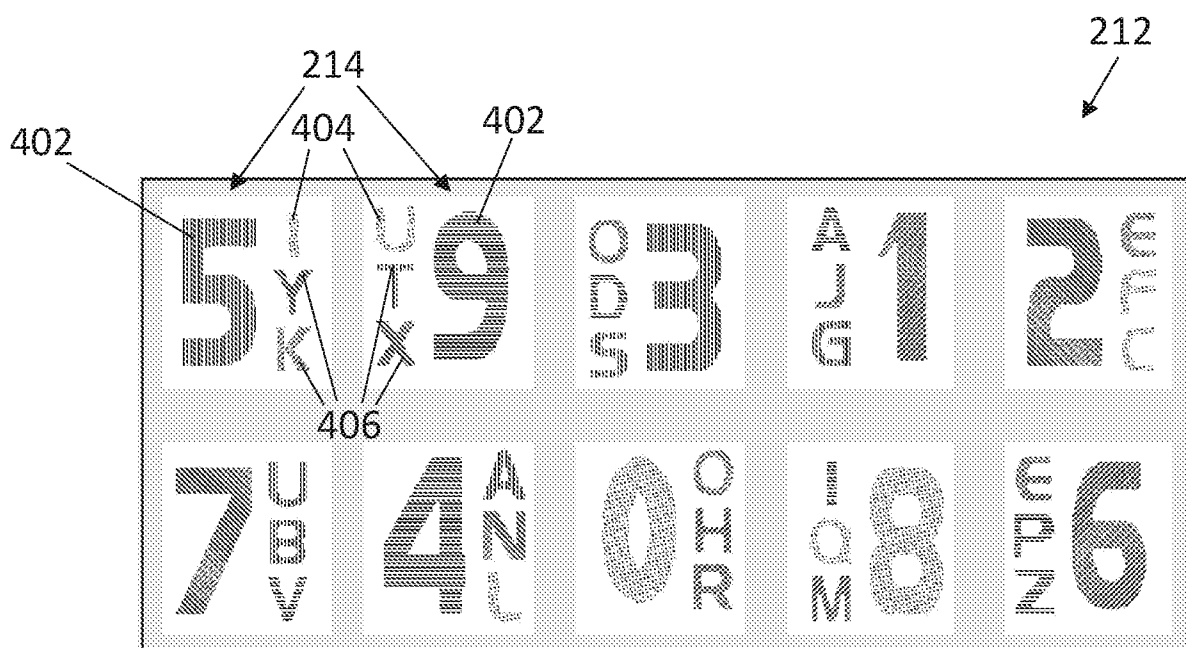


FIG. 4A

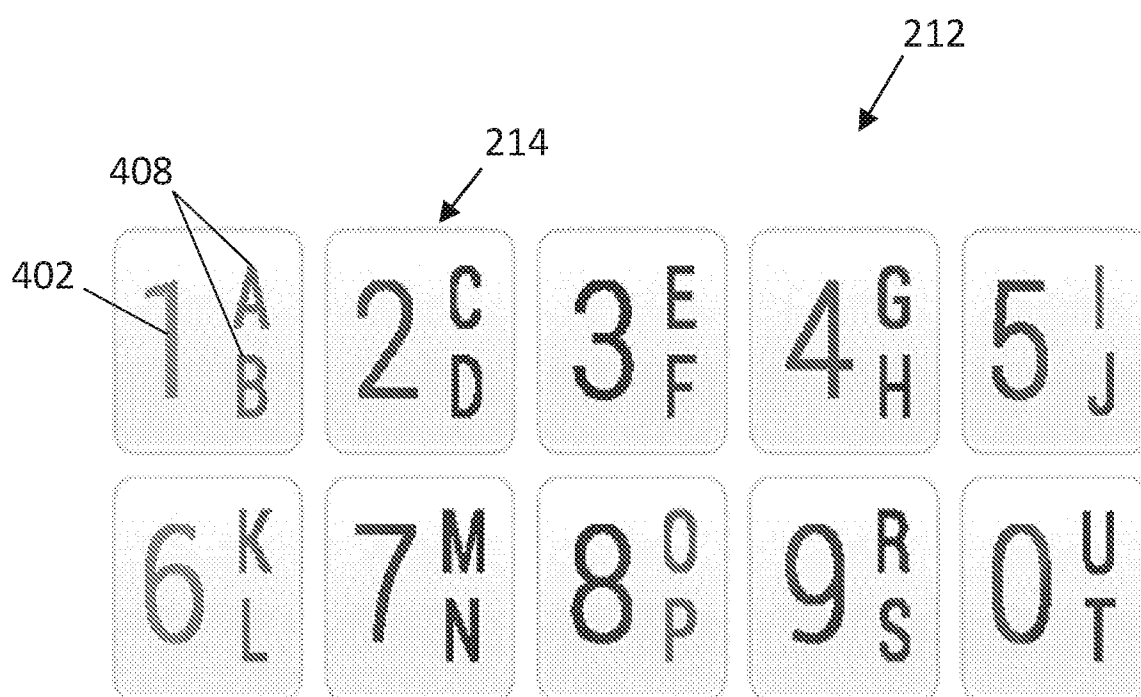


