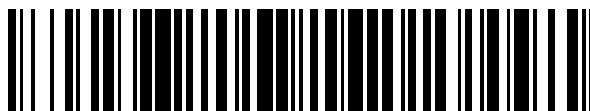


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 577 149**

51 Int. Cl.:

G06F 21/36 (2013.01)

G06F 21/31 (2013.01)

G07C 9/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **14.12.2012 E 12306587 (2)**

97 Fecha y número de publicación de la concesión europea: **23.03.2016 EP 2605167**

54 Título: **Sistema de seguridad de gesto privado/público y método de funcionamiento del mismo**

30 Prioridad:

15.12.2011 US 201161576256 P

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

13.07.2016

73 Titular/es:

**ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris , FR**

72 Inventor/es:

**ODESSKY, ADAM y
GAY, JULIAN**

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 577 149 T3

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

DESCRIPCIÓN

Sistema de seguridad de gesto privado/público y método de funcionamiento del mismo

5 Campo del sistema actual

El sistema actual se refiere a un sistema de acceso seguro basado en los gestos y, más específicamente, a un método basado en los gestos para generar y/o distribuir claves criptográficas privadas y/o públicas para cifrar y/o descifrar un contenido.

10 Antecedentes del sistema actual

Por lo general, los métodos de criptografía se usan para cifrar o bloquear los datos para formar texto cifrado y, posteriormente, descifrar o desbloquear el texto cifrado para obtener una copia de los datos originales. Un método de criptografía común se conoce como la criptografía de clave pública/privada (normalmente denominada criptografía de clave pública o simplemente PKC) y usa dos claves que pueden asociarse con un propietario: una primera clave (por ejemplo, una clave de cifrado o bloqueo) para bloquear o cifrar datos tales como los datos de texto sin formato que pueden usarse para formar un texto cifrado; y una segunda clave (por ejemplo, una clave de descifrado o desbloqueo) para desbloquear o descifrar el texto cifrado. Las claves normalmente incluyen unos datos de texto cifrado o de texto plano que denotan una cierta firma digital. Por lo general, una de las claves asociadas con los datos puede estar publicada o indicada públicamente de otro modo y la otra clave normalmente se retiene por una entidad que puede ser privada. La criptografía de clave pública permite que diferentes tipos de métodos de comunicaciones tales como un método de comunicaciones seguro y/o un método de comunicaciones de verificación de firma se realicen en función de si las claves de cifrado o descifrado son públicas o privadas. Por ejemplo, en un sistema de comunicaciones criptográfico seguro de clave pública/privada, la clave de cifrado es pública mientras que la clave de descifrado es privada. Sin embargo, en un sistema de comunicaciones criptográfico de verificación de firma, la clave de cifrado es privada y la clave de descifrado es pública (por ejemplo, véase, en.wikipedia.org/wiki/Public-key_cryptography).

30 Por desgracia, los métodos de cifrado convencionales se basan en unos métodos basados en texto para generar las claves de cifrado y un método de entrada de texto para comunicar las claves de cifrado. Por lo tanto, la generación y/o la comunicación de las claves por lo general requieren la interacción física del usuario con un teclado de un ordenador para generar y/o comunicar las claves de cifrado o descifrado antes de que pueda realizarse una comunicación segura del contenido (por ejemplo, archivos, directorios, etc.). Este proceso puede ser una carga y un inconveniente.

40 El documento "Method for access control via gestural verification gestual" del boletín de divulgación técnica de IBM, IBM Corp. (Thornwood), US, vol. 36, n.º 9B, 1 de septiembre de 1993, páginas 487/488 desvela un método de comunicaciones seguro, comprendiendo el método obtener una información de sensor de al menos un usuario, comprendiendo la información de sensor una o más de entre una información de imagen y una información de profundidad y reconocer al menos un gesto de acuerdo con la información de sensor de el al menos un usuario.

Sumario del sistema actual

45 De acuerdo con un aspecto del sistema actual, se desvela un sistema, un método, un dispositivo, un programa informático, una interfaz de usuario, y/o un aparato (en lo sucesivo en el presente documento, cada uno de los cuales denominados comúnmente como un sistema, a menos que el contexto indique lo contrario en aras de la claridad) para generar y/o distribuir las claves de cifrado privadas y/o públicas, de acuerdo con un enfoque basado en los gestos. En consecuencia, un usuario puede producir y/o distribuir una o más de las claves de cifrado privadas y/o públicas usando unos métodos basados en los gestos. Además, las realizaciones del sistema actual pueden autorizar el acceso a recursos tales como aplicaciones, directorios, y/o contenidos (por ejemplo, archivos, etc.) de acuerdo con los gestos privados y/o públicos formados por uno o más usuarios. Por otra parte, el sistema puede proporcionar una interfaz de usuario natural (NUI) para que un usuario interactúe usando unas entradas basadas en el movimiento tales como los gestos y similares.

55 De acuerdo con las realizaciones del sistema actual, se desvela un método de comunicaciones seguro, pudiendo el método incluir unas acciones que se realizan mediante un procesador, pudiendo las acciones incluir: obtener una información de sensor de al menos un usuario, comprendiendo la información de sensor una o más de entre la información de imagen y la información de profundidad; reconocer al menos un gesto de acuerdo con la información de sensor del al menos un usuario; determinar si cada uno de los al menos un gesto reconocido es un gesto público o un gesto privado de acuerdo con una zona en la que se ha realizado el gesto, seleccionándose la zona de una pluralidad de zonas; y autorizar el acceso a un recurso cuando se determina que el al menos un gesto está determinado para ser el gesto público o el gesto privado.

65 El método puede incluir además una acción para determinar las localizaciones de cada una de la una pluralidad de zonas en relación con una estructura corporal del al menos un usuario, en el que cada zona de la pluralidad de

zonas es una zona pública o una zona privada. Además, el método puede incluir una acción para determinar que el primer gesto es un gesto público cuando se determina que el primer gesto se ha realizado en la zona pública. Por otra parte, el método puede incluir una acción para determinar que el segundo gesto es un gesto privado cuando se determina que el segundo gesto se ha realizado en la zona privada. Además, la acción para autorizar el acceso al recurso puede incluir una acción para proporcionar una llamada de video segura o una acción para autorizar a el al menos un usuario a acceder al recurso, el recurso puede incluir una base de datos, una aplicación de ordenador, o un contenido. También se prevé que el método pueda incluir una acción para obtener al menos una de entre una clave de cifrado pública correspondiente al gesto público y una clave de cifrado privada correspondiente al gesto privado en respuesta a el al menos un gesto reconocido. Por otra parte, el método puede incluir unas acciones de asociar la clave de cifrado pública con el gesto público y asociar la clave de cifrado privada con el gesto privado.

De acuerdo con otro aspecto más del sistema actual, se desvela un sistema de comunicaciones seguro que incluye un procesador que: obtiene una información de sensor de al menos un usuario, incluyendo la información de sensor una o más de entre una información de imagen y una información de profundidad; reconoce los gestos primero y segundo de acuerdo con la información de sensor del al menos un usuario; determina si el primer gesto incluye un gesto público; determina si el segundo gesto incluye un gesto privado; y/o autoriza el acceso a un recurso cuando se determina que el primer gesto incluye un gesto público y el segundo gesto incluye un gesto privado.

Se prevé además que el procesador pueda determinar las localizaciones de las zonas públicas y privadas en relación con una estructura corporal del al menos un usuario; y/o puede determinar que el primer gesto es un gesto público cuando se determina que el primer gesto se ha realizado en la zona pública. Del mismo modo, se prevé que el procesador pueda determinar además que el segundo gesto es un gesto privado cuando se determina que el segundo gesto se ha realizado en la zona privada. También se prevé que para autorizar el acceso al recurso, el procesador puede autorizar una llamada de video segura y/o puede autorizar a el al menos un usuario a acceder a un recurso que incluye una base de datos, una aplicación de ordenador, o un contenido. Se prevé además que el procesador pueda obtener además al menos una de entre una clave de cifrado pública correspondiente al gesto público y una clave de cifrado privada correspondiente al gesto privado en respuesta a el al menos un gesto reconocido. Por otra parte, se prevé que el procesador pueda asociar la clave de cifrado pública con el gesto público y asociar la clave de cifrado privada con el gesto privado, durante, por ejemplo, un proceso de formación realizado por una aplicación de formación.

De acuerdo con un aspecto adicional más del sistema actual se desvela un programa informático almacenado en un medio de memoria no transitoria legible por ordenador, pudiendo el programa informático configurarse para realizar un proceso de comunicaciones seguro, pudiendo el programa informático incluir una parte de programa configurada para: obtener una información de sensor de al menos un usuario, comprendiendo la información de sensor una o más de entre una información de imagen y una información de profundidad; reconocer al menos un gesto de acuerdo con la información de sensor del al menos un usuario; determinar si cada uno de los al menos un gesto reconocido es un gesto público o un gesto privado de acuerdo con una zona en la que se ha realizado el gesto, seleccionándose la zona de una pluralidad de zonas; y autorizar el acceso a un recurso cuando se determina que el al menos un gesto está determinado para ser el gesto público o el gesto privado.

Se prevé además que la parte de programa pueda configurarse para determinar las localizaciones de cada una de la una pluralidad de zonas en relación con una estructura corporal del al menos un usuario, en las que cada zona de la pluralidad de zonas es una zona pública o una zona privada. Adicionalmente, la parte del programa puede configurarse además para determinar que el primer gesto es un gesto público cuando se determina que el primer gesto se ha realizado en la zona pública. Por otra parte, la parte del programa puede configurarse además para determinar que el segundo gesto es un gesto privado cuando se determina que el segundo gesto se ha realizado en la zona privada. También se prevé que la parte de programa pueda configurarse además para autorizar una llamada de video segura o autorizar a el al menos un usuario a acceder a un recurso que incluye una base de datos, una aplicación de ordenador, o un contenido, cuando la parte de programa autoriza el acceso al recurso. Se prevé además que la parte de programa pueda configurarse adicionalmente para obtener al menos una de entre una clave de cifrado pública correspondiente al gesto público y una clave de cifrado privada correspondiente al gesto privado en respuesta a el al menos un gesto reconocido.