FIG. 4B

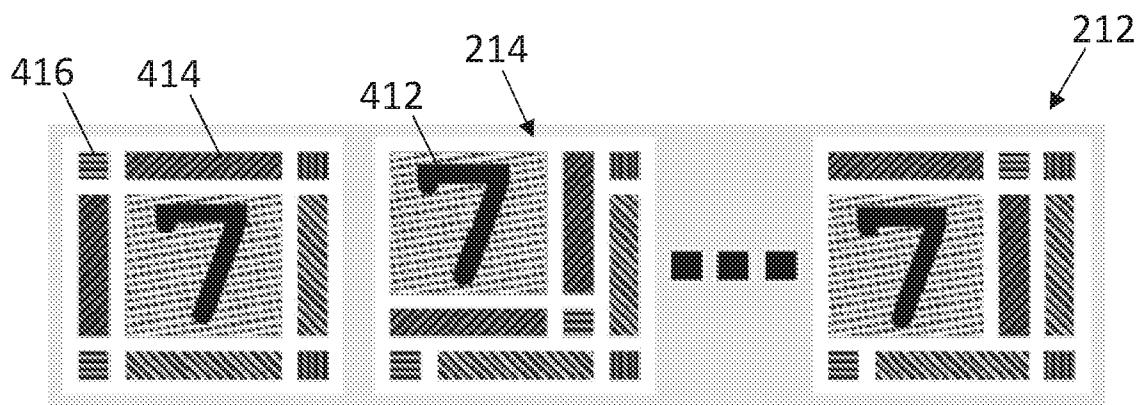


FIG. 4C

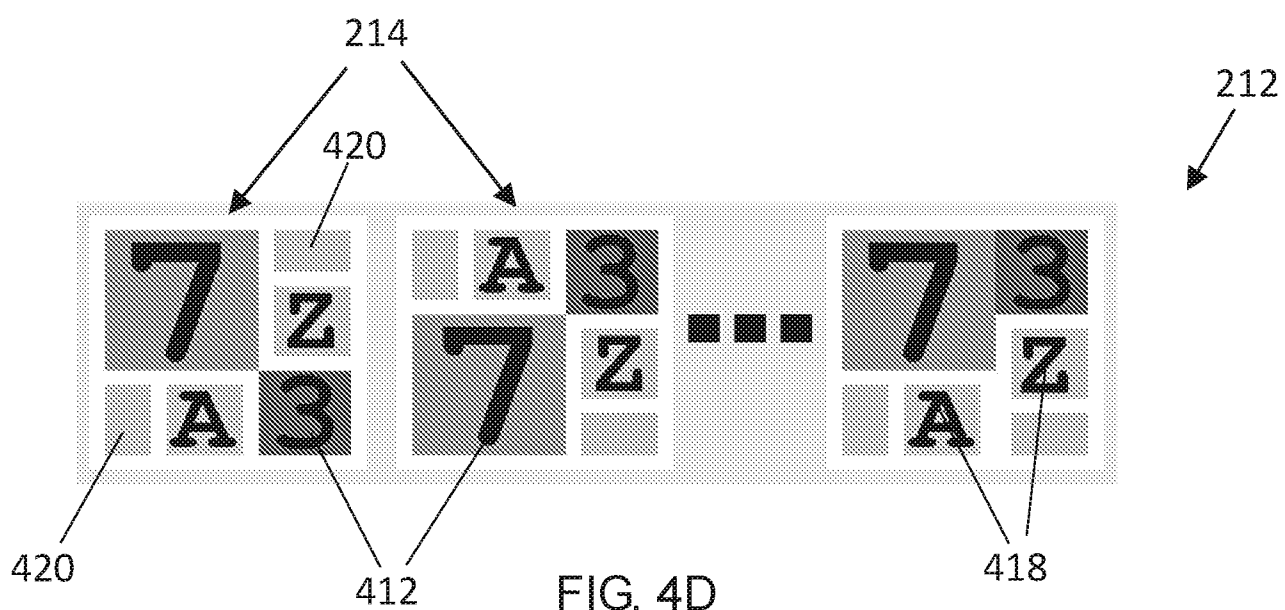


FIG. 4D

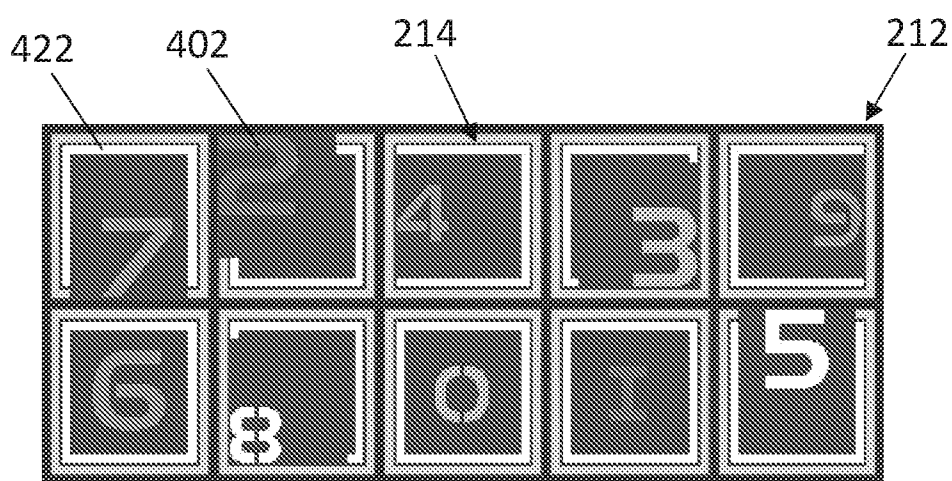


FIG. 4E

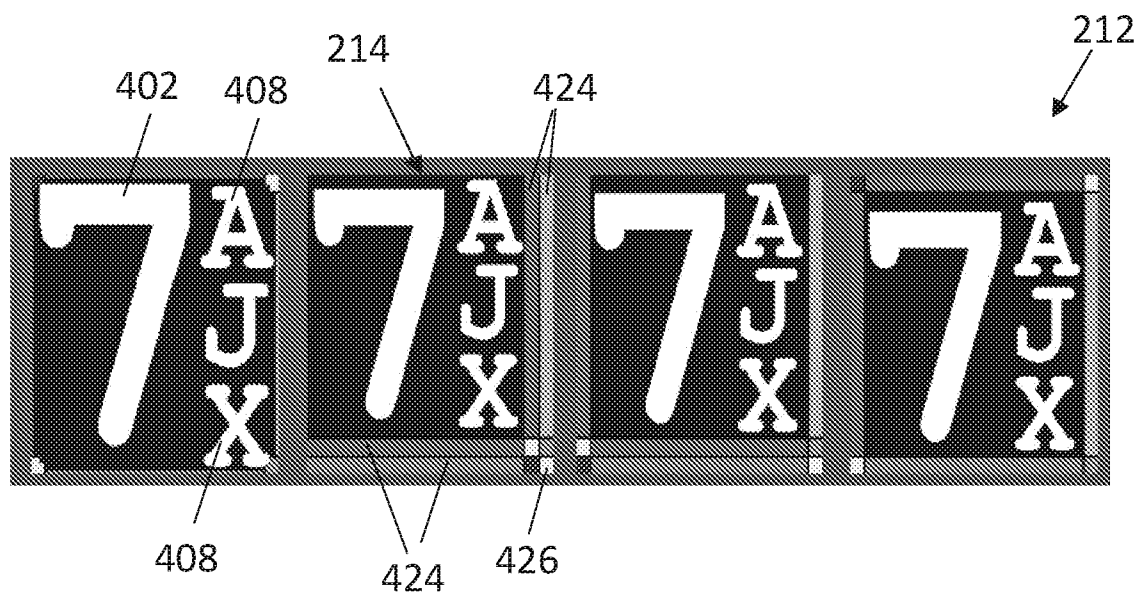