Breve descripción de los dibujos

La invención se explica con más detalle, y a modo de ejemplo, con referencia a los dibujos adjuntos en los que:

La figura 1 muestra una parte de un sistema de acuerdo con las realizaciones del sistema actual;

La figura 2A muestra una captura de pantalla de un usuario que introduce un gesto público de acuerdo con las realizaciones del sistema actual;

La figura 2B muestra una captura de pantalla del usuario que introduce un gesto privado de acuerdo con las realizaciones del sistema actual;

La figura 2C que muestra una captura de pantalla del usuario que introduce al mismo tiempo un gesto público y un gesto privado;

La figura 3 muestra un diagrama de flujo que ilustra un proceso de acuerdo con las realizaciones del sistema actual;

La figura 4 muestra unas capturas de pantalla de las estaciones móviles que reproducen una llamada de video entre dos usuarios de acuerdo con las realizaciones del sistema actual; y

La figura 5 muestra una parte de un sistema de acuerdo con las realizaciones del sistema actual.

5 Descripción detallada del sistema actual

Las siguientes son unas descripciones de unas realizaciones ilustrativas que cuando se toman junto con los siguientes dibujos demostrarán las características indicadas y ventajas indicadas anteriormente, así como otras adicionales. En la siguiente descripción, con fines de explicación más que de limitación, se exponen los detalles ilustrativos tales como la arquitectura, las interfaces, las técnicas, los atributos de elementos, etc. Sin embargo, será evidente para los expertos en la materia que otras realizaciones que se apartan de estos detalles deberían entenderse que aún están dentro del alcance de las reivindicaciones adjuntas. Por otra parte, con el fin de la claridad, se omiten las descripciones detalladas de los dispositivos, circuitos, herramientas, técnicas y métodos bien conocidos para no oscurecer la descripción del sistema actual. Debería entenderse expresamente que los dibujos se incluyen con fines ilustrativos y no representan el alcance del sistema actual. En los dibujos adjuntos, los números de referencia similares en diferentes dibujos pueden designar elementos similares.

El término reproducción y las formas del mismo como se usan en el presente documento se refieren a proporcionar el contenido, tal como unos medios digitales que pueden incluir, por ejemplo, información de imagen, contenidos, mensajes, información de estado, configuraciones, información de audio, información audiovisual, información de vídeo, datos, archivos, etc., de tal manera que pueden percibirse por al menos un sentido de usuario, tal como un sentido de la vista y/o un sentido del oído. Por ejemplo, el sistema actual puede reproducir una interfaz de usuario (UI) en un dispositivo de visualización de tal manera que pueda verse e interactuarse por un usuario.

La figura 1 muestra una parte de un sistema 100 de acuerdo con las realizaciones del sistema actual. El sistema 100 puede incluir un procesador 104 acoplado a uno o más de los sensores 102 y una memoria 106. Los sensores 102 pueden incluir uno o más de entre una cámara (por ejemplo, una cámara de vídeo, etc.), un micrófono (por ejemplo, para grabar una voz de un usuario, etc.), un sensor de profundidad y/o de distancia (pudiendo denominarse ambos en lo sucesivo en el presente documento como un sensor de profundidad a menos que el contexto indique otra cosa por el bien de la claridad, por ejemplo, sensores de infrarrojos (IR), sensores de microondas, etc.), un sensor de condición ambiental (por ejemplo, un termómetro, un barómetro, un higrómetro, un sensor de precipitación, etc.), y/o sensores biométricos (por ejemplo, un lector de huellas digitales, un lector de iris, etc.). Los sensores 102 pueden detectar un usuario 101 y capturar una información de imagen (por ejemplo, una información de fotografía, una información de imagen de vídeo, etc.) del usuario 101, y/o una información de profundidad (y/o distancia) relacionada con una o más partes del usuario 101 y/o los entornos y la forma del usuario correspondiente a la información de sensor (SI). La SI puede transmitirse al procesador 104 para su posterior procesamiento, tal como un análisis de acuerdo con las realizaciones del sistema actual. Los sensores 102 pueden incluir unos sensores de detección de movimiento convencionales, tales como los sensores Kinect™ o de tipo Kinect™ que pueden proporcionar una entrada sensorial para proporcionar una NUI para que el usuario interactúe. Además, los sensores 102 pueden determinar la información de condición ambiental (por ejemplo, temperatura, presión, humedad, precipitación, etc.) y/o la información de localización (por ejemplo, la localización geográfica, etc.) en la localización de los sensores 102 e incluir esta información en la SI. Por otra parte, los sensores biométricos pueden capturar la información biométrica relacionada con el usuario (por ejemplo, tal como un escaneo del iris) e incluir esta información en la SI.

De acuerdo con las realizaciones del sistema actual, el procesador 104 puede controlar el funcionamiento global del sistema 100. Después de recibir la SI, el procesador 104 puede analizar la SI usando un método o métodos de análisis de datos adecuado (por ejemplo, análisis de imágenes, procesamiento de señales digitales (DSP), etc.) para identificar el usuario 101, seguir una estructura corporal del usuario 101, determinar si el usuario 101 ha realizado cualquier gesto, y/o para identificar estos gestos si se realizan. Por ejemplo, el procesador 104 puede identificar al usuario 101 usando el reconocimiento de imágenes, el reconocimiento de voz, los datos biométricos, etc. Además, el procesador 104 puede obtener una información de usuario de la memoria 106 y determinar si un usuario identificado es un usuario autorizado. De acuerdo con las realizaciones del sistema actual, un usuario autorizado es un usuario que se reconoce y se autoriza para una acción determinada (tal como proporcionando uno o más de entre un gesto público y/o privado como se describe adicionalmente en el presente documento) basándose en los datos de usuario. Por ejemplo, los datos de usuario pueden almacenarse en la memoria 106 y/o pueden generarse por el sistema 100 tal como una información de cuenta de usuario, una información de gestos pre-almacenada (PGI), una SI, etc.

De acuerdo con las realizaciones del sistema actual, los gestos pueden incluir los gestos públicos o privados y pueden introducirse individualmente, de manera secuencial y/o en serie. El sistema actual discrimina y reconoce tanto los gestos públicos como los privados. Como se usa en el presente documento, un gesto público puede ser un gesto realizado por un usuario (por ejemplo, un usuario autorizado) que se hace dentro de una zona que está determinada por el sistema para ser una zona pública. Como se usa en el presente documento, un gesto privado puede ser un gesto realizado por un usuario (por ejemplo, un usuario autorizado) que se hace dentro de una zona que está determinada por el sistema para ser una zona privada. De acuerdo con las realizaciones del sistema actual,

el sistema actual reconoce los gestos públicos y privados y discrimina su respuesta basándose en este reconocimiento, así como de si un usuario está reconocido y/o autorizado.

5 Además, la memoria 106 puede almacenar la información de gesto (por ejemplo, los gestos predeterminados) que
 10 corresponde a los gestos que autorizan el acceso a unos recursos determinados, un grupo de recursos, etc. En otras
 palabras, el procesador 104 puede utilizar los gestos almacenados en la memoria 106 para determinar si un gesto
 proporcionado por un usuario es el gesto correcto para obtener el acceso al uno o más recursos. Además, la
 15 memoria 106 puede almacenar una información que identifique si el gesto correcto es un gesto público o privado. De
 este modo, para obtener el acceso al recurso, el usuario necesita proporcionar el gesto predeterminado dentro de la
 zona apropiada. Por ejemplo, un gesto determinado proporcionado en la zona privada puede obtener el acceso del
 usuario al recurso, mientras que el mismo gesto determinado proporcionado en la zona pública puede y/o no puede
 proporcionar el acceso a un recurso determinado diferente. Además, garantizando que el gesto se proporciona por
 un usuario autorizado, incluso los gestos adecuados pueden rechazarse cuando no se proporcionan por un usuario
 autorizado. Como hay multitud de gestos y secuencias de gestos disponibles, la seguridad de los recursos puede
 garantizarse mientras que se simplifica en gran medida la interacción del usuario con el recurso.

20 Por ejemplo, durante una videoconferencia, puede suponerse que los gestos públicos pueden verse por otros (por
 ejemplo, no son seguros) y los gestos privados no deberían verse por otras personas (por ejemplo, son seguros).
 Por lo tanto, de acuerdo con las realizaciones del sistema actual, los gestos privados del usuario 101 pueden
 capturarse por los sensores 102, pero no pueden transmitirse (por ejemplo, a otros participantes durante una
 llamada de videoconferencia) de manera que permanecen seguros. Por ejemplo, al participar en una llamada de
 25 video, el usuario 101 (por ejemplo, una persona que llama en el presente ejemplo) puede formar un gesto público
 que puede capturarse por una cámara de los sensores 102 y, posteriormente, transmitirse a los otros participantes
 de la llamada (por ejemplo, a un destinatario de la llamada). Sin embargo, si el usuario 101 forma un gesto privado,
 aunque puede capturarse por los sensores 102, no debería transmitirse a los otros participantes de la llamada.
 Naturalmente, como puede apreciarse fácilmente, de acuerdo con las realizaciones del sistema actual, los gestos
 reconocidos, ya sean públicos o privados pueden también no transmitirse, sin embargo, pueden utilizarse por el
 sistema actual, (por ejemplo, para el descifrado/cifrado del texto cifrado).

30 De acuerdo con las realizaciones del sistema actual, el sistema 100 puede definir unas zonas públicas y privadas
 como unas zonas de dos o tres dimensiones en relación con una estructura corporal del usuario 101 en las que los
 gestos pueden realizarse por el usuario 101. Cada zona puede ocupar un espacio de dos o tres dimensiones y
 puede localizarse cerca del cuerpo del usuario 101 de tal manera que el usuario 101 puede realizar los gestos
 dentro de una zona correspondiente. El sistema puede formar una zona pública de tal manera que sea más grande
 35 que una zona privada correspondiente. Además, el sistema puede localizar una zona privada cerca de un centro de
 una estructura corporal de un usuario y delante del usuario en oposición a una zona pública que puede colocarse
 lejos del cuerpo del usuario.

40 Por consiguiente, el procesador 104 puede analizar la SI para determinar la localización así como una forma y/o un
 tamaño de cada una de las zonas públicas y privadas en relación con una estructura corporal de un usuario 101 en
 el espacio de dos o tres dimensiones. De acuerdo con las realizaciones del sistema actual, las localizaciones así
 como una forma y/o un tamaño de cada una de las zonas públicas y privadas pueden estar en relación con un objeto
 y/o una persona que no sea el usuario 101. Por ejemplo, una localización, una forma y/o un tamaño de una zona
 45 privada puede ajustarse en relación con una persona que se encuentre delante de los sensores 102 que no es el
 usuario que sin embargo tiene una visión dentro del área del sensor. En estas realizaciones, el sistema puede
 ajustar las zonas públicas y/o privadas en relación con la persona. Por ejemplo, la zona privada puede ajustarse por
 el sistema de tal manera que corresponde a un área alrededor del cuerpo del usuario 101, que no es visible por la
 persona. Este ajuste de las zonas públicas/privadas también puede proporcionarse en relación con unos objetos
 tales como ventanas, puertas, espejos, etc., dentro de un área alrededor del usuario 101 para garantizar que los
 50 gestos, por ejemplo, proporcionados dentro de la zona privada, no son visibles por otras personas que no sea el
 usuario 101 debido a estos objetos.

Además, el sistema 100 puede recortar la información de imagen del usuario 101, que se capta por los sensores 102
 de tal manera que la información de imagen dentro de la zona privada se mantiene segura y no se transmite a otros
 55 tal como otros participantes de una llamada de video. El procesador 104 puede definir además las zonas públicas
 y/o privadas en el espacio usando un sistema de coordenadas adecuado, tal como un sistema de coordenadas
 cartesiano que usa los ejes x, y, y/o z mínimos y máximos. Del mismo modo, el procesador 104 puede determinar
 una localización de la estructura corporal del usuario y definir esta localización usando los ejes x, y, y/o z mínimos y
 máximos. Aunque un sistema de dos zonas se describe por el bien de la claridad, se ha previsto que el sistema
 60 pueda configurarse con otros números de zonas tales como un sistema de tres o cuatro zonas, etc. Además, aunque
 en el presente documento se describen zonas continuas, se prevé que en otras realizaciones, las zonas puedan ser
 discontinuas, si se desea.

65 Ejemplos de gestos públicos y privados introducidos por un usuario se describen con referencia a las figuras 2A y
 2B, respectivamente. La figura 2A muestra una captura de pantalla 200A de un usuario 201 que introduce un gesto
 público como se muestra por la estructura de gesto 207 de acuerdo con las realizaciones del sistema actual. Los

sensores del sistema actual pueden capturar una información de imagen y/o de profundidad del usuario 201 y el sistema puede realizar un seguimiento de, por ejemplo, una estructura corporal del usuario usando esta información. Posteriormente, el sistema puede definir una zona privada 203 y una zona pública 205 con relación a este usuario, con relación a otras personas que puedan estar alrededor del usuario (por ejemplo, dentro de una zona que puede detectarse por el sensor) y/o con relación a unos objetos (por ejemplo, ventanas, puertas, espejos, etc.) que pueden estar alrededor del usuario. De acuerdo con las realizaciones del sistema actual, una imagen del usuario 201 puede reproducirse por conveniencia del usuario 201. Además, si se desea, la zona privada 203 y/o la zona pública 205 pueden superponerse sobre esta imagen (por ejemplo, en tiempo real). Además, el sistema puede resaltar y/o usar cajas de texto (por ejemplo, véanse, las cajas 213 y 215) para resaltar y/o de otra manera enfatizar la localización de las zonas, por ejemplo, reproducidas superpuestas en una pantalla visible para el usuario 201 (por ejemplo, véase, la figura 5, el dispositivo de reproducción 530) para conveniencia del usuario 201. Además, el sistema puede resaltar otras personas, objetos, etc., alrededor del usuario 201 que afectan a la determinación de una localización, una forma y/o un tamaño de estas zonas. Por ejemplo, el sistema puede resaltar y/o de otra manera enfatizar la localización de la persona y una puerta alrededor del usuario que afecta a la localización, la forma y/o el tamaño de la zona privada. De acuerdo con las realizaciones del sistema actual, esta es una manera de que el usuario 201 pueda ajustar fácilmente la posición de su cuerpo para afectar a la posición, la forma y/o el tamaño determinados de la zona privada. Por ejemplo, puede ser que, debido a las posiciones de la persona y de la puerta en relación con el usuario 201, la localización, la forma y/o el tamaño de la zona privada sea un inconveniente para el usuario o que no existe ninguna zona privada adecuada. En este ejemplo, el usuario puede ajustar la posición de su cuerpo, por ejemplo, dando la espalda a la persona y/o a la puerta de manera que se establece una zona privada más adecuada. Además, el usuario 201 puede cerrar la puerta, cambiar la posición de la persona, reposicionarse el mismo, etc., de tal manera que el posicionamiento de la puerta/persona no tiene un efecto adverso (por ejemplo, ya no afecta tal como cerrando la puerta) en la determinación de la zona privada.

Cuando se ha identificado un gesto, el sistema puede resaltar el gesto usando cualquier método adecuado, tal como usando la estructura de gesto 207, si se desea. Además, el sistema puede superponer la estructura de gesto 207 sobre la información de imagen del usuario 201. Además, con respecto a los gestos, el sistema puede identificar los gestos por el tipo. Por ejemplo, en el presente ejemplo, el sistema puede identificar el gesto como una “onda de mano abierta pública”. Para identificar los gestos, el sistema puede referirse a una biblioteca de gestos almacenada en una memoria del sistema y que puede incluir una identificación de los gestos. Además, el usuario 201 puede entrenar el sistema para los gestos específicos para el usuario y/o el recurso y almacenar esto en la biblioteca de gestos en asociación con el usuario.

La figura 2B muestra una captura de pantalla 200B del usuario 201 introduciendo un gesto privado 209 de acuerdo con las realizaciones del sistema actual. La figura 2B es similar a la figura 2A, sin embargo, el usuario 201 está realizando un gesto privado. En consecuencia, el sistema puede detectar y resaltar este gesto usando cualquier método adecuado, tal como usando un estructura de gesto 209, si se desea. El sistema puede identificar además el gesto actual como un “signo V privado”. De acuerdo con las realizaciones del sistema actual, un mismo gesto (por ejemplo, el signo V) se interpretará de manera diferente por el sistema actual basándose en si un gesto se reconoce a partir de una zona pública o privada.

En los ejemplos mostrados en las figuras 2A y 2B, los gestos públicos y privados se introducen por separado el uno del otro (por ejemplo, uno a la vez) y, por lo tanto, pueden considerarse unos gestos secuenciales. Se prevé además que una secuencia de los gestos primero y segundo (es decir, los gestos que están reconocidos) pueda compararse con un orden de secuencia predefinido o una pluralidad de diferentes órdenes de secuencia. En consecuencia, si se encuentra que el orden de los gestos no está de acuerdo con el de la configuración de la secuencia predefinida o con una de las configuraciones de secuencia predefinidas, el usuario no será autorizado a realizar una acción, tal como descifrar un documento o de otra manera proporcionársele el acceso a un recurso. Por lo tanto, la acción para autorizar el acceso a un recurso puede depender de que uno o más usuarios proporcionen los gestos en una secuencia correcta.

Sin embargo, los gestos también pueden introducirse simultáneamente, como se ilustra en la figura 2C que muestra una captura de pantalla 200C del usuario introduciendo al mismo tiempo un gesto público (por ejemplo, véase, el gesto 207S) y un gesto privado (por ejemplo, véase, la estructura de gesto 209S). De manera similar al gesto mostrado en la figura 2A, el gesto público es una “onda de mano abierta”. Además, el gesto privado es similar al gesto de la figura 2B, un “signo V”. En estas realizaciones, la acción para autorizar el acceso a un recurso puede depender de uno o más usuarios que proporcionan los gestos correctos sustancialmente de manera simultánea. En otras realizaciones, la acción para autorizar el acceso a un recurso puede depender de uno o más usuarios que proporcionan los gestos correctos sin tener en cuenta un tiempo relativo para proporcionar cada uno de los gestos correctos.

De acuerdo con las realizaciones del sistema actual, cuando se están reconociendo los gestos secuenciales, el sistema puede determinar cuándo un gesto se ha recibido y/o se hace por ejemplo analizando la información de sello de tiempo que puede incluirse en la SI. De acuerdo con las realizaciones del sistema actual, la secuenciación de las imágenes puede utilizarse para determinar un orden de los gestos reconocidos. Por ejemplo, una imagen (por ejemplo, de un gesto privado) que sigue a otra imagen (por ejemplo, de un gesto público) puede determinarse para

seguir en la secuencia de los gestos reconocidos. El sistema puede utilizar un periodo de tiempo de gestos durante el cual los gestos pueden seguirse entre sí. En estas realizaciones, cuando transcurra el periodo de tiempo de gestos, los gestos realizados por el usuario pueden ignorarse y el usuario puede tener que volver a introducir un par de gestos (por ejemplo, puede incluir los gestos público y privado) de acuerdo con una secuencia predeterminada, de manera que puede configurarse por el sistema, el usuario, o predeterminarse de otro modo (por ejemplo, un gesto privado a continuación uno público dentro de tres segundos, etc.).

Haciendo referencia de nuevo a los gestos, pueden realizarse en las zonas públicas o privadas, y pueden incluir un movimiento o contorsión del cuerpo, incluyendo los movimientos de las extremidades (por ejemplo, el movimiento de las manos, brazos, pies), los movimientos faciales (por ejemplo, cejas, ojos, boca, orejas, sonrisas, etc.), y otros movimientos del cuerpo. Los gestos pueden combinarse también con unos métodos de autenticación tales como las contraseñas de texto, reconocimientos de voz, datos biométricos, etc., con el fin de que se produzca la autenticación. Así, por ejemplo, puede solicitarse a un usuario que introduzca un patrón de voz para un reconocimiento de voz antes de que el sistema pueda aceptar los gestos, por ejemplo, para autorizar el acceso a un recurso.