FIG. 4F

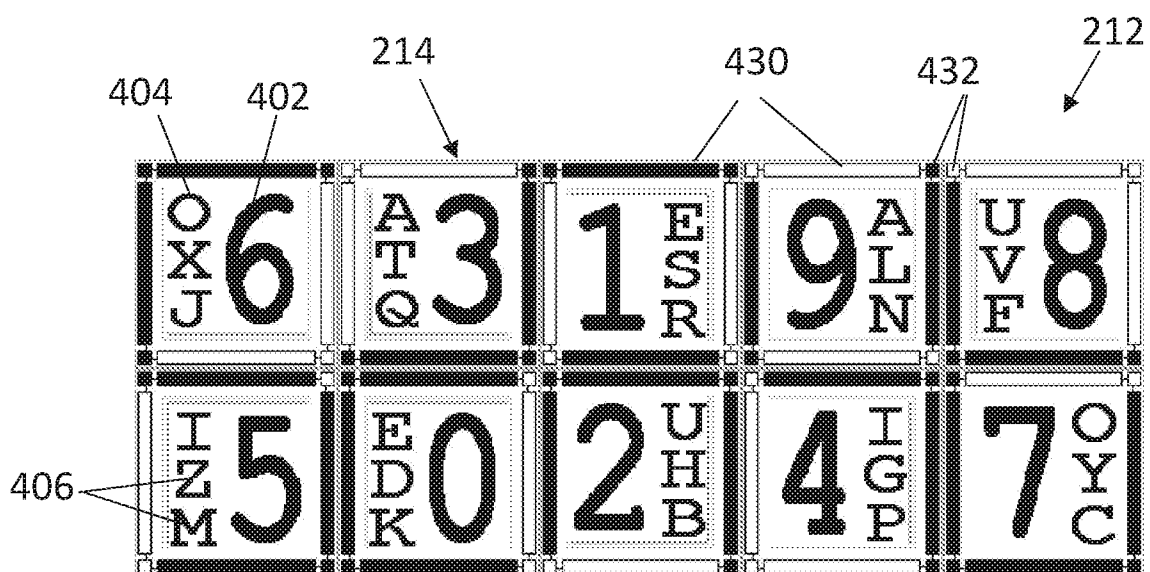
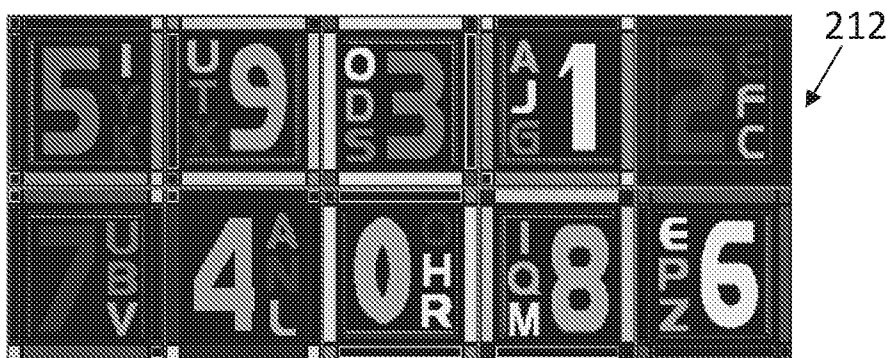