Al introducir un gesto en el sistema, el usuario puede estar de pie en un campo de visión de los sensores del sistema, tales como los sensores de cámara y/o de profundidad que pueden capturar la información de imagen, la información de profundidad de usuario y/o de las personas y/o de los objetos que rodean al usuario. Posteriormente, esta información puede analizarse por el sistema para detectar los gestos, determinar las zonas públicas y/o privadas y/o para determinar si los gestos se realizan dentro de una zona especificada (por ejemplo, una zona pública o una zona privada en el presente ejemplo). Se prevé además que el sistema pueda reproducir una solicitud para que el usuario realice un gesto tal como un gesto público o un gesto privado. En algunas realizaciones, un gesto puede tener una clave de cifrado asociada que puede recuperarse en respuesta a un gesto reconocido y puede usarse como una clave de cifrado/descifrado. En la misma o en otras realizaciones, un gesto puede tener una clave de gesto asociada que puede utilizarse directamente.

De acuerdo con las realizaciones del sistema actual, estas claves pueden, en general, denominarse como una clave pública o una clave privada en función de si se corresponden con un gesto público o privado. Así, por ejemplo, un gesto privado puede tener una clave privada asociada y un gesto público puede tener una clave pública asociada. En consecuencia, cuando se detecta que el usuario ha introducido un gesto privado, el proceso puede obtener una clave privada asociada. De una manera similar, cuando se detecta que el usuario ha introducido un gesto público, el proceso puede obtener una clave pública asociada. Las claves de cifrado asociadas pueden almacenarse en la memoria del sistema o pueden generarse en respuesta a una entrada de gestos correcta. Tras la finalización con éxito del gesto(s), el sistema puede aceptar o rechazar las claves de cifrado correspondientes.

La figura 3 muestra un diagrama de flujo que ilustra un proceso 300 de acuerdo con las realizaciones del sistema actual. El proceso 300 puede realizarse usando uno o más ordenadores que se comunican a través de una red. El proceso 300 puede incluir una o más de las siguientes acciones. Además, una o más de estas acciones pueden combinarse y/o separarse en sub-acciones, si se desea. Durante el proceso 300 solamente se trata un único usuario en aras de la claridad. Sin embargo, de acuerdo con las realizaciones del sistema actual, las acciones operativas del proceso 300 pueden realizarse por una pluralidad de usuarios. Por consiguiente, el proceso puede analizar cada usuario y/o una interacción entre los usuarios para determinar quién puede formar gestos en la interacción entre dos o más usuarios.

En funcionamiento, el proceso 300 puede comenzar durante la acción 301 y a continuación proceder en la acción 303. Durante la acción 303, el proceso puede obtener la información de sensor (SI) de un usuario de uno o más sensores del sistema. La información de sensor puede transmitirse en respuesta a una solicitud del proceso o puede promoverse cuando, por ejemplo, se detecta al usuario. Sin embargo, también se prevé que la información de sensor pueda recogerse cuando, por ejemplo, el usuario realiza ciertas acciones, tales como cuando el usuario inicia una aplicación determinada (por ejemplo, una aplicación de llamadas de video, una aplicación de puerta de entrada de seguridad, etc.), intenta de acceder a un directorio o archivo, etc. Como se ha tratado en otra parte, la información de sensor puede incluir una información de imagen y una información de profundidad del usuario. Sin embargo, otra información tal como el tiempo (por ejemplo, de captura), la localización (por ejemplo, geofísica, etc.), la voz, atmosférica, etc., pueden incluirse en la información de sensor, si se desea. Después de completar la acción 303, el proceso puede continuar en la acción 305.

Durante la acción 305, el proceso puede realizar un seguimiento de una estructura corporal del usuario. Por consiguiente, el proceso puede analizar la información de imagen y/o la información de profundidad del usuario y determinar la estructura corporal del usuario en tiempo real. La estructura corporal del usuario puede representarse como un espacio de dos o tres dimensiones (por ejemplo, un área o un volumen) colocado en relación con el cuerpo del usuario. Además, el proceso puede determinar (por ejemplo, de acuerdo con la información de imagen del usuario, etc.) una orientación del usuario (por ejemplo, frente a la cámara, etc.). Después de completar la acción 305, el proceso puede continuar en la acción 307.

5 Durante la acción 307, el proceso puede definir unas zonas de acuerdo con la estructura corporal del usuario. Así, por ejemplo, el sistema puede definir las zonas públicas y privadas como un espacio de dos o tres dimensiones en relación con la estructura corporal del usuario. En el presente ejemplo, las zonas públicas y privadas son excluyentes entre sí. Por consiguiente, el proceso puede tener en cuenta un campo de visión de una cámara que puede proporcionar una información de imagen del usuario a transmitirse durante, por ejemplo, una llamada de vídeo y ajustar la localización, la forma y/o el tamaño de las zonas públicas y privadas en consecuencia. Con respecto a la zona pública, esta zona puede definirse como un espacio colocado alrededor de una estructura corporal del usuario y que no está localizado de la zona privada (por ejemplo, véase, la estructura 205, figuras 2A y 2B). Además, la zona privada puede definirse como un espacio colocado delante de una estructura corporal de un usuario.

15 Se prevé que puedan definirse también otras áreas y/o zonas y que puedan definirse en relación con la estructura corporal del usuario basándose en un entorno del usuario y/o en unas aplicaciones usadas por el usuario. Por ejemplo, cuando se participa en una llamada de vídeo, la zona pública puede extenderse desde el torso del usuario por encima de la zona privada (por ejemplo, véase, la figura 4, 400C y 400D). En consecuencia, el proceso puede recortar las imágenes del usuario que se transmiten (por ejemplo, durante una llamada de vídeo, etc.) a otros participantes de la llamada de acuerdo con la localización, la forma y/o el tamaño de las zonas públicas y privadas. Además, las localizaciones, la forma y/o el tamaño de cada una de las zonas públicas y privadas pueden estar en relación con un objeto y/o una persona alrededor del usuario. Después de completar la acción 307, el proceso puede continuar en la acción 309.

25 Durante la acción 309, el proceso puede determinar si el usuario ha realizado al menos un gesto, tal como determinando que el usuario ha realizado un gesto reconocido (por ejemplo, después de la captura y el análisis de una o más imágenes capturadas). En un caso en el que se determina que el usuario ha realizado al menos un gesto, el proceso puede continuar en la acción 313. Sin embargo, si se determina que el usuario no ha realizado al menos un gesto, el proceso puede repetir la acción 309 y esperar una entrada de uno o más gestos por el usuario que se corresponda con un gesto reconocido.

30 Durante la acción 313, el proceso puede determinar una zona en la que se ha realizado al menos un gesto. En consecuencia, si se determina que la zona en la que se ha realizado el al menos un gesto es una zona privada, el proceso puede determinar que el al menos un gesto es un gesto privado y continuar en la acción 315. Del mismo modo, si se determina que la zona en la que se ha realizado el al menos un gesto es una zona pública, el proceso puede determinar que el al menos un gesto es un gesto público y continuar en la acción 317. Además, si se determina que la zona en la que se ha realizado el al menos un gesto es una zona indefinida (por ejemplo, la localización estaba fuera de una zona definida, tal como las zonas pública y privada), el proceso puede determinar que el al menos un gesto es un gesto de zona indefinida y continuar en la acción 319.

40 Durante la acción 315, después de reconocerse un gesto privado por el sistema, el proceso puede obtener o generar una clave privada asociada con el al menos un gesto. En la presente realización, con el fin de simplificar la siguiente exposición, se supondrá que la clave privada es común a todos los gestos privados reconocidos. Sin embargo, de acuerdo con las realizaciones del sistema actual, una clave privada puede ser específica de un gesto privado específico. Por ejemplo, si el gesto privado es una palma abierta, el proceso puede obtener una primera clave privada, mientras que, si el gesto privado es una palma cerrada, el proceso puede obtener una clave privada diferente. Además, la clave privada puede ser una simple clave (por ejemplo, un indicador, un bit, etc.) o puede ser una clave criptográfica (por ejemplo, un número de múltiples dígitos complejo). Después de completar la acción 315, el proceso puede continuar en la acción 321.

50 Durante la acción 317 después de reconocerse un gesto público por el sistema, el proceso puede obtener o generar (dependiendo de los ajustes del sistema) una clave de gesto público correspondiente con el al menos un gesto. En la presente realización, se supondrá que la clave de gesto público será común a todos los gestos públicos. Sin embargo, también se prevé que una clave de gesto público pueda ser específica de un gesto público específico. Por ejemplo, en un caso en el que el gesto público es una palma abierta, el proceso puede obtener una primera clave de gesto público, mientras que, si el gesto público es una palma cerrada, el proceso puede obtener una clave de gesto público diferente. Además, se prevé que el proceso pueda distribuir la clave pública a uno o más contactos y/o direcciones deseados (por ejemplo, a Bob, a una dirección de página web, a una dirección de correo electrónico, etc.) usando cualquier método adecuado (por ejemplo, el correo electrónico, un SMS, un registro de página web, etc.) si se desea. Después de completar la acción 317, el proceso puede continuar en la acción 321.

60 Durante la acción 319 después de que se determina que el al menos un gesto es un gesto de zona indefinida, el proceso puede reproducir un mensaje que puede informar al usuario de que se ha realizado el al menos un gesto en una zona indefinida y solicitar la reintroducción de un gesto o secuencia de gestos. Después de completar la acción 319, el proceso puede repetir la acción 309.

65 Durante la acción 321, el proceso puede autorizar el acceso a un recurso tal como un contenido, una base de datos, una aplicación, un archivo, una llamada de vídeo, etc., de acuerdo con las claves privadas y/o públicas que pueden haberse obtenido durante las acciones 315 y/o 317, anteriores. Por ejemplo, en las realizaciones del sistema actual,

si se obtienen tanto las claves públicas como las privadas, entonces el proceso puede autorizar a un usuario a acceder a un directorio, un archivo, un contenido, una aplicación, etc., de acuerdo con los ajustes del sistema que pueden establecerse por el sistema y/o el usuario. Además, se prevé que el proceso pueda interactuar con una aplicación de cifrado de terceros (por ejemplo, Pretty Good Privacy (PGPTM), etc.) para cifrar/señalar y/o descifrar/verificar el contenido de acuerdo con las técnicas de encriptación asimétrica y/o simétrica usando, las claves privadas y/o públicas recuperadas, si se desea. Después de completar la acción 321, el proceso puede continuar en la acción 323, en la que el proceso puede actualizar la información histórica (por ejemplo, incluyendo una información relacionada con el usuario tal como la identificación, la localización, los intentos de acceso, los resultados, los tiempos, los gestos, la información de sensor, etc.) y almacenar esta información en una memoria del sistema para su uso posterior. Posteriormente, el proceso puede continuar en la acción 325, en la que puede terminar.