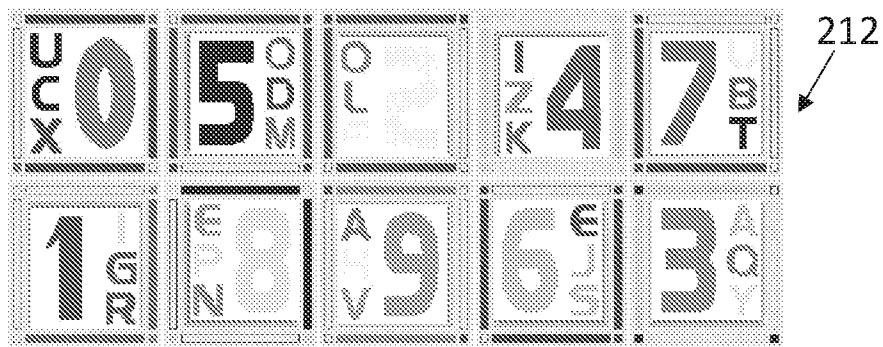
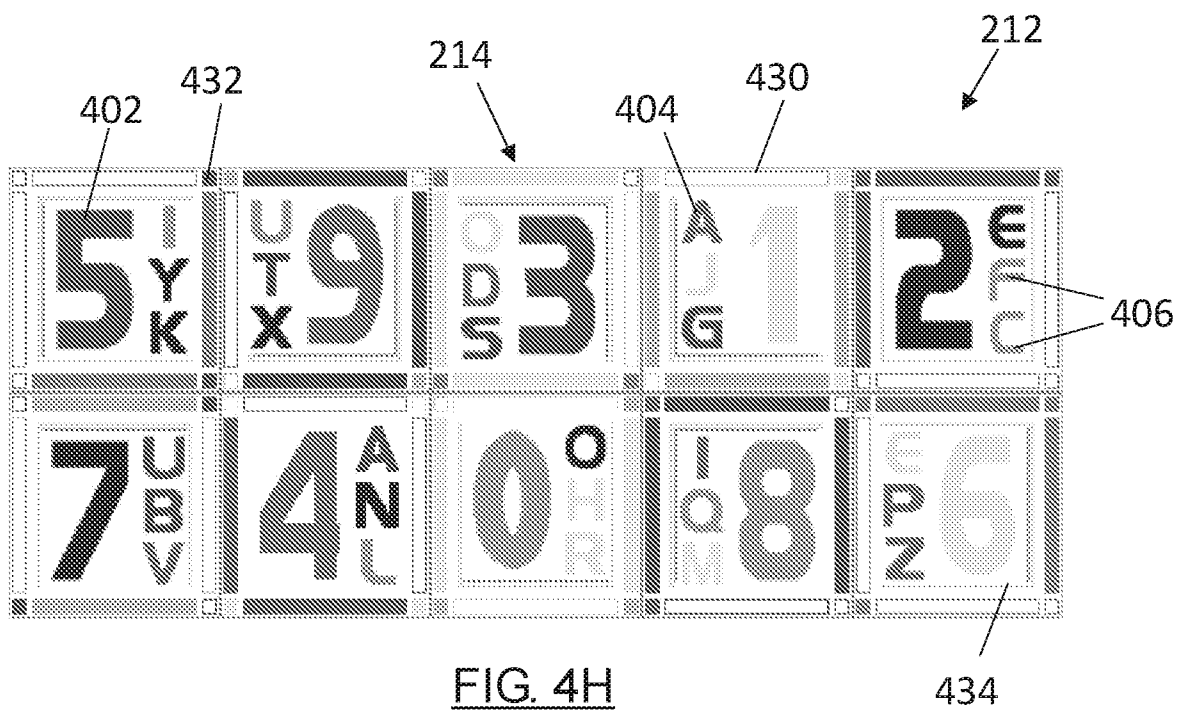