La figura 4 muestra las capturas de pantalla de 400A a 400F de las estaciones móviles (MS) MS-1 y MS-2 reproduciendo una llamada de vídeo entre dos usuarios de acuerdo con las realizaciones del sistema actual. En el siguiente ejemplo, la MS-1 es la MS de Jane y la MS-2 es la MS de Bob. Por consiguiente, la MS-1 está reproduciendo vídeo recibido desde la MS-2 y viceversa como puede apreciarse fácilmente. Además, la MS-1 puede reproducir también una imagen de lo que se está remitiendo a la MS-2 (tal como en una inserción dentro de la interfaz de usuario).

Las capturas de pantalla 400A y 400B ilustran una llamada de vídeo no segura entre Bob y Jane. Haciendo referencia a las capturas de pantalla 400B y 400C, si durante la llamada, Bob y Jane deciden participar en una llamada de vídeo segura, cada uno de ellos puede formar uno o más de los gestos privados (por ejemplo, 409) y/o de los gestos públicos (por ejemplo, los gestos privados 407) para generar u obtener sus propias claves de cifrado públicas y privadas correspondientes. Tras detectar que las claves son correctas (por ejemplo, a través de una comparación con las claves esperadas de una memoria del sistema), el proceso puede autorizar un recurso que en el presente ejemplo, es una aplicación de videoconferencia segura que puede codificar las transmisiones de vídeo conferencia entre los participantes (por ejemplo, el vídeo en el presente ejemplo) usando la clave pública de un destinatario y descifrar la información de llamada usando una clave privada de un receptor. En consecuencia, la aplicación de llamada de vídeo segura en cada respectiva MS pueden intercambiar de manera automática (por ejemplo, distribuir) la clave de cifrado pública. Durante la llamada, los gestos privados de Bob y Jane se muestran en un campo sin imágenes 417 que está en un área privada que no se transmite al otro participante durante la llamada en lugar de un campo de imagen 413 que está en un área pública y puede transmitirse al otro participante durante la llamada. En consecuencia, Bob y Jane pueden participar en una llamada de vídeo segura, como se muestra en las capturas de pantalla 400E y 400F formando uno o más de entre un gesto público y/o privado. De acuerdo con las realizaciones del sistema actual, durante la llamada, las MS pueden mostrar un elemento de menú que indica un estado de la llamada (por ejemplo, seguro o no seguro, como se muestra en las capturas de pantalla de la figura 4). Para finalizar la llamada, o para finalizar el cifrado de la llamada, Bob y/o Jane pueden formar otros gestos predeterminados que pueden reconocerse por sus respectivas MS y la llamada puede terminarse o posteriormente puede ser no segura (por ejemplo, no cifrada) basándose en el reconocimiento de estos gestos.

Además, se prevé que el sistema pueda determinar si un espacio específico en relación con una estructura corporal de un usuario es seguro (o no) y por lo tanto no puede (o puede) observarse por otras cámaras y/o personas no autorizadas. En consecuencia, el sistema puede examinar un espacio tridimensional (por ejemplo, usando un análisis de imágenes, DSP, etc.) para determinar si hay alguna persona no autorizada, cámaras, ventanas, etc., y/u otros dispositivos (por ejemplo, cámaras, sensores o, etc.) en una línea de visión de los sensores que potencialmente pueden ver o grabar un gesto formado en un espacio en cuestión. Si es así, el sistema puede determinar que el espacio determinado no es seguro y el sistema puede ajustar en consecuencia este espacio como un espacio no seguro (por ejemplo, una zona pública) y no localizará una zona privada en el espacio no seguro. De esta manera, el sistema puede determinar si un espacio corresponde a un espacio público o un espacio privado en relación con otro (por ejemplo, que no sea el usuario que realiza el gesto) objeto, persona, etc., además de o en lugar de determinar el espacio basándose en el usuario que realiza el gesto.

Posteriormente, el sistema podrá tener en cuenta los espacios no seguros al determinar una localización, una forma y/o un tamaño de una zona privada de tal manera que la zona privada no se localiza dentro de la totalidad o una parte de la zona no segura. Además, si ya se ha definido una zona privada, el sistema puede informar a un usuario (por ejemplo, a través de un mensaje tal como "la zona privada no es segura") y puede ajustar el tamaño, la forma y/o la localización de la zona privada de tal manera que la zona privada ya no se localice en una zona no segura. De acuerdo con las realizaciones del sistema actual, este análisis puede realizarse en tiempo real. En consecuencia, por ejemplo, si el sistema detecta que un individuo no autenticado ha entrado en una habitación con el usuario, el sistema puede determinar una localización, así como una orientación (por ejemplo, frente a la cámara, frente al usuario, etc.) de una persona y puede determinar si una zona privada es no segura. Posteriormente, el sistema puede informar al usuario con un mensaje apropiado tal como "la zona privada es no segura" y/o puede redimensionar, reformar y/o relocalizar la zona privada en consecuencia.

Por consiguiente, el sistema actual puede proporcionar un sistema para permitir a un usuario generar u obtener al menos una de entre una clave pública usando un gesto público y una clave privada usando un gesto privado.

Además, cuando el sistema detecta que un usuario ha introducido unos gestos privados y/o públicos correctos, el sistema puede autorizar un recurso seleccionado tal como un contenido, archivos, directorios, aplicaciones (por ejemplo, software, firmware y/o hardware), etc. Por ejemplo, en una realización del sistema actual, se prevé que el recurso seleccionado pueda incluir un bloqueo de puerta automático que puede desbloquearse cuando se autoriza el acceso al mismo.

Por otra parte, los gestos pueden caracterizarse adicionalmente como gestos comunes o personalizados, como puede establecerse por el sistema y/o el usuario. En estas realizaciones, un gesto común puede ser un gesto que está predeterminado por el sistema mientras que un gesto personalizado puede corresponder a un gesto que se enseña al sistema por un usuario tal como, por ejemplo, durante un proceso de inicialización y/o durante otra interacción del usuario con el sistema. La información relacionada con los gestos comunes puede obtenerse de una biblioteca de gestos comunes del sistema, mientras que los gestos personalizados pueden entrenarse por el usuario usando una aplicación de entrenamiento del sistema actual.

Además, un gesto de mano "signo V" puede identificarse por el sistema cuando el usuario extiende dos dedos de una mano correspondiente para formar una "V" con independencia de la orientación del signo V. Sin embargo, de acuerdo con las realizaciones del sistema actual, un gesto de mano con tres dedos extendidos puede identificarse por el sistema cuando el usuario extiende solo tres dedos de la mano correspondiente hacia el exterior (por ejemplo, en lugar de hacia abajo, hacia arriba, etc.). En estas realizaciones, la orientación del gesto puede comprender una parte del gesto y de ese modo, una respuesta diferente ilícita (por ejemplo, reconocida/no reconocida) en función de la orientación.

Se prevé además que, en otras realizaciones del sistema actual, el gesto público pueda ser un gesto que se realice lejos o cerca de un cuerpo de un usuario, pero, que no se realiza delante del cuerpo del usuario ya que esta zona puede estar reservada para una zona privada. Por lo tanto, los gestos privados pueden realizarse delante del cuerpo del usuario. Por ejemplo, un gesto privado puede incluir un gesto tal como un signo V, mientras que un gesto público puede incluir un movimiento tal como mover un brazo desde la rodilla a la cabeza del usuario.

El sistema puede comenzar a monitorizar los gestos una vez que se ha identificado una estructura corporal del usuario. Además, el sistema puede autenticar a los usuarios tal como se trata en el presente documento antes y/o después de que se haya reconocido un gesto. Además, los usuarios pueden autenticarse para proporcionar un gesto solo si tienen permiso para acceder al sistema, o de otra manera de acuerdo con la configuración del sistema. Posteriormente, el sistema puede monitorizar solo los gestos de los usuarios autenticados, si se desea.

Por lo tanto, las realizaciones del sistema actual pueden autorizar solo a un usuario si el usuario realiza un gesto público que pueda verse por los demás, y un gesto privado que solo puede verse por los sensores del sistema actual. De acuerdo con las realizaciones del sistema actual, un gesto/clave privado puede utilizarse para el cifrado o el descifrado con la clave pública correspondiente (por ejemplo, de un tercero) utilizada para el descifrado o cifrado.

Además, el sistema actual puede interactuar con los dispositivos de captura de imágenes basados en movimiento convencionales tales como el sistema Xbox™ Kinect™ de Microsoft™ Corporation que puede capturar la información de imagen, así como la información de profundidad en relación con el cuerpo del usuario o unas partes del mismo. A continuación, esta información puede procesarse mediante un procesador del sistema para hacer un seguimiento de los movimientos y/o de los gestos de un usuario en tiempo real y determinar las acciones realizadas por el usuario, tales como gestos, etc. Además, el sistema puede solicitar otra información antes de autenticar a un usuario o autorizar a un usuario a acceder a determinados recursos. Por ejemplo, el sistema puede autorizar solo el acceso a un recurso si las condiciones ambientales (por ejemplo, temperatura, presión, etc.) en la proximidad del usuario están dentro de un cierto intervalo (por ejemplo, 70-75 grados, etc.), en función de los ajustes del sistema.

La figura 5 muestra una parte de un sistema (por ejemplo, un procesador, una estación móvil, etc.) de acuerdo con una realización del sistema actual. Por ejemplo, una parte del sistema actual puede incluir un procesador acoplado operativamente a una memoria, una pantalla, unos sensores, y un dispositivo de entrada de usuario. La memoria puede ser cualquier tipo de dispositivo para almacenar los datos de aplicación, así como otros datos relacionados con el funcionamiento descrito, tales como datos de usuario, datos de gestos, etc. Los sensores pueden incluir una cámara (por ejemplo, una cámara de imágenes fijas, una cámara de vídeo, etc.) para generar la información de imagen de un usuario y/o los sensores de profundidad que pueden generar la información para determinar la profundidad y/o la distancia de una o más partes del cuerpo de un usuario (por ejemplo, uno respecto al otro y/o a otros objetos). Los datos de aplicación y otros datos se reciben por el procesador para configurar (por ejemplo, programar) el procesador para realizar las acciones de funcionamiento de acuerdo con el sistema actual. El procesador configurado de esta manera se convierte en una máquina de fin especial específicamente adecuada para realizarse de acuerdo con el sistema actual.