FIG. 4G



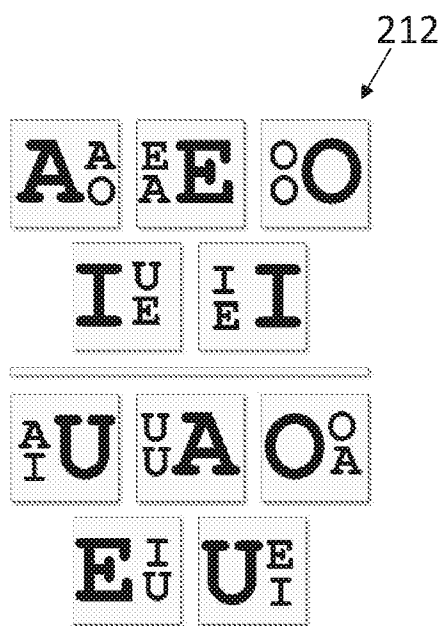


FIG. 4K

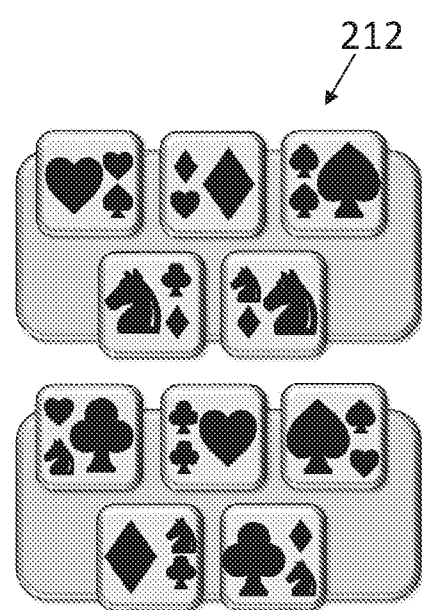