Las acciones de funcionamiento pueden incluir solicitar, proporcionar, y/o reproducir el contenido. Las acciones de funcionamiento pueden incluir una o más de entre identificar un usuario, determinar las zonas públicas y/o privadas, identificar los gestos, etc. La entrada de usuario puede incluir un teclado, un ratón, un ratón de bola u otro dispositivo, incluyendo unas pantallas táctiles sensibles, que pueden ser independientes o formar parte de un

- 5 sistema, tal como parte de un ordenador personal, un asistente personal digital, un teléfono móvil, un teléfono inteligente, un equipo decodificador, un televisor u otro dispositivo para comunicarse con el procesador 510 a través de cualquier enlace operable. El dispositivo de entrada de usuario 570 puede hacerse funcionar para interactuar con el procesador 510, lo que incluye permitir la interacción dentro de una UI como se ha descrito en el presente documento. Evidentemente el procesador 510, la memoria 520, la pantalla 530 y/o el dispositivo de entrada de usuario 570 pueden ser total o parcialmente una parte de un sistema de ordenador u otro dispositivo, tal como un cliente y/o un servidor como se ha descrito en el presente documento.
- 10 Los métodos del sistema actual son específicamente adecuados para realizarse por un programa de software de ordenador, conteniendo tal programa unos módulos correspondientes a una o más de las etapas o las acciones individuales descritas y/o previstas por el sistema actual. Tal programa puede, por supuesto, realizarse en un medio legible por ordenador (por ejemplo, una memoria no transitoria), tal como un chip integrado, un dispositivo periférico o una memoria, tal como la memoria 520 u otra memoria acoplada al procesador 510.
- 15 El programa y/o las partes del programa contenidas en la memoria 520 configuran el procesador 510 para implementar los métodos, las acciones de funcionamiento y las funciones desveladas en el presente documento. Las memorias pueden distribuirse, por ejemplo, entre los clientes y/o los servidores, o localmente, y el procesador 510, en el que pueden proporcionarse procesadores adicionales, también puede distribuirse o puede ser singular. Las memorias pueden implementarse como una memoria eléctrica, magnética u óptica, o cualquier combinación de las mismas u otros tipos de dispositivos de almacenamiento. Por otra parte, el término "memoria" debería interpretarse de manera suficientemente amplia como para abarcar cualquier información capaz de leerse desde o escribirse a una dirección en un espacio direccionable accesible por el procesador 510. Con esta definición, la información accesible a través de una red está todavía dentro de la memoria, por ejemplo, debido a que el procesador 510 puede recuperar la información de la red para su funcionamiento de conformidad con el sistema actual. El procesador 510 puede hacerse funcionar para proporcionar unas señales de control y/o realizar unas operaciones en respuesta a las señales de entrada desde el dispositivo de entrada de usuario 570, así como en respuesta a otros dispositivos de una red y ejecutar las instrucciones almacenadas en la memoria 520. El procesador 510 puede ser un circuito(s) integrado de aplicación específica o de uso general. Además, el procesador 510 puede ser un procesador dedicado para realizarse de acuerdo con el sistema actual o puede ser un procesador de fin general en el que solo una de las muchas funciones se hace funcionar para realizarse de acuerdo con el sistema actual. El procesador 510 puede funcionar utilizando una parte de programa, múltiples segmentos de programa, o puede ser un dispositivo de hardware que utiliza un circuito integrado dedicado o de uso múltiple.
- 20
- 25
- 30
- 35 Otras variaciones del sistema actual se ocurrirán fácilmente a un experto en la materia y estarán abarcadas por las siguientes reivindicaciones. A través del funcionamiento del sistema actual, se proporciona una solicitud de entorno virtual a un usuario para permitir una inmersión simple en un entorno virtual y sus objetos.

REIVINDICACIONES

1. Un método de comunicaciones seguro, comprendiendo el método unas acciones que se realizan mediante un procesador, comprendiendo las acciones:
- 5 obtener una información de sensor de al menos un usuario, comprendiendo la información de sensor una o más de entre una información de imagen y una información de profundidad;
reconocer al menos un gesto de acuerdo con la información de sensor del al menos un usuario;
autorizar el acceso a un recurso cuando el al menos un gesto corresponde a un gesto predefinido;
- 10 estando la autorización caracterizada por que comprende además:
- determinar si el al menos un gesto reconocido comprende un par de gestos que comprenden un gesto público y un gesto privado de acuerdo con una zona en la que se ha realizado el gesto, seleccionándose la zona a partir de una pluralidad de zonas en relación con una estructura corporal del al menos un usuario, en el que cada zona de la pluralidad de zonas es una zona pública o una zona privada; y
- 15 autorizar el acceso a un recurso basándose en el gesto público determinado y en el gesto privado determinado.
2. El método de la reivindicación 1, que comprende además una acción para determinar que el primer gesto es un gesto público cuando se determina que el primer gesto se ha realizado en la zona pública.
- 20 3. El método de la reivindicación 1, que comprende además una acción para determinar que el segundo gesto es un gesto privado cuando se determina que el segundo gesto se ha realizado en la zona privada.
- 25 4. El método de una de las reivindicaciones anteriores, en el que la acción para autorizar el acceso a un recurso comprende una acción para autorizar una llamada de video segura o una acción para autorizar a el al menos un usuario a acceder a un recurso que comprende una base de datos, una aplicación de ordenador o un contenido.
- 30 5. El método de las reivindicaciones anteriores, que comprende además una acción para obtener al menos una de entre una clave de cifrado pública correspondiente al gesto público y una clave de cifrado privada correspondiente al gesto privado en respuesta a el al menos un gesto reconocido.
6. Un servidor de comunicaciones seguro que comprende un procesador configurado para:
- 35 obtener una información de sensor de al menos un usuario, comprendiendo la información de sensor una o más de entre una información de imagen y una información de profundidad;
reconocer al menos un gesto de acuerdo con la información de sensor del al menos un usuario;
autorizar el acceso a un recurso cuando el al menos un gesto corresponde a un gesto predefinido;
- 40 estando el servidor caracterizado por que está configurado además para:
- determinar si el al menos un gesto reconocido comprende un par de gestos que comprenden un gesto público y un gesto privado de acuerdo con una zona en la que se ha realizado el gesto, seleccionándose la zona a partir de una pluralidad de zonas en relación con una estructura corporal del al menos un usuario, en el que cada zona de la pluralidad de zonas es una zona pública o una zona privada; y
- 45 autorizar el acceso a un recurso basándose en el gesto público determinado y en el gesto privado determinado.
7. El servidor de la reivindicación 6, en el que el procesador determina además que el primer gesto es un gesto público cuando se determina que el primer gesto se ha realizado en la zona pública.
- 50 8. El servidor de la reivindicación 6, en el que el procesador determina además que el segundo gesto es un gesto privado cuando se determina que el segundo gesto se ha realizado en la zona privada.
9. El servidor de una de las reivindicaciones 6 a 8, en el que cuando el procesador autoriza el acceso a un recurso el procesador autoriza una llamada de video segura o autoriza a el al menos un usuario a acceder a un recurso que comprende una base de datos, una aplicación de ordenador, o un contenido.
- 55 10. El servidor de una de las reivindicaciones 6 a 9, en el que el procesador obtiene además al menos una de entre una clave de cifrado pública correspondiente al gesto público y una clave de cifrado privada correspondiente al gesto privado en respuesta a el al menos un gesto reconocido.
- 60 11. Un programa informático almacenado en un medio de memoria no transitoria legible por ordenador, estando el programa informático configurado para realizar una comunicación segura de acuerdo con una de las reivindicaciones 1 a 5.
- 65