FIG. 4L

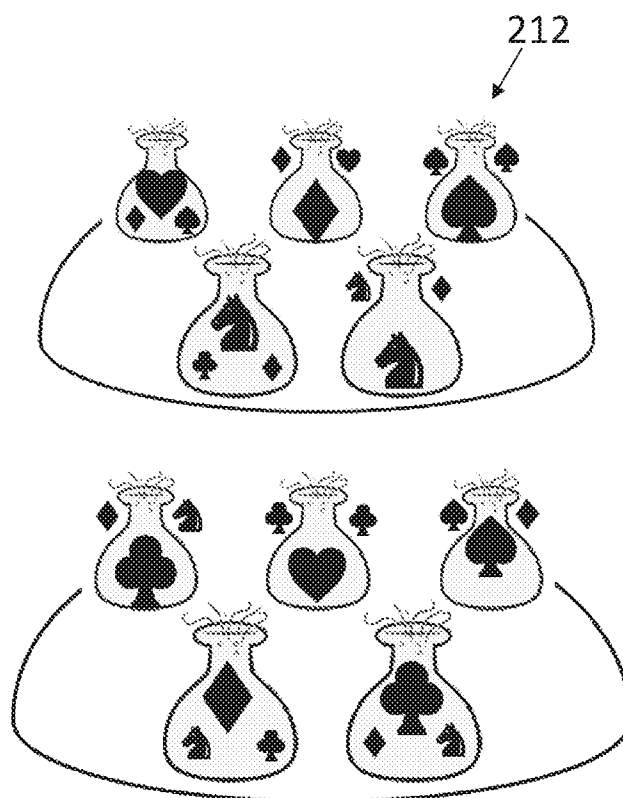


FIG. 4M

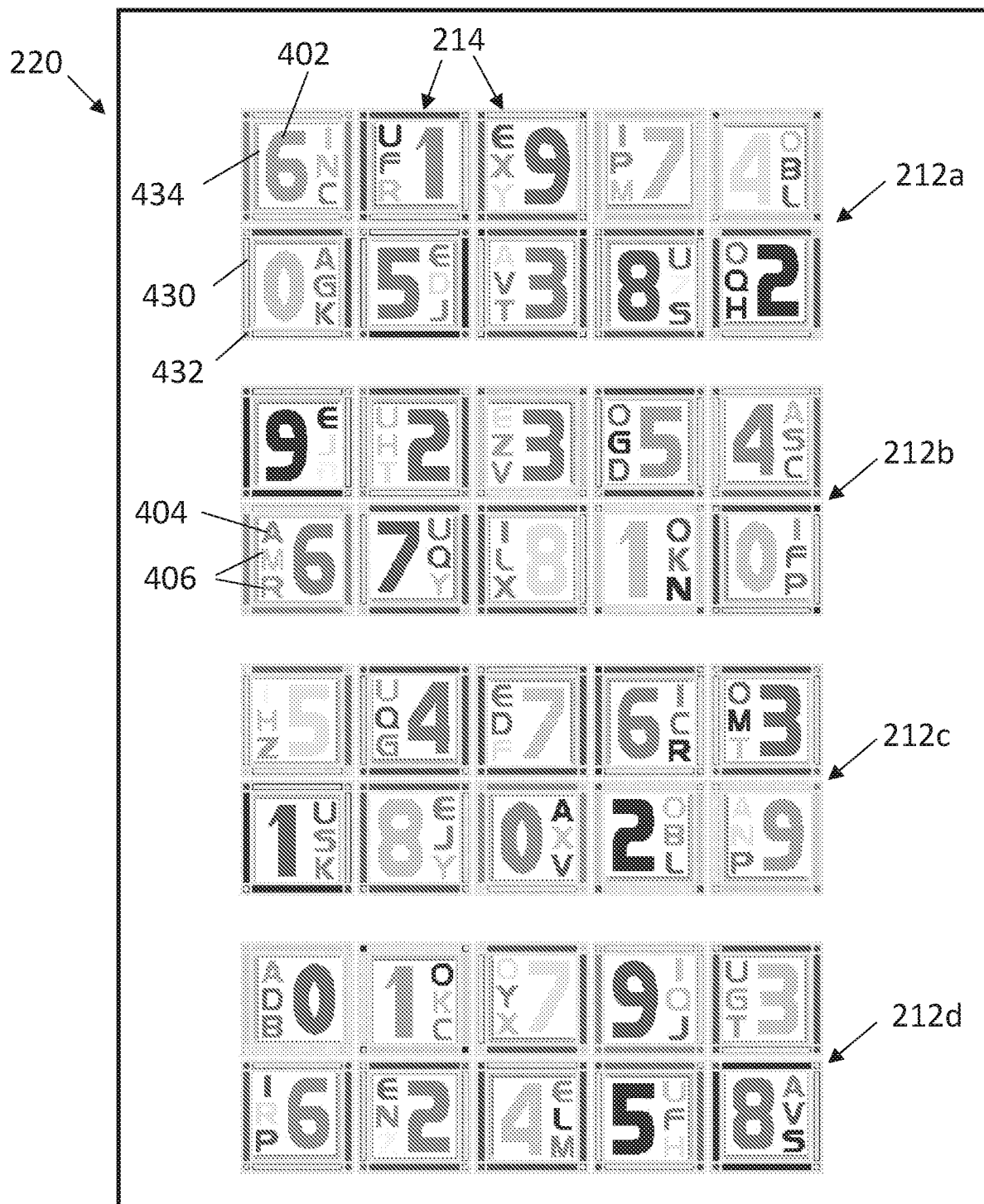


FIG. 5