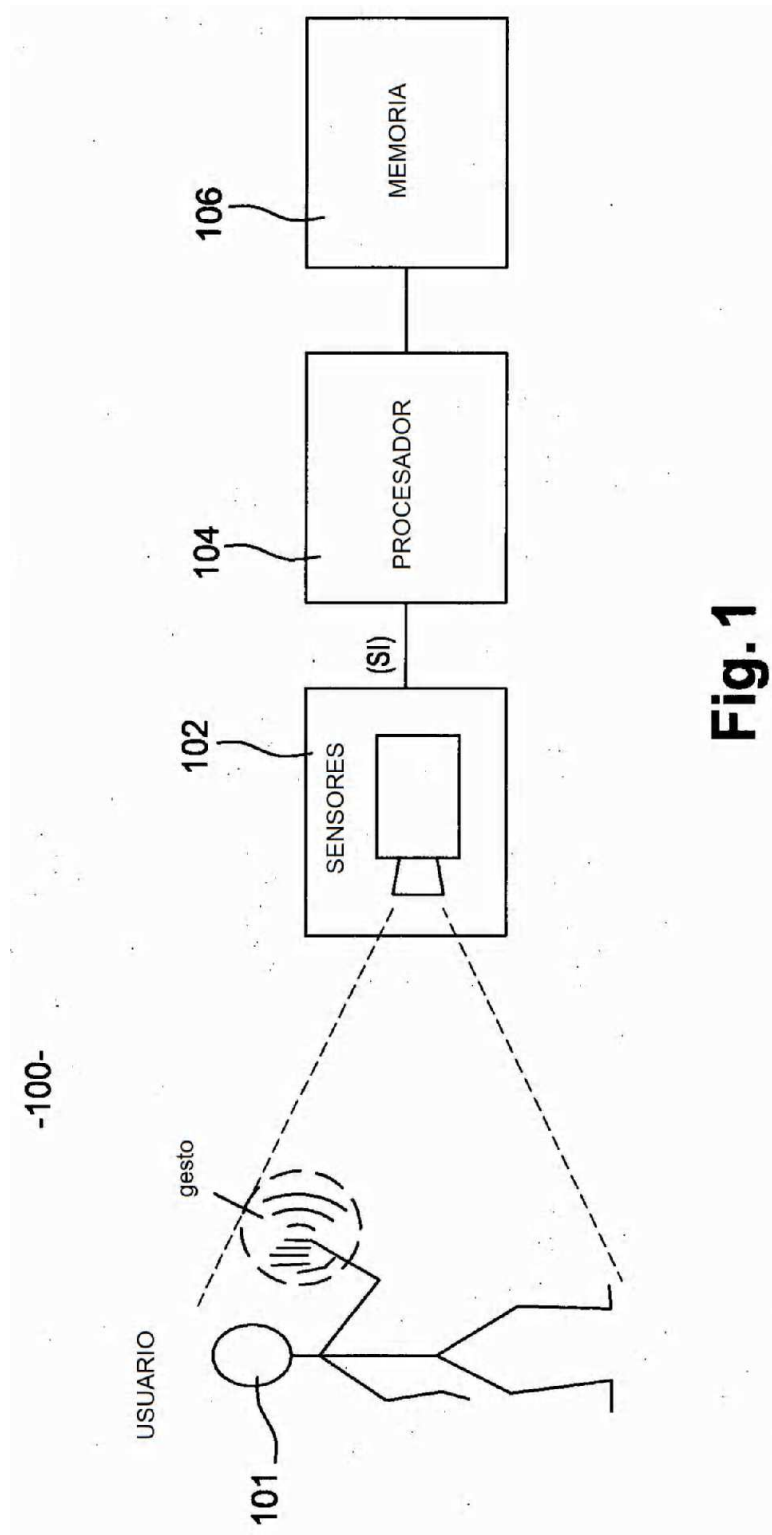
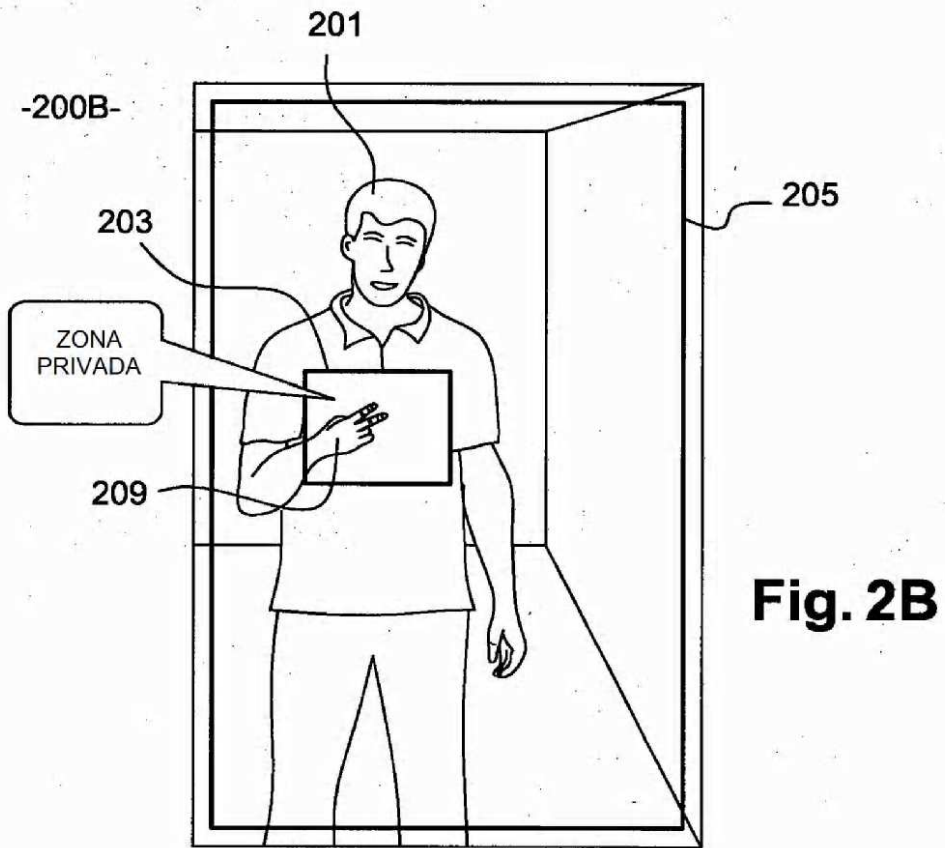
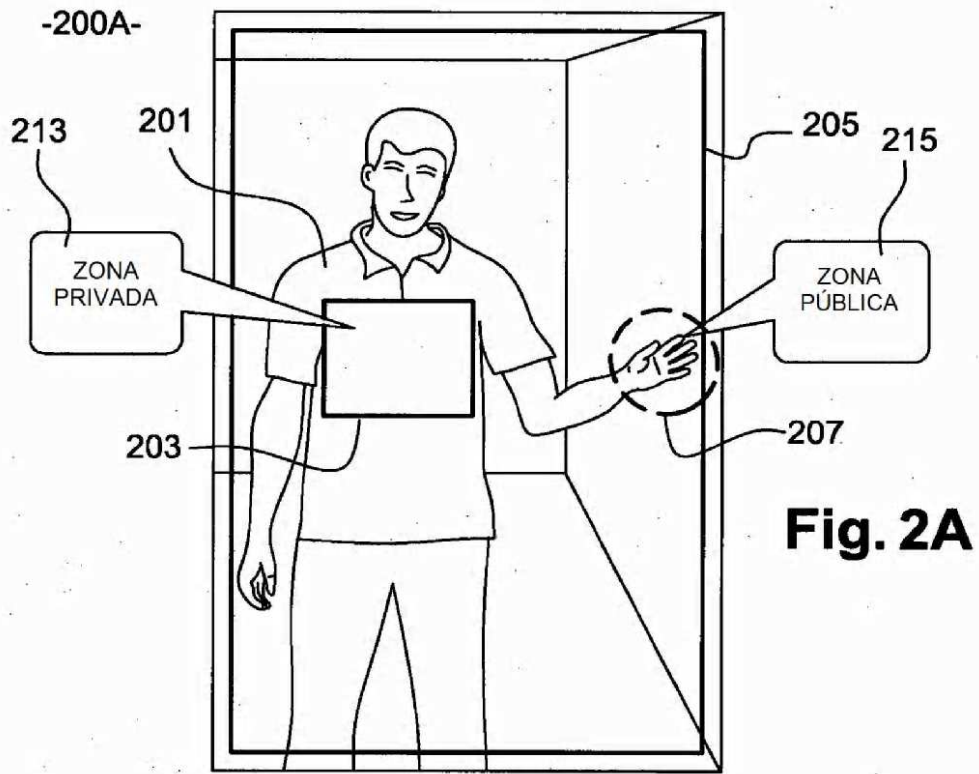
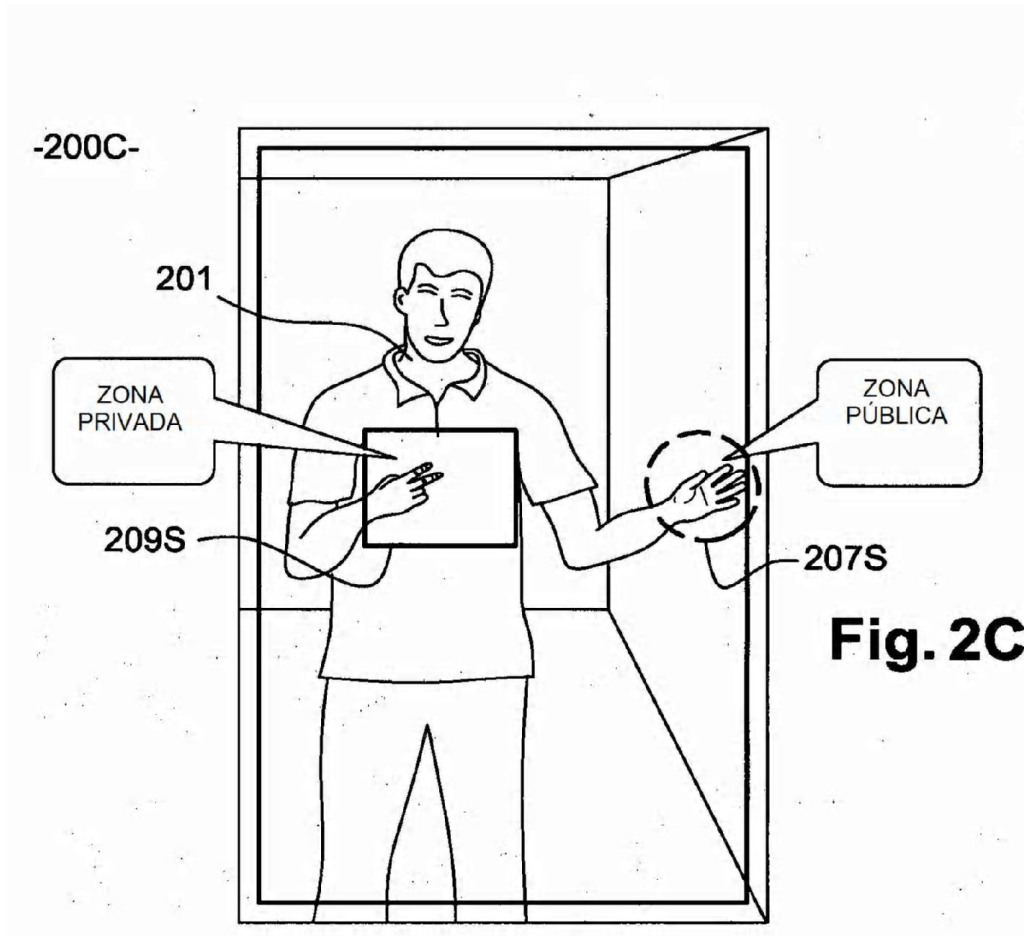


Fig. 1





-300-

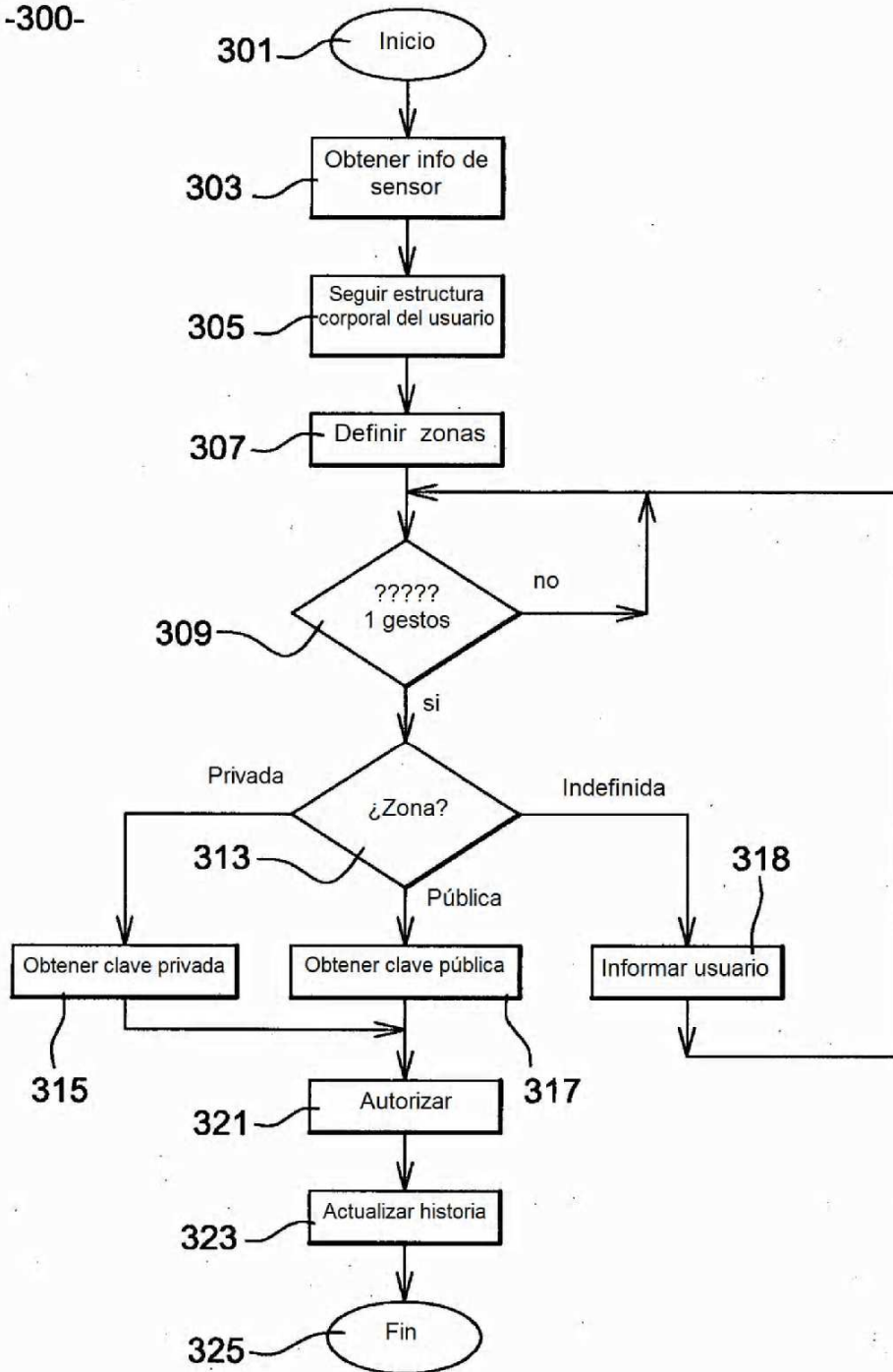
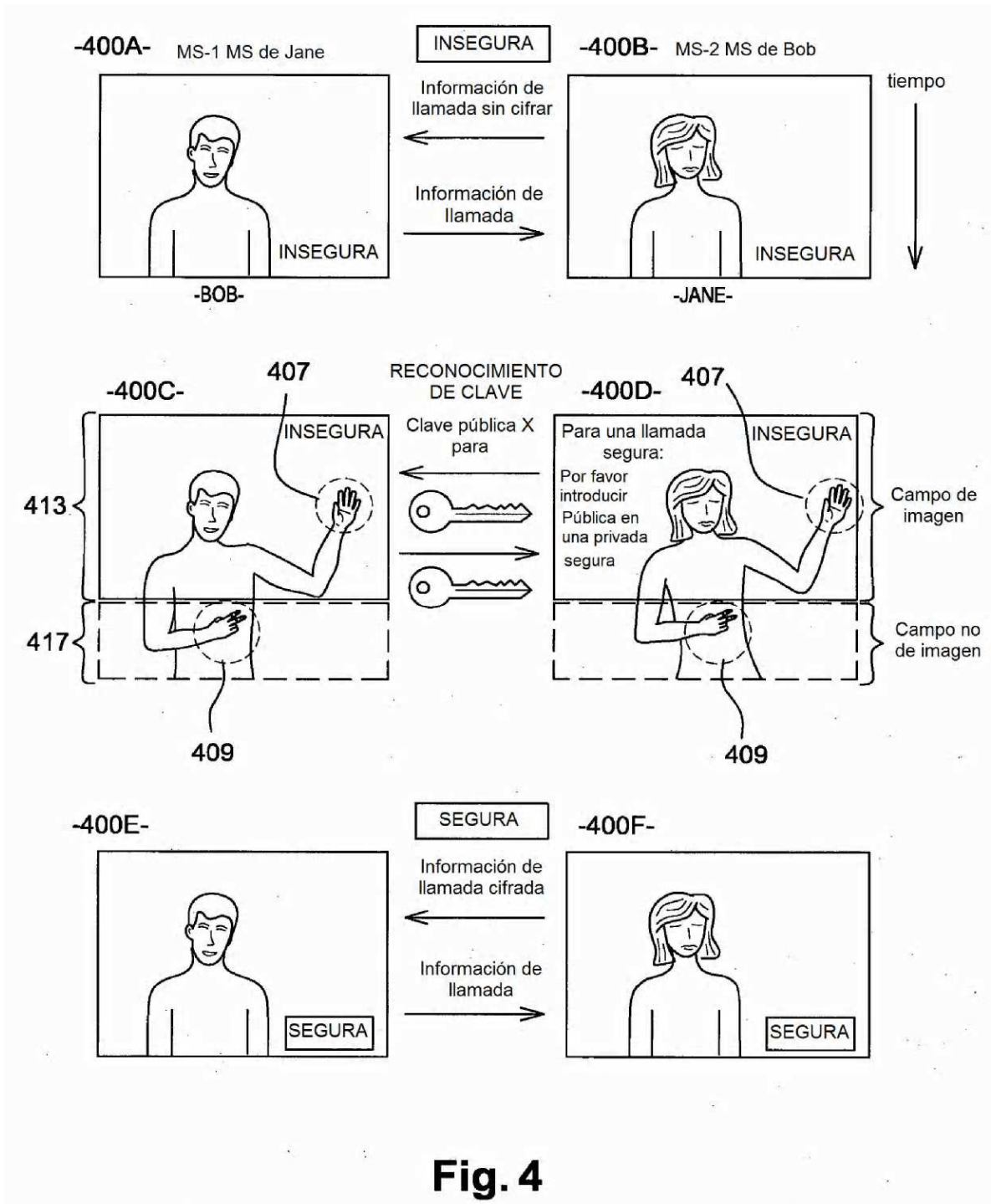


Fig. 3



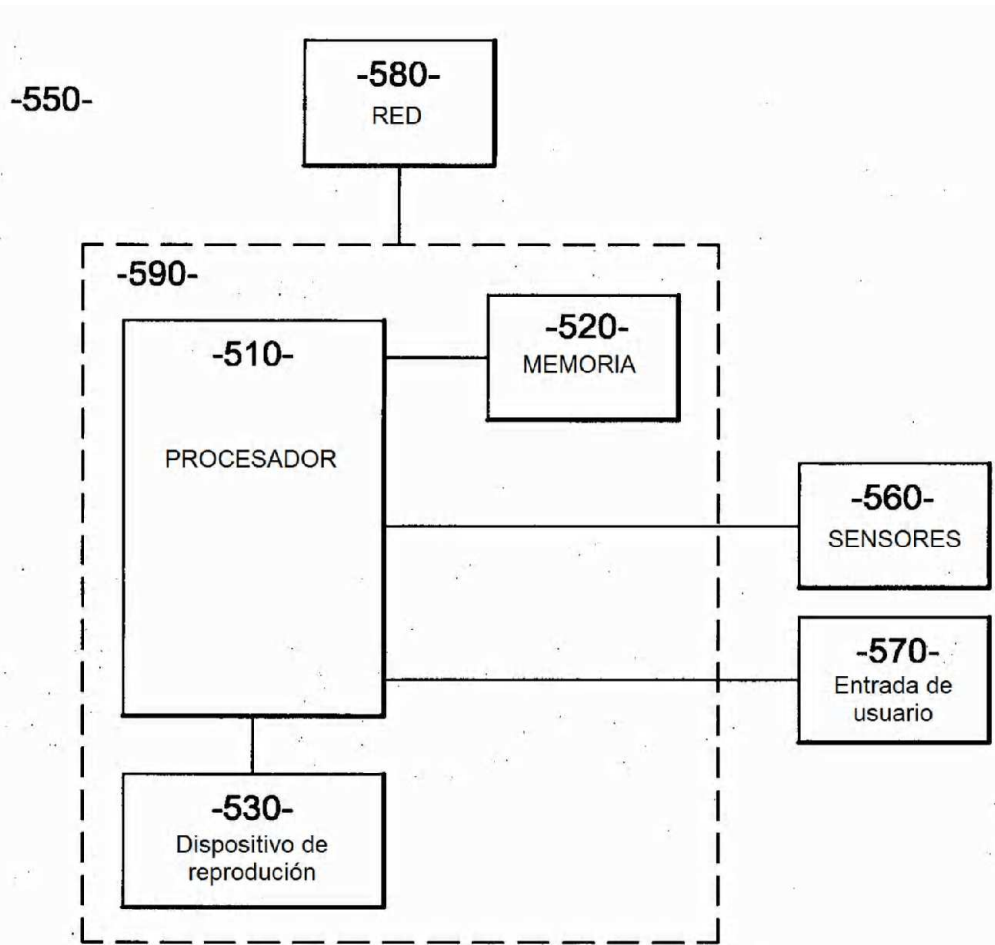


Fig. 5